Claims Intelligence Series

Siniestros de Ciber: el RGPD y ataques que comprometen las cuentas de usuario impulsan la siniestralidad

Ataques que comprometen las cuentas de usuario han superado al ransomware y a la violación de datos que llevan a cabo los hackers como el principal impulsor de los siniestros de Ciber de AIG EMEA[1], según las últimas estadísticas de Siniestros de Ciber. Casi una cuarta parte de los incidentes notificados en 2018 se debieron a ataques que comprometieron cuentas de usuario, lo que supone un aumento significativo con respecto al 11% registrado en 2017. Ransomware, la violación de datos por hackers y la violación de datos por negligencia de los empleados fueron los otros principales casos de brechas de seguridad en 2018.

Ataques que comprometen las cuentas de usuario[2] han entrado en el informe este año en una nueva categoría, dado el elevado número de siniestros que AIG ha recibido en los últimos 12 meses relacionados con este tipo de estafa.

En la mayoría de los casos, la estafa se puede rastrear hasta un correo electrónico de suplantación de identidad, tipo "phishing", que contiene un enlace o un archivo adjunto. Si el destinatario accede al contenido de un correo electrónico de phishing, puede permitir la intrusión en la bandeja de entrada del usuario. La mayoría de los usuarios están familiarizados con el concepto de "phishing", pero sigue habiendo un gran número de incidentes en los que el usuario sigue un enlace que dirige al destinatario a una pantalla de inicio de sesión fraudulenta. Tan pronto como la víctima introduce sus credenciales, éstas son capturadas por el ciberdelincuente, quien tiene la información necesaria para acceder a la cuenta de correo electrónico de la víctima.

El delincuente puede entonces enviar y recibir correos electrónicos desde la dirección de correo electrónico de la víctima y acceder a toda la información en la bandeja de entrada de su correo electrónico. En muchos casos, los ataques que comprometen las cuentas de usuario se ven agravados por el malware que propaga el ataque a los contactos de la bandeja de entrada del destinatario. Se trata de un tipo de estafa relativamente simple; quienes perpetran los ataques que comprometen las cuentas de usuario suelen dirigirse a las personas responsables de realizar los pagos, utilizando cuentas falsas para hacerse pasar por los ejecutivos senior o proveedores y solicitan transferencias de dinero, declaraciones de impuestos u otros datos confidenciales.

Titulares

- Los ataques que comprometen las cuentas de usuario son actualmente la principal causa de pérdidas en los siniestros de Ciber, seguida por el ransomware, que se está convirtiendo cada vez más en un objetivo y un factor desestabilizador, que afecta a los costes de interrupción de negocio. Todas las repercusiones de los ciberataques siguen estando fuertemente marcadas por el fallo humano.
- Los servicios profesionales son actualmente el sector más afectado por los siniestros de ciber riesgos, seguido de los servicios financieros. Sin embargo, los incidentes siguen extendiéndose entre una serie de sectores, lo que indica que ningún sector es inmune al ciberataque.
- En 2018 continuó la tendencia a largo plazo del aumento de la siniestralidad, con aproximadamente el mismo número de siniestros que en los dos años anteriores juntos.

Fig 1 **Siniestros de Ciber recibidos por AIG EMEA (2018) - Por incidente notificado**

Metodología

AIG realizó un análisis de más de 1.100 siniestros notificados en EMEA en el marco de sus pólizas de Ciber entre 2013 y diciembre de 2018. Los resultados de este análisis muestran una visión general de esta área solamente.

Cabe señalar que otras industrias y sectores que no se destacan en este informe también pueden ser objeto de siniestros frecuentes y graves. En 2018, el número de siniestros notificados en el marco de las pólizas de Ciber de AIG se ajustaba en gran medida al crecimiento de las primas de AIG para este producto.

*Ataques por denegación de servicio, procedimientos legales/regulatorios basados en las violaciones de la normativa sobre protección de datos

[1] Europa, Oriente Medio y África

[2] Anteriormente, estos ataques se enmarcaban en el ámbito de "otros fallos de seguridad/acceso no autorizado".

Otros ataques se centran en el contenido de la bandeja de entrada del destinatario, y la recopilación de información de los clientes y empleados, incluyendo los datos personales. También pueden estar dirigidos a información corporativa confidencial, incluyendo secretos comerciales, pero la mayoría están motivados por la obtención de beneficios económicos.

