GUÍA CYBER

CASOS PRÁCTICOS DE SINIESTROS CIBERNÉTICOS

SU GESTIÓN Y LA PARTICIPACIÓN DEL SEGURO

COMISIÓN DE TRABAJO
RIESGOS TECNOLÓGICOS

agers

CASOS PRÁCTICOS DE SINIESTROS CIBERNÉTICOS

SU GESTIÓN Y LA PARTICIPACIÓN DEL SEGURO

COMISIÓN DE TRABAJO DE RIESGOS TECNOLÓGICOS AGERS

ISBN: 978-84-09-67410-7
Registro: M-26145-2024
Copyright: DEP638675558877660852
Nota Legal - Copyright

ÍNDICE

PRÓLOGO

En el contexto actual, donde la economía global depende cada vez más de los activos digitales, la ciberseguridad se posiciona como una prioridad estratégica para todas las organizaciones. La guía "Casos prácticos de siniestros cibernéticos", desarrollada por la Comisión de Riesgos Tecnológicos de AGERS, es un recurso esencial que combina experiencia práctica y análisis detallado para fortalecer la capacidad de respuesta ante incidentes cibernéticos. Desde CyberMadrid, queremos aportar una reflexión sobre la importancia del sector asegurador en este ámbito, especialmente en lo relativo a la protección de las pequeñas y medianas empresas (pymes) y los autónomos, quienes enfrentan desafíos únicos en la gestión de riesgos digitales.

Según datos recientes, para 2024 se espera que **más del 60% del PIB mundial esté directamente relacionado con actividades digitales**. Este cambio hacia una economía digital ha hecho que las organizaciones, independientemente de su tamaño, enfrenten riesgos cibernéticos significativos.

El ransomware, las filtraciones de datos y los ataques a infraestructuras críticas son solo algunas de las amenazas que pueden paralizar operaciones, dañar reputaciones y generar pérdidas económicas millonarias. Por ejemplo, en el último año, el mercado global ha reportado **un incremento del 40% en incidentes relacionados con ransomware y un 28% en violaciones de datos personales**. Estos eventos subrayan la vulnerabilidad generalizada y la urgencia de implementar medidas efectivas de mitigación y respuesta.

En este panorama de riesgos , el sector asegurador se ha convertido en un aliado imprescindible para gestionar los riesgos cibernéticos. Los ciberseguros no solo ofrecen una red de protección financiera, sino que también proporcionan acceso a servicios especializados como análisis forense, gestión de crisis y recuperación de datos. Según las últimas cifras, **el mercado global de ciberseguros se valoró en 14.000 millones de dólares en 2023, con una proyección de crecimiento anual compuesto del 25% hasta 2030**. Este crecimiento refleja tanto la creciente percepción del riesgo como la necesidad de soluciones estructuradas para enfrentarlo.

Sin embargo, es fundamental destacar que el alcance de los ciberseguros no debe limitarse a grandes corporaciones. **Las pymes y los autónomos representan más del 95% del tejido empresarial global y, a menudo, carecen de los recursos necesarios para abordar** de manera independiente las consecuencias de **un incidente cibernético**. Un informe reciente señala que menos del 15% de estas empresas cuentan con una cobertura adecuada de ciberseguridad, lo que las deja expuestas a pérdidas potencialmente devastadoras.

Desde CyberMadrid, consideramos que la extensión de las herramientas de cobertura de riesgos cibernéticos hacia las pymes y autónomos debe ser una prioridad estratégica. Las cifras indican que **más del 60% de las pequeñas empresas que sufren un ataque cibernético cierran en los seis meses posteriores al incidente**. Esto se debe, en gran medida, a la falta de recursos para recuperar operaciones, mitigar impactos reputacionales o afrontar las posibles sanciones regulatorias asociadas.

CyberMadrid, como clúster líder en ciberseguridad en la región de Madrid, fomenta activamente la colaboración entre empresas, instituciones públicas y privadas para impulsar la resiliencia digital. Participamos en la promoción de soluciones accesibles para pymes y autónomos, subrayando la importancia de una cobertura adecuada y de la formación continua en ciberseguridad.

Por tanto vayan por delantes nuestras recomendaciones a las empresas, y en particular a aquellas consideradas Pymes:

- Adoptar ciberseguros como una parte integral de su estrategia de gestión de riesgos. Esto no solo protege frente a pérdidas económicas, sino que también facilita el acceso a expertos en situaciones críticas.

- Fomentar la concienciación y formación en ciberseguridad, ya que muchas brechas de seguridad se originan en errores humanos; la educación puede ser una barrera eficaz contra estas vulnerabilidades.

- Colaborar con clústeres y asociaciones, que permiten compartir experiencias y soluciones, fortaleciendo el ecosistema de seguridad digital.

La digitalización ha transformado profundamente el panorama empresarial, pero también ha traído consigo nuevos desafíos. La guía "Casos prácticos de siniestros cibernéticos" ofrece herramientas clave para comprender y gestionar estos riesgos, mientras que el sector asegurador juega un papel esencial en la construcción de un entorno resiliente y protegido. Desde CyberMadrid, destacamos la necesidad de extender estas soluciones hacia las pymes y autónomos, asegurando que ningún actor quede fuera del círculo de protección.

Tiene pues el lector en sus manos una guía imprescindible para comprender y enfrentar los retos de la ciberseguridad en el entorno empresarial actual. Su enfoque práctico, basado en casos reales, la convierte en un recurso de referencia que trasciende tamaños y sectores, aportando lecciones valiosas tanto para grandes corporaciones como para pymes y autónomos. Cada página refleja el conocimiento acumulado de expertos y profesionales comprometidos con la seguridad digital, ofreciendo herramientas que pueden marcar la diferencia en la gestión de incidentes cibernéticos.