"En definitiva, lo que está detrás de muchos de estos casos es el crimen organizado", señala Jonathan Ball, socio de Norton Rose Fulbright. "No están interesados en robar datos personales y venderlos en la Dark Web. Es puro fraude financiero".

Los ataques que comprometen las cuentas de usuario suelen tener éxito porque utilizan la ingeniería social para crear correos electrónicos que parecen legítimos. Incluso las organizaciones más grandes pueden caer en las estafas, explica José Martínez, Vicepresidente de Grandes Siniestros de Líneas Financieras de AIG para EMEA, y sugiere que se necesita más inversión para formar al personal con el fin de identificar mejor los mensajes fraudulentos. "Todavía estamos viendo un nivel sorprendentemente alto de estas formas de fraude que se están perpetrando y algunas están afectando a clientes bastante grandes y sofisticados. Se puede pensar que todos los directores financieros de una gran empresa ya lo sabrían, pero sigue ocurriendo".

Para los siniestros cubiertos por ataques que comprometen las cuentas de usuario y suplantación de identidad, la póliza de Ciber cubre el coste de una investigación llevada a cabo por peritos informáticos para determinar si el sistema del asegurado ha estado expuesto e identificar los datos comprometidos. La póliza también cubre el asesoramiento jurídico sobre las obligaciones de información y notificación a los interesados y a los organismos reguladores, aunque a menudo se restringe la cobertura del seguro para las pérdidas financieras debidas a la actividad delictiva.

"Estos incidentes cada vez resultan más caros de investigar", señala Mark Camillo, Director de Ciber de AIG para EMEA. "Cuando un agente delictivo tiene acceso al buzón de correo, hay que hacer una investigación exhaustiva, entender a qué información puede haber tenido acceso y si ha activado algún requerimiento del RGPD".

Aunque las empresas de servicios financieros fueron las primeras en comprar seguros de ciber riesgos y el sector principal, vimos que las empresas de servicios profesionales avanzaron en 2018 en el número de siniestros notificados. Este es también el sector más vulnerable a los ataques que comprometen las cuentas de usuario. En términos interanuales, el número de siniestros procedentes de empresas de servicios profesionales, incluidos bufetes de abogados y auditores, ha pasado del 18% al 22%.

Fig 2 **Siniestros de Ciber recibidos por AIG EMEA (2018) - Por sector**

*Alimentos y bebidas, construcción, educación
Nota: Es posible que la suma de las cifras no alcance el 100% debido al redondeo.

Camillo cree que tales empresas pueden ser más propensas a ataques que comprometen las cuentas de usuario debido a la falta de sofisticación cuando se trata de seguridad cibernética. "Los delincuentes van a ir a donde haya más dinero en juego", dice.
"Debido a que están tan fuertemente regulados, uno tiende a descubrir que las empresas de servicios financieros tienen mejores controles que otros sectores, incluidos los servicios profesionales".

Él plantea la hipótesis de que cuando la Norma técnica revisada como parte de la Directiva de servicios de pago (PSD2, Payment Services Directive) entre en vigor en septiembre de 2019, puede haber una disminución en la frecuencia de los ataques que comprometen las cuentas de usuario. Según la directiva, se exigirá a los proveedores de servicios de pago que cumplan con los requisitos de autenticación de cliente sólida (SCA, Strong Customer Authentication) y acceso de terceros a cuentas bancarias, lo que debería dificultar que los estafadores roben y desvíen fondos

La seguridad de la contraseña es un problema recurrente, ya que los ciberdelincuentes explotan a las empresas que no han activado sus funciones de seguridad de Microsoft Office 365, donde la configuración predeterminada no habilita todas las características de seguridad necesarias, como la autenticación multifactor. Esto sigue siendo un incidente de alta frecuencia que se informa al equipo de reclamaciones cibernéticas de AIG casi a diario, según Kathy Avery, tramitadora de grandes siniestros de líneas financieras, AIG.

"Para las empresas afectadas por los ataques que comprometen las cuentas de usuario, puede ser muy perjudicial para su prestigio", continúa. "Siempre hay mucha preocupación por parte de los asegurados acerca de cómo van a informar a sus clientes. Con frecuencia solo se enteran del ataque porque sus clientes reciben correos electrónicos falsos y de phishing que parecen proceder del asegurado y que se han producido como resultado del ataque".

La preocupación por la seguridad en torno a las contraseñas y la autenticación multifactorial es importante, pero sigue siendo un hecho que muchos ataques sencillos pueden evitarse aumentando la concienciación del personal sobre los correos electrónicos de phishing e implementando un protocolo claro para el tratamiento de los correos electrónicos sospechosos.

Los servicios financieros son actualmente el segundo sector con mayor número de notificaciones de siniestros de Ciber. Tras haber ocupado anteriormente el primer puesto, actualmente representa el 15% de los siniestros en 2018, frente al 18% del año anterior.

Sin embargo, los porcentajes no reflejan toda la realidad. De hecho, el total de notificaciones de siniestros de los clientes de servicios financieros casi se duplicó entre 2017 y 2018, lo que demuestra que el sector sigue siendo un objetivo muy importante a pesar de su enfoque más sofisticado del ciberriesgo.

Lo mismo ocurre con la hostelería y el ocio. Si bien disminuyeron proporcionalmente del 5% al 4% interanual, las cifras reales de siniestralidad casi se duplicaron de nuevo en 2018. "Vemos muchas violaciones de los programas de fidelización, y las empresas de hostelería y las aerolíneas suelen verse afectadas", señala Ball. "Muchas de las marcas de hostelería son franquicias, pero comparten sus datos de afiliación y, a menudo, en cualquier hotel del mundo cualquiera puede acceder a estos datos".

El Factor Humano

Los errores humanos y el comportamiento siguen siendo un factor importante en los siniestros de Ciber. Pese a que muchas organizaciones lo recomiendan, los empleados suelen utilizar contraseñas inadecuadas o las mismas contraseñas en múltiples aplicaciones, por ejemplo.

"Un cliente muy conocido que aseguramos frustró un ataque después de detectar un intruso en su sistema", comenta Kathy Avery. "Decidieron que debían restablecer todas las contraseñas y pidieron a todos los empleados que adoptaran nuevas contraseñas, pero se dieron cuenta de que no podían deshacerse del intruso debido a este problema de seguridad con las contraseñas. Así que tuvieron que hacerlo por segunda vez usando contraseñas generadas al azar para cada usuario y esto, finalmente, logró bloquear el acceso".

En las estadísticas de siniestros de este año, las notificaciones de siniestros por negligencia de los empleados se duplicaron del 7% al 14%. Las pérdidas son provocadas por el personal que envía correos electrónicos que contienen datos de la empresa a personas equivocadas o por la pérdida de ordenadores portátiles y otros dispositivos. En el marco del RGPD ha aumentado el número de notificaciones de incidentes de este tipo.

"Estamos viendo problemas como cuando los archivos adjuntos de los correos electrónicos no se comprueban correctamente antes de su envío y, sin darse cuenta, el remitente de lo que cree que es un único registro de datos personales confidenciales que se envía al interesado, termina enviando una mayor recopilación de datos personales confidenciales de otros interesados", afirma Jonathan Ball.

Otro error común son las hojas de cálculo de Excel. "Hay demasiados empleados que no entienden cómo funciona el programa Excel y que, por ejemplo, puede ser que solo se puedan ver ciertos datos de la hoja de cálculo en la pantalla, pero eso se debe a que el botón de filtrado está activado", dice Ball. "Y luego envían el documento sin darse cuenta de que si el destinatario va a la línea superior y pulsa 'quitar filtros' aparecen otras cien mil líneas de datos. Hace poco tuvimos que enfrentarnos a un incidente muy grave que ocurrió de esta manera en un banco".

"Hay toda clase de errores humanos que se arrastran", continúa. "Los usuarios siguen haciendo clic en los correos electrónicos de phishing continuamente, a pesar de la formación. Y una de las cosas que realmente agrava el coste de hacer frente a los incidentes, incluido el aumento tanto de la necesidad como de los costes de las notificaciones a los organismos reguladores y a los interesados, es el uso por parte de los empleados del correo electrónico de la empresa para asuntos privados, en particular para asuntos financieros privados".