Desde CyberMadrid, queremos felicitar a AGERS y a todas las organizaciones e individuos que han participado en la elaboración de este excelente trabajo. Su esfuerzo y dedicación no solo fortalecen el ecosistema de ciberseguridad, sino que también proporcionan un marco sólido para avanzar hacia un futuro digital más seguro y resiliente. Invitamos a los lectores a explorar esta guía con detenimiento y a aplicarla como una brújula para navegar con éxito por el complejo mundo de los riesgos digitales.

Jorge Hurtado Rojo
Junta Directiva CyberMadrid

1. PRESENTACIÓN

Las encuestas sobre los principales riesgos a los que se enfrentan las organizaciones llevan ya algunos años situando entre los primeros puestos el riesgo cibernético. Se trata de un riesgo que además de preocuparnos exige que nos ocupemos. Y esta es precisamente la razón de ser de una colección de Guías Prácticas que la Comisión de Riesgos Tecnológicos de Agers ha ido publicando desde el año 2017:

- Terminología de ciberseguridad.
- Top 10 Cyber Risks.
- Mapa de Ciber Riesgos.
- Estudio de pólizas de Ciber Riesgos del Mercado Español.
- Buenas prácticas en protección de ciberriesgos (para no expertos).

En esta ocasión hemos querido que el lector de esta guía se ponga en la situación de tener que participar en la gestión de un siniestro cibernético. Para ello hemos vuelto a acudir al método del caso y hemos recogido tres tipos de siniestros:

- Un ataque de ransomware
- Una operación de compra de una sociedad en la que se produce un incidente cibernético.
- Una violación de datos personales.

Los tres casos tienen un gran impacto en las organizaciones, por lo que se producirá una situación de crisis. En ellos hemos recogido cómo se gestiona esta crisis desde su comienzo hasta su finalización. Una de las premisas es que las sociedades atacadas contaban con una póliza de protección de riesgos cibernéticos, que ofrecen por un lado servicios para gestionar la crisis y por otro soportan una parte importante del impacto económico negativo.

Deseamos que ninguno de los lectores tenga que sufrir una situación semejante a las descritas. Pero si no fuese el caso, esperamos que esta guía le aporte un pequeño conocimiento de cómo enfrentarse a esta.

2. AGRADECIMIENTOS

2.1 COMISIÓN DE TRABAJO RIESGOS TECNOLÓGICOS

El Corte Inglés	Juan Gayá **Coordinador - EL CORTE INGLÉS**
	África Sánchez **EL CORTE INGLÉS**
globalvia	Belén Medina **GLOBALVIA**
df	Eva Pérez **DURO FELGUERA**
aena	Álvaro González **AENA**
CEPSA	Juan Miguel García **CEPSA**
	David Martínez **CEPSA**
Sanitas	Ignacio Reclusa **SANITAS**
noatum	Ana Ruiz **NOATUM**
abertis	Juan Ramón Claver **ABERTIS**
ESTEVE	Esther López **ESTEVE PHARMACEUTICALS**
TRANSFESA Logistics	Pedro Morato **TRANSFESA**
MANGO	Raquel Caballero **MANGO**

2.2 EXPERTOS QUE HAN COLABORADO

HOWDEN	Manuel Pérez Martín de la Hinojosa **Head of Cyber, Southern Europe & LatAm HOWDEN GROUP**
wtw	Carmen Segovia **Director FINEX y Ciber riesgos - WTW**
CHUBB	Eloy González **Financial Lines Claims Team Leader and CE Cyber Claims Hub Leader at - CHUBB**
LAZARUS	Manuel Huerta de la Morena **CEO - LAZARUS TECHNOLOGY, S.L.**
	Juan Manuel Martínez Álcala **CTO - LAZARUS TECHNOLOGY, S.L.**
AON	Verónica Jiménez Romero **Director Specialty Cyber Insurance - AON**
	Carlos Bereciartua González **Director Cyber Consulting - AON SPAIN**
	Erick Guillermo Erazo **Cyber Security Consultant - AON**
DARKDATA	Martin Souto **Sales Director - DARKDATA**

3. LOS CASOS

Hemos escogido tres casos, dos de ellos se encuentran entre los más frecuentes y con mayor impacto: un ataque de ransomware (al que se añade el robo de información personal) y otro de robo de información personal. Para el tercero hemos seleccionado un caso en el que el incidente se genera dentro de la organización por parte de un empleado descontento y para complicarlo se produce en el contexto de una operación de compra de una sociedad.

Cada caso comienza con una breve explicación de la empresa objeto del caso. A continuación, se describe que está pasando en la empresa y que pasos se van dando para enfrentarse y solucionar el problema. Téngase en cuenta que con carácter general no vamos a tener una foto clara de lo que está ocurriendo hasta pasado un cierto tiempo, por lo que las primeras decisiones habrá que tomarlas con una información bastante limitada.

Una vez finalizado el siniestro, tendremos una idea clara del impacto económico que ha tenido en la empresa. Esta será la segunda parte de este trabajo, relacionar las distintas partidas que han supuesto un coste para la empresa y determinar, en base a las coberturas habituales de las pólizas de seguro (ver Estudio de pólizas de Ciber Riesgos del Mercado Español), que parte indemnizaría el seguro.

Cada incidente es distinto (incluso aunque fuesen exactamente iguales, las características de cada organización los harán diferentes), por lo que en ningún caso debe tomarse de forma literal ni el desarrollo de los acontecimientos, ni las medidas establecidas para solventarlas, ni la cobertura de las pólizas….

4. PRIMER CASO – ATAQUE DE RANSOMWARE

Descripción de la empresa

La empresa objeto de análisis se dedica a la venta de textil y complementos utilizando tanto tiendas físicas como la web, en ambos medios se presta servicio de atención a clientes.

Cuenta con unos servicios centrales (100 empleados), cuatro almacenes logísticos (50 empleados) y 100 tiendas repartidas entre España y Portugal (12 personas de media por tienda). En total 1.500 empleados.

Dispone de un departamento de diseño, pero la fabricación está externalizada. Sus principales proveedores están en España, Portugal, Marruecos y Turquía. Se trabaja con un nivel de stock que requiere un abastecimiento semanal de productos.