Aumenta el ransomware selectivo

El ransomware, que era el principal tipo de violación en 2017 cuando representaba el 26% de las notificaciones, se ha reducido ligeramente, llegando al 18% de las notificaciones de siniestros de Ciber en 2018. Sin embargo, como se pronosticó en el informe del año pasado, hay una serie de casos que muestran que los ataques de ransomware y extorsión se están volviendo más selectivos, con el ataque a Norsk Hydro como uno de los ejemplos de más alto perfil.

El gigante noruego de la fundición de aluminio fue víctima de un ataque de ransomware de difícil detección conocido como "LockerGoga", a través del cual los ciberdelincuentes accedieron a las redes de la empresa en un ataque dirigido. La empresa se vio obligada a detener la producción en varias plantas de Europa y los EE.UU. y se vio obligada a cambiar a operaciones manuales mientras intentaba contener el problema, lo que causó pérdidas generalizadas de interrupción de negocio.

La decisión de pagar o no la solicitud de rescate o extorsión sigue dependiendo de la forma en que la organización haya realizado la copia de seguridad de sus datos y de la posible interrupción de negocio que pueda derivarse de ello. "El impacto del ransomware se puede mitigar en gran medida si existe una buena gestión de las copias de seguridad", afirma Avery. "Pero vemos repetidamente que los procedimientos son deficientes".

Mientras tanto, las solicitudes de rescate han aumentado en magnitud. Mientras que las cantidades iniciales exigidas por los atacantes de WannaCry estaban entre 300 $ y 600 $, en 2018 ha habido casos en los que los ciberdelincuentes han solicitado decenas de miles a millones de dólares.

Mientras tanto, los costes por desestabilización e interrupción de negocio asociados con estos ataques han aumentado. Y en una era del RGPD, también existe la necesidad de establecer si los datos sensibles se han visto comprometidos.

"Hemos visto una mayor incidencia de extorsión en 2018 y un mayor gasto para que los sistemas puedan volver a estar en línea", afirma Camillo. "Incluso si pagas un rescate para descifrar tus archivos, es un proceso muy laborioso de doble comprobación para que el descifrado funcione, y luego aislar tus datos para asegurarte de que no te vuelvas a infectar y limpiar tus archivos antes de volver a instalarlo todo. Es muy caro y es muy problemático, además de ser un último recurso, cuando la ley lo permite".

Anticipa que los siniestros de Ciber por interrupción de negocio continuarán siendo significativos en el futuro, a medida que los ataques ransomware y extorsión se volverán más selectivos, mientras que los asegurados serán más conscientes del alcance de su cobertura.

"Anticipamos un aumento de los siniestros a nivel mundial", señala Camillo. Los incidentes selectivos, como el ataque a Norsk Hydro, podrían ser más alarmantes en 2019. La rápida propagación de malware o el ataque a un proveedor de servicios clave por parte de entidades gubernamentales podría causar pérdidas generalizadas por interrupción de negocio e interferir en una amplia gama de sectores, lo que también podría causar daños físicos significativos".

“Efecto RGPD” y siniestralidad

Ha habido un fuerte "efecto RGPD" en la siniestralidad de 2019, con un aumento de las notificaciones tras la aplicación del Reglamento General de Protección de Datos de la UE en mayo de 2018. Las disposiciones de la nueva normativa, incluidas las estrictas directrices de notificación de las violaciones, están dando lugar a notificaciones en tiempo y forma por parte de los clientes.