El volumen de facturación es de 300 millones de euros al año. La venta en tienda física supone el 80% de los ingresos y la venta por la web el 20%.

Para el desarrollo de la actividad utilizan herramientas y sistemas de información que soportan los procesos de negocio, destacando:

- ERP (Enterprise Resource Planning). Es el software que contiene el conjunto de aplicaciones dentro del mismo entorno, como ventas, finanzas, producción, compras, marketing, RRHH. Su principal función es dar apoyo a los clientes internos de la empresa.
- WEB. Es el software utilizado para interactuar con los clientes externos no presenciales en el proceso de venta y que estos dispongan de información durante el proceso previo a la entrega.
- Utilidades, como el correo, CRM, etc.

Las aplicaciones que dan soporte al negocio se encuentran en los servidores de la empresa ubicados en sus oficinas centrales. Las tiendas pueden vender sin necesidad de tener conexión con los ordenadores centrales.
Para las aplicaciones complementarias, correo, etc. se utilizan proveedores de servicios.

La empresa no tiene segmentación de redes.

Cada tienda tiene un servidor y de media 4 terminales, en los centros logísticos dos servidores y 20 terminales y en los servicios centrales 10 servidores y 200 terminales. En total 118 servidores y 680 terminales.

Se realizan backups diarios, durante la noche/madrugada, antes y después de la ejecución de los procesos nocturnos, en una ubicación distinta a la de los servidores centrales.

Desarrollo de incidencia

Día 1 – 11:00 h.

El departamento de atención al cliente, de forma general, ha reportado que están fallando los accesos para consultar información de clientes no pudiendo dar servicio en la mayoría de sus gestiones. Se está comunicando a los clientes que llamen más tarde.

Se comunica la incidencia al departamento de TI, que procede a gestionarla.

Día 1 – 12:00 h.

En las tiendas se están produciendo dos incidencias:

- Cuando se cobra la mercancía, la cantidad que figura en el ticket de compra es bastante inferior (de media un 50%) al precio que figura en la etiqueta, incluso después de aplicar los descuentos publicitados (cuando existen)
- Fallan los sistemas que acceden a la información de clientes

Se comunican incidencias al departamento de TI, que proceden a gestionarlas.

Día 1 – 13 h.

Se confirma que no existe ninguna campaña especial, que el sistema no tiene un porcentaje de descuento, pero que los precios que tienen los sistemas (en las tiendas y el sistema central) para los productos no son los que deberían tener.

También se detecta que el fichero de clientes está encriptado, por lo que no se puede dar ningún servicio que requiera la consulta de clientes.

Se comunica la situación al Director General que procede a activar al Comité de Crisis.

Día 1 – 13 h.

En las redes sociales se está pasando la noticia de que la marca está cobrando bastante menos de lo que marcan las etiquetas. Se está produciendo una mayor afluencia a las tiendas que se asocia a esta noticia.

Se valora que respuesta dar en las redes.

Día 1 – 13 h.

Se reúne el Comité de Crisis. Se informa de la situación.

Se desconoce si ambos incidentes (alterar el fichero de precios y encriptar el fichero de clientes) han sido causados por el mismo actor.

IT está trabajando para conocer el alcance.

Se activa la póliza de ciberseguridad. Se solicita el servicio de análisis forense.

Se pide la valoración del impacto de vender por debajo de precio para decidir sobre la suspensión del proceso de venta en tienda física. Se da orden de cerrar la venta online (que ya estaba fallando al no disponer del fichero de clientes).

IT sigue trabajando en el incidente.

Se empieza a trabajar en una primera comunicación para el personal.

Día 1 – 14 h.

Se recibe un correo de un supuesto cibercriminal indicando que han procedido a sustituir el fichero de precios, reduciendo el precio de forma aleatoria entre el 50 y el 80%. Además, han encriptado el fichero de clientes y otros (que no detallan). Para comunicar la clave para desencriptarlo la empresa deberá pagar 1 millón de euros en bitcoins. Dan las instrucciones para realizar el pago. Si este no se realiza en las próximas 24 horas, el precio aumentará un 50% y además procederán a

filtrar los ficheros de clientes que también han extraído. Entregan una muestra con estos datos.

El Comité de Crisis solicita que el seguro haga intervenir a los asesores en ciberextorsión para que analicen el mensaje. En principio, entendiendo que se podrá recuperar la información de los backups no se es partidario de atender el pago.

Se incorpora el DPO al Comité de Crisis.

Se paran y aíslan todos los sistemas para evitar una mayor propagación hasta que se disponga de una evaluación completa.

Se solicita la elaboración de una nueva comunicación para empleados, para clientes (público en general) y para el Consejo de Administración (al que el Director General ya ha informado de la situación de crisis). Se solicita que se realice un especial seguimiento en las redes sociales.

Día 1 – 15 h.

Todos los sistemas están paralizados, por lo que la actividad de la empresa está suspendida.

El personal es informado de que se ha producido un incidente que ha paralizado los sistemas de información, que se está trabajando en este y que se irán comunicando los avances.

Se informa en las redes sociales que se han producido una incidencia que ha paralizado las aplicaciones temporalmente.

Las tiendas continúan abiertas pero solo a los efectos de que los clientes puedan ver la mercancía, incluso reservarla, pero no se puede comprar. En la web aparece un mensaje informando que temporalmente el proceso de compra está suspendido.

Atención al cliente informa a los clientes que pospongan la llamada hasta mañana.

Los equipos de IT y forense están analizando el alcance del incidente. Se están analizando los backups para preparar la futura restauración del sistema.

Los expertos en ciberextorsión están estudiando la información aportada y escuchando en la darkweb noticias sobre el incidente. Se comunican con el ciberdelincuente para solicitar una prueba de vida (que disponen de las claves para desencriptar alguno de los ficheros dañados).

Los expertos en ciberextorsión y el análisis forense determina que ambos ataques (modificación de precios y encriptación de los ficheros) han sido causados por la misma organización.

El DPO está preparando una posible comunicación a la AEPD y a los clientes.

Día 2 – 6 h.

Se detecta que también está cifrado el fichero de proveedores. Esto provocará el rechazo de los pagos a estos, bloquea el proceso de nuevos pedidos y el de la recepción de la mercancía en los almacenes. Se trabaja con stocks bajos en los almacenes, (los pedidos se hacen semanalmente y toca hacer el próximo dentro de dos días) por lo que se podría producir en breve un problema de desabastecimiento.

Se amplía el alcance del análisis forense y de las medidas de recuperación.
Se prepara comunicación del incidente para los proveedores.

En los almacenes se preparan espacios para recoger la mercancía entrante, para retenerla temporalmente hasta que se les pueda asignar, con los sistemas, su ubicación o destino definitivo.

Día 2 – 9 h.

En la investigación del incidente se detecta el origen de la infiltración. El equipo de forensic averigua el vector de entrada. Un usuario de los Servicios Centrales de la empresa recibe un correo de una dirección que a priori piensa que es conocida y lo abre junto con el fichero que se adjunta. Como consecuencia de esto, el sistema se infecta y se encriptan los ficheros

de clientes y proveedores. En los equipos del usuario no existe información crítica, pero sí en los servidores afectados.

En principio, la alteración de precios se debe haber producido en el mismo ataque.

Se verifica que la prueba de vida permite desencriptar ficheros de clientes auxiliares.

Se inicia el proceso de verificación de terminales en las tiendas, que se estima durará 72 horas. Se comienza con las tiendas con mayor venta. Se recupera el fichero de precios y traslada la información a las tiendas. Las tiendas se mantendrán aisladas de los sistemas centrales. Se contratan recursos de TI adicionales para poder reducir el plazo de recuperación de terminales.

Día 2 – 12 h.

La primera tienda física comienza a vender de nuevo. Se ha comunicado a cada tienda el día/hora estimado en que podrá volver a vender.

Los pagos se realizan con merchant (tarjetas de crédito), que son infraestructuras independientes: se puede pagar con tarjeta de crédito pero no se aplican las ventas en las tarjetas de fidelización. Para estos casos, se indica a los clientes que dentro de una semana llamen a atención al cliente para que se les indique como recuperar los beneficios asociados a las compras que están realizando.

Se da prioridad al servidor de venta online, para recuperar la actividad de venta por este canal, o al menos tener disponible el catálogo de productos lo antes posible, aunque para esto sea necesario también de disponer del fichero de clientes operativo.

Día 2 - 12 h.

El Comité de Crisis, en el que está el DPO, sigue valorando hacer la comunicación a la Agencia Española de Protección de Datos. La información aportada por los ciberdelincuentes hace muy probable que se haya producido la filtración, aunque se desconozca la dimensión de esta.

Se gestiona la subcontratación de una infraestructura de servidores en servicios centrales para restaurar la situación en estos hasta que se termine de analizar y limpiar los sistemas infectados.

La sustitución del fichero de clientes generará inconsistencias con el resto del sistema, debido a la diferencia de horas entre el backup y la situación a recuperar.

Día 2 – 14 h.

Se recibe un nuevo correo de los cibercriminales indicando al no haber recibido el pago del rescate, este se incrementa hasta 1,5 millones de euros. Informan que han filtrado 1.000 clientes en la dark web y que seguirán filtrando 1.000 nuevos clientes cada hora hasta que se realice el pago.

Se solicita que se localice en la darkweb si es cierta la amenaza de filtración de datos.

Día 2 – 15 h.

El Comité de Crisis recibe la confirmación de los expertos en ciberextorsión de que el modus operandi se corresponde con una de las grandes organizaciones dedicadas a la ciberdelincuencia. Se ha rastreado la información de clientes en la web y se confirma la filtración.

Se solicitada al DPO que proceda a comunicar a la AEPD la filtración e iniciar el procedimiento para estos casos (CONTINUAR CON EL CASO DE FUGA DE INFORMACIÓN).

Día 2 – 15 h.

Se ha formalizado la contratación de servidores en los que restaurar los sistemas. Se ha verificado que los bakups que se van a utilizar no están afectados.

Día 3 – 9 h.

Llegan los servidores que se utilizarán para reinstalar las aplicaciones.

Se inicia el proceso de reinstalar los sistemas y los datos.

Día 4 – 9 h.

Se han instalado los sistemas y recuperado los datos de los backups. Se inician las pruebas antes de dar de nuevo el servicio.

Se mantienen informadas todas las partes afectadas.

En paralelo, se sigue estudiando en los equipos originales, el impacto del incidente.

Día 4 – 15 h.

Se inicia de nuevo el servicio de forma progresiva, comenzando con la venta online.

Se informa a las partes afectadas.

Se bloquea la descarga de ficheros, salvo autorización de Proceso de Datos.

Día 5 – 9 h.

Todos los sistemas están funcionando de nuevo, aunque se producen incidencias puntuales originadas por el proceso de recuperación.

DÍA 5 – 9 h.

Las zonas de acceso a los almacenes están desbordadas. Se ha contratado personal extraordinario para agilizar el proceso de ubicación de la mercancía en sus estanterías.

Al haberse reducido de forma significativa la venta, no se ha producido un problema de desabastecimiento.

El departamento de atención al cliente ha sido reforzado también para poder regularizar la situación de gestiones extraordinarias lo antes posible.

Se prepara comunicación a los clientes para que puedan ejercer los derechos asociados al programa de fidelización impedidos por el incidente.

Día 10 – 9 h.