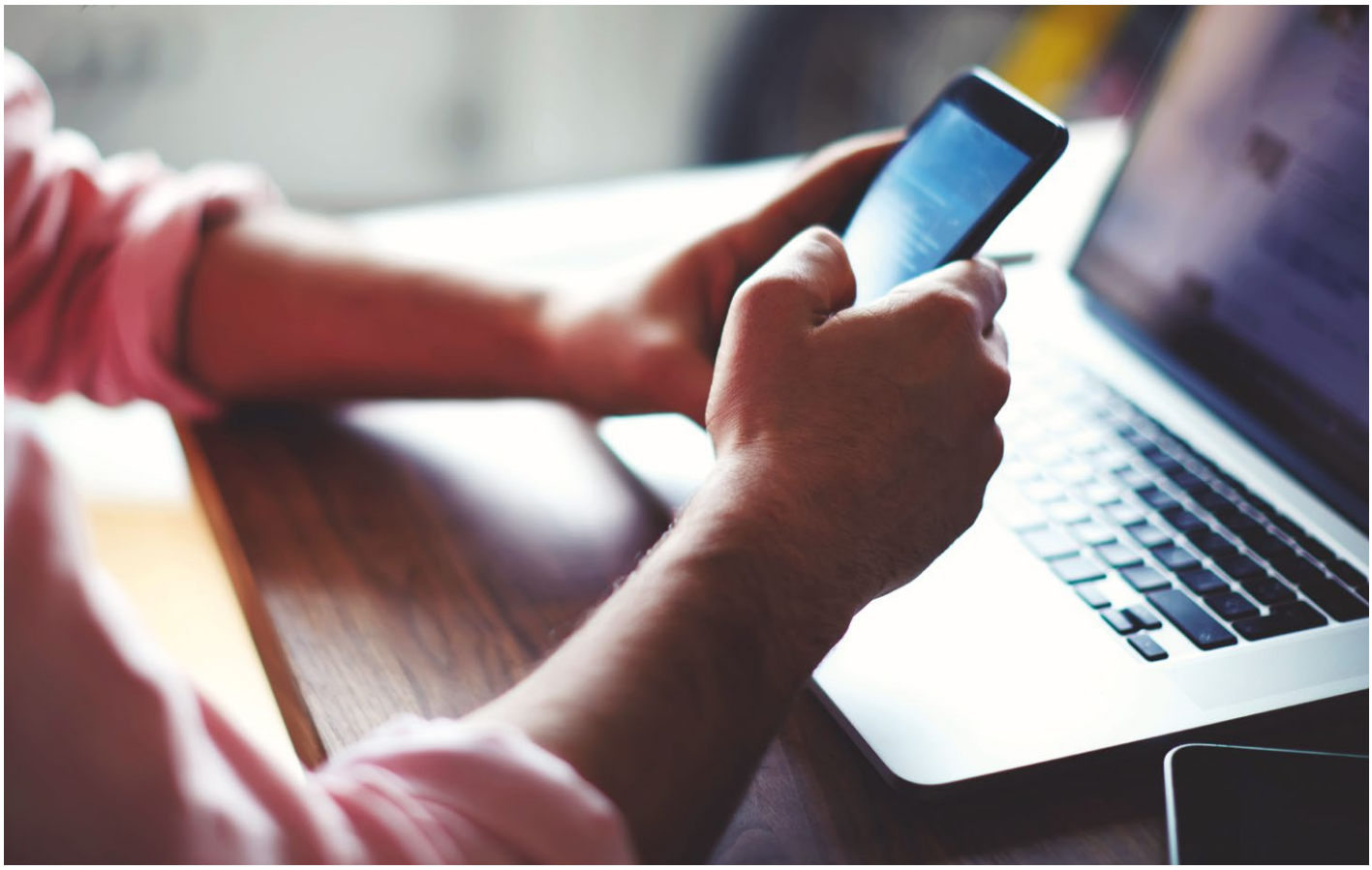
"Hay un límite de tiempo muy estricto, particularmente para informar al organismo regulador y, como consecuencia de ello, hay un aumento en los costes iniciales", señala Avery. "En nuestra póliza, tenemos un periodo de 48 o 72 horas para asumir los costes iniciales, y estamos viendo un aumento en la siniestralidad para estos primeros periodos como resultado del RGPD. Además, los costes legales, periciales e informáticos también han aumentado, lo que puede dar lugar a mayores desembolsos en el marco de la póliza".

Algo menos del 20% de los siniestros de AIG que se recibieron en 2018 incluían una notificación en virtud del RGPD, con unos costes de ajuste significativamente superiores en comparación con los siniestros en los que no se notificaron las violaciones relativas a los datos. El número de siniestros que se comunican a nuestro ‘Servicio de primera respuesta ante incidentes’ ha aumentado en más de un 50% en el caso de los siniestros en los que se notificó a los interesados y/o a las autoridades de protección de datos, y los asegurados recibieron asesoramiento y asistencia legal para preparar sus notificaciones reglamentarias.

"Hemos observado que nuestra empresa recibe un gran volumen de trabajo y, obviamente, existe un aumento en los costes en que incurren los asegurados y/o la aseguradora en la gestión de los incidentes del RGPD por incumplimientos que en realidad son de poca importancia", señala Jonathan Ball, de Norton Rose Fulbright. "Son el tipo de incidentes que antes del RGPD, una organización probablemente habría resuelto por sí misma sin asesoramiento legal externo".