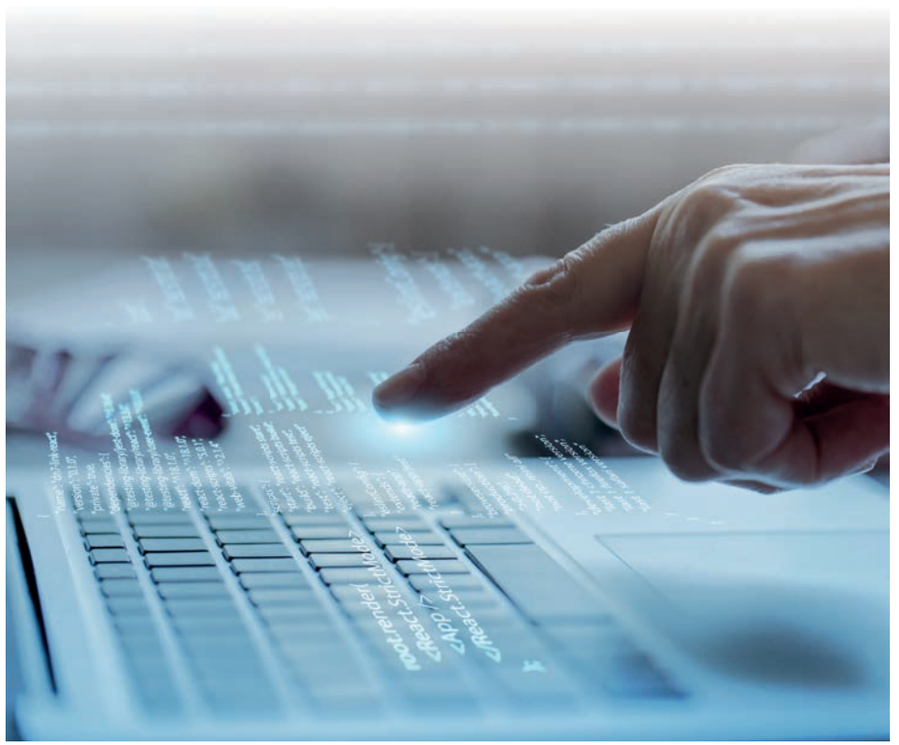
Ha finalizado el análisis forense. Los equipos originales pueden ser de nuevo utilizados, una vez realizadas las tareas de limpieza. Se prepara la transferencia de bases de datos para operar con estos equipos y devolver los alquilados.

El análisis forense concluye con una serie de mejoras en ciberseguridad que dificulten la repetición de este tipo de incidentes.

Día 12 – 9 h.

Los sistemas están operativos en los equipos de la empresa.
Se han instalado las mejoras recomendadas.

Se siguen produciendo incidencias puntuales, pero se considera que se ha recuperado la situación previa al incidente.



Asuntos destacados en la gestión del incidente

1. Puesta a disposición de la empresa/empleados otros equipos para operar cuanto antes y minimizar la pérdida de negocio, así como mantener la operativa (gestión de pedidos para evitar rotura de stocks/ gestión de pagos(nominas).
2. Restauración back up, aplicaciones e información en todos los equipos.
3. Recuperación desde cero en cada equipo de manera independiente.
4. Coordinación del siniestro según protocolo de gestión de incidentes de la aseguradora, integración de equipos internos de IT, legales, comunicación, con peritos, forensic…. Esta coordinación la realizar el Incidence Response Manager (figura establecida en el Plan de Continuidad de Negocio).
5. En el panel de expertos del protocolo a firmar con la aseguradora es recomendable que se valore la inclusión del proveedor de sistemas (que será el que mejor conozca el sistema del asegurado) y DPO del asegurado (si es externo).

Cobertura / valoración de siniestro

Establecer si se trata de uno o dos siniestros es quizás uno de los primeros pasos para confirmar si **estamos ante la aplicación de una o dos franquicias**. En este caso, la definición de siniestros o siniestros interrelacionados nos pueden ayudar a limitar el número de franquicias en un incidente.

Es habitual que la póliza tenga una cobertura de 72 h en la que no se aplica franquicia para gastos asociados al **servicio de respuesta** ante el incidente. Este servicio de respuesta puede incluir forensic, servicios de IT, legal y comunicación. El resto de las coberturas compensan los daños que tiene el asegurado con el abono de una indemnización.

TIPOLOGÍA DEL DAÑO	DESCRIPCIÓN DEL DAÑO	COBERTURA DE LA PÓLIZA	OBSERVACIONES
PÉRDIDA DE BENEFICIOS	Pérdida de ventas (WEB).	Las pólizas cubren habitualmente la pérdida de beneficios consecuencia de la paralización del servicio.	La póliza cubriría la pérdida de beneficios descontando la franquicia temporal, que suele ser de 12 horas.
	Pérdida de ventas (tienda física).	Las pólizas cubren habitualmente la pérdida de beneficios consecuencia de la paralización del servicio.	La póliza cubriría la pérdida de beneficios descontando la franquicia temporal.
	Perdida de ingresos por estar vendiendo con precios erroneos (media un 50% por debajo del precio correcto), consecuencia de la modificación maliciosa en los ficheros de precios.	Las pólizas no cuentan habitualmente con cobertura de pérdida de beneficios consecuencia de manipulación de precios. De forma puntual se puede encontrar la cobertura por manipulación de precios en la página web.	En principio, daño no cubierto.
	Pérdida de negocio a futuro. El siniestro puede suponer una perdida de confianza de los clientes y una mala imagen de la marca (riesgo reputacional).	Tampoco es habitual que se cubra la pérdida de beneficios consecuencia de la pérdida de reputación.	Normalmente estas pérdidas no tienen cobertura aunque si se puede establecer algunas coberturas que reducen la pérdida futura del asegurado como: • Ampliar el periodo indemnizable hasta 90 dias despues de reanudar la operación y estableciendose la reclamación con la comparación de las ventas del año anterior. • Boletos de Goodwill (Se establecen descuentos a los clientes dentro de los 30 dias siguientes al siniestro).
	Perdida de beneficio por rotura de stock.	La paralización de los sistemas ha impedido que se reaprovisionen los almacenes, lo que podría haber provocado perdida de venta por falta de mercancía.	No se llega a producir una rotura de stock.

TIPOLOGÍA DEL DAÑO	DESCRIPCIÓN DEL DAÑO	COBERTURA DE LA PÓLIZA	OBSERVACIONES
EXTRACOSTES	Horas extras personal de TI y ciberseguridad.	Los extracostes dirigidos a reducir la pérdida de beneficios están habitualmente cubiertos en las pólizas ciber. Si el extracoste es superior a la reducción de pérdida, puede limitarse a esta.	
	Contratación de personal para agilizar la actuación sobre los equipos en tienda.	Los extracostes dirigidos a reducir la pérdida de beneficios están habitualmente cubiertos en las pólizas ciber. Si el extracoste es superior a la reducción de pérdida, puede limitarse a esta.	
	Contratación de personal para agilizar la ubicación de la mercancía a la que no se había dado entrada.	En principio, una vez reactivados los sistemas, no se cubriría este coste.	
	Contratación de equipo de refuerzo para gestiones con clientes con incidentes derivados de la paralización de los sistema.	En principio, una vez reactivados los sistemas, no se cubriría este coste.	
	Alquiler y plataformar servidores durante el periodo transitorio para reducir el periodo de paralización de los sistemas.	Los extracostes dirigidos a reducir la pérdida de beneficios están habitualmente cubiertos en las pólizas ciber. Si el extracoste es superior a la reducción de pérdida, puede limitarse a esta.	
SERVICIOS	Analisis forense.	Esta cobertura está incluida en la póliza. Esta cuenta con un panel de proveedores, que serán pagados directemente por la aseguradora.	
	Asesores en Comunicación (especialistas en crisis).	Esta cobertura está incluida en la póliza. Esta cuenta con un panel de proveedores, que serán pagados directemente por la aseguradora.	
	Asesores legares	Esta cobertura está habitualmente incluida en la póliza. Esta cuenta con un panel de proveedores, que serán pagados directemente por la aseguradora.	

TIPOLOGÍA DEL DAÑO	DESCRIPCIÓN DEL DAÑO	COBERTURA DE LA PÓLIZA	OBSERVACIONES
SERVICIOS	Asesores en ciberextorsión.	Esta cobertura está habitualmente incluida en la póliza. Esta cuenta con un panel de proveedores, que serán pagados directamente por la aseguradora.	
RECLAMACIONES DE TERCEROS	Errores en las reservas o retrasos en la recepción de pedidos.	Las pólizas suelen incluir exclusiones por incumplimiento contractual y un de los puntos que se trata en estos siniestros es cual sería el limite entre lo cubierto o no, o si se trata de incumplimiento extracontractual o contractual del asegurado.	No se cubren las penalizaciones comerciales dentro de un contrato. En caso de una reclamación de tercero, se activa lo primero gastos de defensa y tambien estaría cubierto los daños y perjuicios del tercero.
OTROS	Pago de rescate.	Si la empresa hubiese optado por pagar un rescate, podría tener cobertura dependiendo de la póliza.	Las compañias aseguradoras establecen controles previos al pago de la extorsión , entre otros, confirmar que el ciber delincuente no se encuentre en la lista OFAC. (https://ofac.treasury.gov/faqs/topic/1616). Es cobertura de reembolso que decide el asegurado y la regulación de posible sanción tambien le afecta al asegurado.
	Acciones en medios para limitar el daño reputacional.	El coste de las acciones para reducir el daño reputacional causado por el cliente están habitualmente cubiertos por la póliza.	
PROTECCIÓN DE DATOS	La información sobre estos gastos la encontrará en caso de Fuga de información.		

NOTA: Al importe total de la cantidad soportada por el seguro hay que restar el importe de la franquicia.

Al importe total de la cantidad soportada por el seguro hay que restar la franquicia correspondiente.

Algunas estimaciones relativas a la valoración del siniestro:

- La venta online ha estado paralizada 3 días y 4 horas. La media diaria es de 164.000 euros (20% de la venta diaria). El coste estimado es de 518.2040 euros. Si el coste del producto es del 50%, la pérdida de beneficios alcanza los 259.120 euros.
- La venta física ha estado paralizada completamente durante 9 horas y de forma parcial (las tiendas se iban abriendo según se replataformaban los terminales) durante 3 días más. Como se daba prioridad a las tiendas de mayor venta, las pérdidas se estiman en el 40%. El coste estimado es de 492.000 (cierre total) + 787.000 (cierre parcial) = 1.297.200. Si el coste de la mercancía es del 50%, el impacto habrá sido de 639.600.
- La venta diaria media es de 820.000 euros. Si se han reducido los precios un 50%, la pérdida de ingresos es de 410.00 euros. La venta OL no funciona al no estar operativo el fichero de clientes, que supone el 20% de las ventas, por lo que la pérdida alcanza los 328.000 euros. El sistema ha estado funcionando 4h sobre las 12 horas de apertura, por lo que el impacto ha sido de 82.000 euros.
- Personal interno de TI entre 90-420 €/h.
- Los costes técnicos internos de levantar las plataformas (400 terminales y 100 servidores) serían de 5 a 8 jornadas con un coste hora de 90€.
- Diseñar la estrategia de comunicación en redes sociales entre 10/30 mil €.
- Asesoría legal 10/15 mil €.
- Coste de gestión de siniestro (incident manager, forense y técnico) de 140 €a 230 €.
- Gestión de la ciberextorsion sería aproximadamente 7.500 $.
- Cupón goodwill con un precio unitario por boleto 10 a 20 € con un límite máximo entre 0.5 a 1 M€.

Lecciones aprendidas / Conclusiones

- Es muy importante para reducir el tiempo de gestión de la crisis disponer de un Plan de Continuidad de Negocio,
- Conocer el vector de entrada es determinante para limitar el impacto del siniestro y permitir que la empresa pueda volver a operar normalmente.
- Se recomienda informar del incidente lo antes posible, normalmente los asegurados activan la póliza en el momento que el incidente impacta en el negocio pero la recomendación sería activar lo antes posible.
- Establecer un protocolo consensuado con la aseguradora y que este protocolo se haya comunicado internamente va a permitir que cada responsable conozca cada uno de los pasos a seguir. Adicionalmente, la recomendación sería que este protocolo forme parte del plan de continuidad de negocio.
- Selección adecuada de Incidence Response Manager. Esta persona debe integrar los servicios de la aseguradora y aquellos designados por el asegurado. La recomendación sería que se establezca a priori y quede reflejado en un protocolo a utilizar en caso de siniestro El protocolo incluye el panel de expertos, con al menos, el asesor jurídico, el de sistemas y el de comunicación.