En Europa existe una clara división entre el norte y el sur en lo que respecta a las notificaciones de violaciones de datos del RGPD, siendo el norte de Europa responsable de la gran mayoría de las notificaciones, lo que sugiere una diferencia en la forma de cumplir con el reglamento. Por ejemplo, cuando en Irlanda el 48% de los siniestros comunicados dieron lugar a una notificación a un organismo regulador, menos del 10% de los siniestros comunicados en España fueron notificados (por la tipología de incidente y mecanismos de seguridad en los datos comprometidos no ha sido obligatorio/recomendable el proceso de notificación al regulador). El RGPD también puede aplicarse a clientes ubicados en jurisdicciones fuera de Europa. Esto se ve confirmado por el aumento de las notificaciones de la región de Oriente Medio y África, donde ha habido una mayor siniestralidad en los últimos 12 meses.

Si desglosamos las estadísticas de AIG sobre reclamaciones de Ciber por región, se observa que en los últimos 12 meses se han producido aumentos significativos en las notificaciones procedentes de Bélgica, los Países Bajos, Alemania, Francia e Irlanda, mientras que también han aumentado las notificaciones de Suecia y Grecia. España y Reino Unido se matienen como países con mayor frecuencia de notificación bajo la poliza de ciber riesgos.



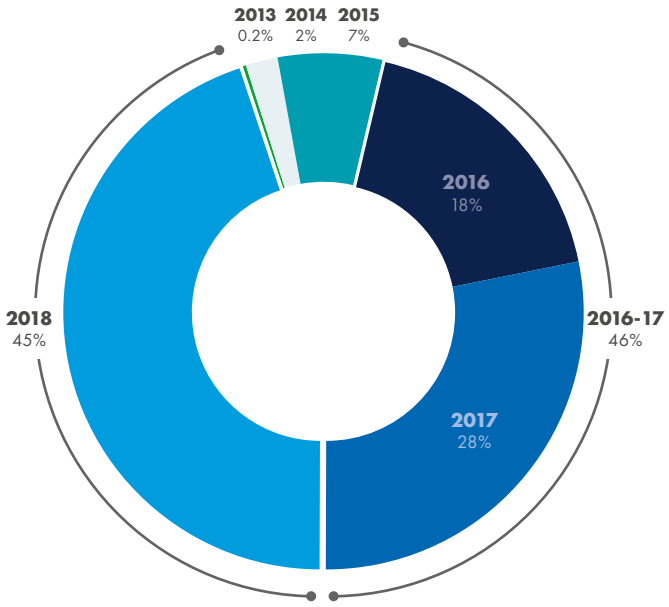
Mirando hacia el futuro: Avanzamos hacia una cobertura afirmativa

La tendencia a largo plazo del aumento de la siniestralidad ha continuado en 2018, al igual que en los cinco años anteriores, lo que refleja tanto el crecimiento y el grado de desarrollo de las soluciones de Ciber de AIG, como la sofisticación cada vez mayor de los compradores y el conocimiento del alcance del producto. A medida que los ciber riesgos se convierten en una amenaza cada vez mayor para muchas organizaciones, según nuestra experiencia en siniestros, las pérdidas previstas seguirán aumentando tanto en frecuencia como en gravedad en los distintos sectores.

Camillo observa un continuo movimiento hacia una cobertura afirmativa por parte de los clientes interesados en asegurarse de que sus pólizas respondan según lo esperado. "Recientemente ha habido algunas percepciones erróneas en la prensa sobre las coberturas de la Ciber póliza".

"Lo que nuestros índices de siniestralidad muestran claramente es que más usuarios están contratando la cobertura y el producto está respondiendo a las necesidades de nuestros clientes", continúa. "Incluye una cobertura flexible y es muy fácil notificar un incidente a través de la línea directa.

Fig 3 **Siniestros de Ciber recibidos por AIG EMEA (2013-2018) – Volumen 2017 28%**



Los clientes prefieren una cobertura de Ciber afirmativa, que los indemnizará frente a una serie de pérdidas cubiertas, incluidos los incidentes de privacidad, la extorsión cibernética y la interrupción de negocio en la red, incluidos los proveedores de servicios subcontratados y los fallos del sistema".