  El incidente es transversal en la empresa, no sólo debiera estar involucrado TI, es recomendable que estén integradas otras áreas y definidas dentro del protocolo de gestión.
- Otra recomendación sería revisar algunas definiciones de pólizas que nos van a permitir que la gestión del siniestro sea más sencilla:

  - Siniestro y siniestros interrelacionados
  - Definición perdida de beneficios, margen bruto o costes, periodo indemnizable. El periodo indemnizable está habitualmente en el rango de 120 - 180 días. Se recomienda incluir en la definición de periodo de indemnización aquel necesario para volver a tener el mismo nivel de operación.
  - La falta de stock también puede impactar en la cobertura de perdida de beneficio.
- Otras coberturas a tener en cuenta:

- Ciertas mejoras de activos, aún con ciertos límites
- Las coberturas de los proveedores del asegurado.
- Cobertura relativas a la parte de protección de datos (reclamaciones, sanciones agencia…).

- Por otra parte, la comunicación a terceros debe ser clara y transparente y realizarse a tiempo para evitar perder la confianza de los clientes (riesgo reputacional).
- Recomendaciones técnicas en TI, utilización de redes segmentadas, EDR (Endpoint Detection Response).

La gestión por fuga de información se trata en el caso 3.

5. SEGUNDO CASO – INCIDENTE EN OPERACIÓN DE M&A

Descripción de la empresa

Global Transportation Ltd. (GlobTrans) es una empresa de transportes con sede en EEUU y presencia internacional, que cuenta con 10.000 empleados y una cifra de negocios superior a los 5.000.000.000 de euros.

Para el desarrollo de su actividad, utilizan herramientas y sistemas de información que les ayudan a gestionar y optimizar sus operaciones de transporte y logística. Algunos de sus sistemas son:

- **ERP (Enterprise Resource Planning)**: Es un software de información que contiene un conjunto de aplicaciones dentro de un mismo entorno, como ventas, finanzas, producción, compras, marketing, recursos humanos, etc. Su función principal es dar apoyo a los clientes internos de la empresa.
- **Sistemas de seguimiento de envíos**: Estos sistemas permiten a las empresas realizar un seguimiento de sus envíos en tiempo real. Estos sistemas proporcionan información sobre la ubicación de los envíos, el estado de los mismos y los tiempos de entrega estimados. Este sistema en concreto es de vital importancia para la operativa de la empresa, ya que la comunicación con los transportistas se hace a través del mismo.
- **Sistemas de gestión de flotas**: Estos sistemas ayudan a las empresas a gestionar sus flotas de vehículos y a optimizar sus operaciones de transporte. Estos sistemas permiten a las empresas realizar un seguimiento de sus vehículos, programar su mantenimiento y gestionar sus rutas.

GlobTrans está planeando adquirir Orient Transports Ltd. (OrienTrans), una empresa de transportes local en Jordania con un volumen de negocios de alrededor de 40 millones de euros.

La adquisición de esta empresa es una compra estratégica para GlobTrans, ya que necesita expandir su presencia en la región para dar servicio en la misma a sus principales clientes. Además, esta compra le proporcionará acceso a una base de clientes más amplia y una entrada en el mercado del transporte de mercancías en Oriente Medio.

Sin embargo, la adquisición de la empresa local presenta desafíos significativos. GlobTrans deberá considerar cuidadosamente los riesgos asociados con la adquisición, incluyendo los riesgos políticos, económicos y culturales.

Para realizar una adquisición exitosa, GlobTrans deberá realizar una Due Diligence (DD) exhaustiva en las áreas Técnica/Operativa, Legal, Financiera e Impuestos.

Descripción de la operación de M&A

La operación de adquisición de OrienTrans por parte de GlobTrans se realiza en dos fases. En la primera, mucho más breve que la siguiente, el equipo de M&A de la empresa compradora se pone en contacto con el CEO y propietario de la compañía objetivo para valorar el potencial de la operación. Los primeros contactos son favorables y se realiza un primer análisis de la información inicial facilitada por la dirección. Tras confirmar el interés por ambas partes se inicia la segunda fase en la que se trabaja en la realización de diferentes procesos de DD completos.

Al tratarse de una operación que GlobTrans considera menor, no se implica en el proceso de DD a la dirección de la empresa, que normalmente se implica completamente en estos procesos trasladando la conciencia en ciberseguridad de la compañía. Se definen como áreas de DD prioritarias (aquellas realizadas por asesores externos) únicamente las tradicionales (Técnica/Operativa, Legal, Financiera e Impuestos) y se realizan DDs internas en las áreas de Riesgos y Seguros, ESG y Ciberseguridad.

A solicitud del vendedor, que quiere liberarse de responsabilidades tras la venta, se realiza una póliza de Warranty and Indemnity (W&I) sobre el contrato de compraventa, que cubre las pérdidas patrimoniales sufridas por el comprador como consecuencia de hechos no detectados en el proceso de compra que supongan un incumplimiento de las manifestaciones otorgadas por el vendedor. El comprador contrata esta póliza con base en las condiciones habituales de mercado. Los aseguradores basan su suscripción en las DD llevadas a cabo por los asesores externos del comprador. Si bien es cierto que hace unos años los aseguradores no aceptaban DD llevadas a cabo internamente por el comprador, hoy en día los aseguradores pueden aceptarlo siempre que obtengan confort del equipo interno que las lleve a cabo.

Una vez realizadas las DD correspondientes GlobTrans confirma que la operación es viable y, tras llegar a un acuerdo en el precio de la operación, se firma un contrato de compraventa (Signing) que se considera muy satisfactorio y se inicia el proceso de obtención de autorizaciones para poder terminar cerrando la operación (Closing) en un plazo menor a 4 meses.