Estudios de casos de siniestros*

El fabricante paga un rescate de 25.000 € tras sufrir una interrupción de negocio.

Se produjo un ataque a los sistemas informáticos del asegurado a través de un programa malicioso de tipo ransomware conocido como "Detractor". Tres servidores de la infraestructura se vieron afectados, los cuales fueron encriptados, lo que provocó la encriptación de las carpetas. Las copias de seguridad disponibles, que estaban en un servidor diferente, fueron eliminadas (presumiblemente por los ciberdelincuentes). Por lo tanto, los sistemas afectados no pudieron ser restaurados a través de las copias de seguridad.

Simultáneamente, los atacantes exigieron que el asegurado pagara un rescate para descifrar el sistema. La actividad del asegurado se vio interrumpida por la imposibilidad de restablecer los sistemas afectados. No podía entregar envíos ni recibir materiales y no podía efectuar pagos ni recibir cobros.

El objetivo del ransomware no era robar información y no había habido una violación de la información personal. Por lo tanto, el día 10 del incidente, el asegurado pagó un rescate de 25.000 € en BitCoin y pudo restablecer su actividad. AIG cubrió el pago del rescate, los gastos de respuesta al incidente y la grave interrupción en la red, que incluía un aumento de los gastos de funcionamiento y de los pedidos cancelados.

La cuenta de correo electrónico se ha visto comprometida en el intermediario de servicios financieros

El asegurado, una empresa de servicios profesionales para PYMES, fue alertado de un incidente después de recibir notificaciones de varios clientes que habían recibido un correo electrónico sospechoso de un empleado de la empresa. El correo electrónico contenía varios enlaces y adjuntaba una factura en PDF en la que se solicitaba el pago a los destinatarios.

Tras la investigación inicial se determinó que la cuenta de correo electrónico del empleado había sido atacada y se había enviado un correo electrónico de phishing que contenía una factura adjunta a 5.500 direcciones de correo electrónico. El asegurado actuó de forma diligente para adoptar medidas correctivas en relación con el correo electrónico de phishing, enviando una notificación a los 720 contactos de correo electrónico de la cuenta atacada e instándoles a no hacer clic en el archivo PDF adjunto. Se cambiaron las contraseñas tanto de la cuenta de correo electrónico atacada como de las de otros empleados de la empresa.

AIG recomendó a los asegurados que notificaran a la Oficina del Comisionado de Información ("ICO", por sus siglas en inglés) por precaución, a pesar de que la única información identificable de los correos electrónicos de phishing eran los nombres y lugares de trabajo de los destinatarios. La recomendación de notificar se debió, en parte, a la naturaleza de las actividades de la empresa, incluida la venta de productos de seguros de Ciber, y a cuestiones de prestigio.

*Los escenarios aquí descritos se ofrecen solo a modo de ejemplo. La cobertura depende de los hechos reales de cada caso y de los términos, condiciones y exclusiones de cada póliza individual. Cualquier persona interesada en los productos anteriores debe solicitar una copia de la propia póliza para obtener una descripción del alcance y las limitaciones de la cobertura. Las indemnizaciones estan expresadas en euros aunque en algunos de estos ejemplos se pagó en otras monedas (1 GBP = 1.10 EUR y 1 USD = 0.90 EUR).

Violación de la red en una empresa internacional de energía y logística con sede en Oriente Medio

A finales del año pasado, el asegurado sufrió una serie de ataques violentos contra la infraestructura de su red, lo que dio lugar a que los ciberdelincuentes obtuvieran acceso a su red, muy probablemente a través de su servidor de correo electrónico en la nube, si bien el método de intrusión específico aún sigue siendo objeto de investigación. La red del asegurado comprende aproximadamente 5.000 dispositivos de EndPoint y, tras el primer análisis, se identificaron aproximadamente 2.900 unidades que podrían haber estado en peligro. Como resultado, todos los usuarios se vieron obligados a cambiar sus contraseñas y, posteriormente, se introdujo la autenticación de dos factores.

El asegurado contactó con los proveedores de servicios de AIG en el periodo de cobertura de 72 horas de Primera Respuesta de la póliza. Debido a las restricciones gubernamentales, el asegurado no podía permitir que sus datos se trataran fuera del país y, por lo tanto, los peritos informáticos se limitaron inicialmente a proporcionar asesoramiento por teléfono y correo electrónico. Pero AIG pudo proporcionar un equipo local de peritos informáticos para llevar a cabo las investigaciones in situ, junto con los asegurados y sus asesores de ciberseguridad.

El objetivo inicial era identificar los puntos de acceso y garantizar que estuvieran cerrados a los ciberdelincuentes. Como resultado de la identificación de los puntos de acceso comprometidos, junto con el análisis del tráfico de red, fue posible identificar cómo los atacantes habían obtenido acceso a las cuentas de usuario. También se identificó que los atacantes podrían haber obtenido acceso a cuentas de correo electrónico de los usuarios y a más de 2.000 archivos con datos personales, además de datos confidenciales de la empresa, como licitaciones, detalles de los proyectos y datos financieros.

Transcurridos más de seis meses, las investigaciones sobre una posible exposición de las cuentas de correo electrónico siguen en curso, al igual que el examen y el análisis de los datos comprometidos. Los costes siguen contrayéndose y hasta la fecha superan los 300.000 €.

Un minorista se ve afectado por un ataque de ransomware y la interrupción de negocio

El asegurado es un minorista internacional con más de 100 tiendas y presencia en Internet. Mientras realizaban algunos cambios en sus sistemas informáticos y en el almacenamiento de datos, sufrieron lo que parecía ser un ciberataque sofisticado y selectivo que encriptó todos sus archivos, incluidos los que se encontraban en la nube. Los ciberdelincuentes exigieron un rescate a cambio de facilitar un código de descifrado.

AIG designó inmediatamente a peritos informáticos que estuvieron en el lugar ininterrumpidamente durante largos periodos de tiempo, trabajando inicialmente para proteger el sistema e intentando recuperar los datos no cifrados. Esto resultó ser muy difícil y no se pudo lograr en un plazo que permitiera la reanudación de la actividad normal. Las tiendas podían seguir operando con cajas manuales, pero el ataque les impidió reponer existencias en las tiendas o procesar pedidos en línea, lo que provocó una importante interrupción de negocio.

Aunque se mostraba reacio a tratar con los ciberdelicuentes, tras un largo periodo de tiempo sin poder realizar su actividad comercial, el asegurado decidió pagar la demanda de rescate (135.000 € en BitCoin). AIG presto asistencia al asegurado en la búsqueda de Bitcoins. Una vez pagado el rescate – un concepto cubierto por la póliza – se proporcionó el código de descifrado. Todos los archivos tuvieron que descifrarse manualmente utilizando el código, un proceso laborioso y costoso en lo que respecta a la mano de obra, que fue abonado por AIG de acuerdo con las condiciones de la póliza.

AIG también cubrió el coste de los honorarios adicionales de los diversos proveedores de software existentes del asegurado para obtener soporte y equipos adicionales que facilitaron el proceso de descifrado. El asegurado tenía un límite de cobertura de solo 1.100.000 €, que resultó ser insuficiente. Solo los honorarios de Servicios de Informática Forense fueron más de 550.000 €. El asegurado recibió el pago del límite de indemnización restante cuando las estimaciones preliminares de la pérdida de beneficios indicaron que la perdida sería superior a 600.000 €. En esta ocasión no hubo constancia de que se hubiera accedido o extraído ningún dato personal, pero el asesoramiento legal e informático para determinar esta circunstancia estaba cubierto por los términos de la póliza del asegurado.

CLAIMS FIRST

www.aig.com.es

CONTACTO

Olivier Marcen
Líder de Producto
CyberEdge Sur de Europa
Olivier.Marcen@aig.com

Carlos Rodriguez
Líder de Producto CyberEdge
España
Carlos.Rodriguez@aig.com

Lucas Scortecci
Director Líneas Financieras
Iberia & Latam
Lucas.Scortecci@aig.com

AUTORES

Mark Camillo
Director de Cíber
para EMEA
mark.camillo@aig.com

Kathy Avery
Tramitadora de Grandes
Siniestros de Líneas Financieras
kathy.avery@aig.com

José Martinez
Vicepresidente, Grandes Siniestros de
Líneas Financieras, EMEA
jose.martinez@aig.com

GBL00003595 0719