Desarrollo de la incidencia y Gestión del incidente

Para realizar las labores propias de la DD interna, GlobTrans involucra, entre otros departamentos, al área de tecnología, infraestructura y ciberseguridad de OrienTrans. Algunos de los empleados de OrienTrans que comienzan a participar en el proceso muestran su intranquilidad con la noticia de la posible adquisición. En especial, uno de ellos - encargado de las labores internas de pentesting entre otras – no está de acuerdo con la asociación de ambas empresas, ya que tiene la creencia de que el objeto de la misma es el uso de su actual compañía para el transporte de mercancías de dudosa ética en un territorio tan convulso como es Oriente Medio.

Dado su carácter hacktivista, así como su capacidad técnica para poner a prueba la seguridad de sistemas y redes, está dispuesto a boicotear la operación con el despliegue de un wiperware en la empresa compradora. Este tipo de malware se caracteriza por tener la capacidad de dañar o destruir información en sistemas informáticos.

El empleado inicia conversaciones con uno de los técnicos de la empresa compradora con el que trabaja en un ejercicio de auto-evaluación. Durante estas conversaciones, en las que el empleado utiliza información deshonesta para las respuestas de esta evaluación y obtiene a su vez información para precisar un posterior mapeo de la red de la entidad. Una vez se produce el Signing de la operación de compra de OrienTrans el 31 de enero, el empleado comienza a acometer las primeras acciones que desencadenarán el posterior ataque, el cual pasa a describirse cronológicamente a continuación:

Días previos al incidente:

En los días anteriores al origen de la incidencia, el empleado llevó a cabo el anteriormente descrito mapeo de la red de la empresa compradora, utilizando herramientas como Nmap y Nessus para identificar servidores, dispositivos y puntos de acceso críticos en la red de GlobTrans. Combinando estas herramientas y la capacidad de monitorizar el tráfico de la red, lanza escaneos de puertos e identifica servicios y vulnerabilidades, como software desactualizado o configuraciones débiles en los sistemas objetivo.

El técnico de la empresa compradora que realizaba el ejercicio con el empleado de OrienTrans reporta que, dentro de las labores de integración, se informa a este último de la existencia de copias de seguridad offline y offsite.

14 de febrero:

- 03:00h: Se detectan los primeros problemas en la operación normal de GlobTrans. Algunos transportistas desaparecen del sistema de seguimiento de envíos, y los incidentes se consideran como fallos de comunicaciones.
- 05:30h: La incidencia parece agravarse, y el sistema de seguimiento de envíos deja de funcionar, lo que supone la pérdida de la situación de todos los transportes y la capacidad de GlobTrans para gestionar nuevos envíos. También se pierde la información de los envíos en tránsito.
- 05:43h: El personal de operaciones contacta telefónicamente con el CISO de la entidad para informarle de la incidencia detectada.
- 08:00h: Se convoca al equipo de gestión de crisis para valorar el impacto del incidente.

Durante ese día, el equipo técnico intenta la recuperación de la entidad por sus propios medios.

15 de febrero:

- 09:00h: El equipo de ciberseguridad inicia la investigación del incidente con la ayuda de un forense. Detectan la presencia del wiperware Shamoon en el sistema de gestión de envíos.

  Shamoon es conocido en la región de Oriente Medio por sus amplias capacidades para el borrado de datos. Entre otros, está diseñado para sobrescribir datos de los discos duros de los equipos infectados, lo que complica e incluso imposibilita la recuperación de datos en los mismos.
- 10:30h: Tras confirmar la presencia de Shamoon se confirma la naturaleza maliciosa del ataque. Comienza la evaluación de la extensión del daño y la identificación del vector de entrada.

16 de febrero:

- 08:00h: El equipo de ciberseguridad identifica el equipo del empleado de OrienTrans como posible paciente cero del ataque a través de análisis de logs y tráfico de red. El empleado procede al borrado de huella digital y a una colaboración activa en la recuperación del incidente para evitar sospechas hacia una posible posición maliciosa. También se determina que el *Shamoon* había sido introducido en el sistema semanas antes, y que estaba configurado para permanecer latente durante un periodo prolongado antes de su activación, permitiendo que el malware se propague y se copie en los sistemas de respaldo – que conocía existían - antes del inicio del ataque.
- 10:00h: Se informa a la dirección de GlobTrans de que el incidente puede tener su origen en la empresa comprada y se convoca a una reunión a los líderes de los distintos grupos de trabajo implicados en la transacción.
- 11:00h: Se realiza la reunión para valorar el impacto del incidente en la operación, incluyendo un posible desistimiento de la misma. Tras analizar el Acuerdo de Compraventa (SPA) se observa que, al no haber sufrido impacto alguno la empresa comprada, no existe ninguna cláusula que permita una salida limpia para GlobTrans. Adicionalmente, se confirma que se mantiene la viabilidad financiera de la operación al no verse OrienTrans afectada en el ataque. Como única medida a tomar se establece la paralización de cualquier contacto entre ambas empresas y se prohíbe a los equipos de operaciones la continuación de los trabajos de integración.
- 12:00h: Se inicia el contacto con las autoridades y se notifica oficialmente el incidente a las partes involucradas.

17 de febrero:

- 07:00h: GlobTrans, junto con expertos forenses externos, realiza una auditoría exhaustiva de la red para identificar la presencia de otros posibles malwares y vulnerabilidades.
- 15:00h: Se implementan medidas de contención para evitar la propagación adicional del wiperware y se desconectan sistemas críticos.

20 de febrero:

- 10:00h: El equipo de respuesta a incidentes de GlobTrans inicia la remediación, eliminando el wiperware de los sistemas afectados.
- 18:00h: Se inicia la restauración de los sistemas desde las copias de seguridad no afectadas por el malware. Lamentablemente, las copias más recientes habían sido afectadas por la presencia continuada del wiperware, por lo que el punto de recuperación objetivo deberá ser anterior a lo esperado.

25 de febrero:

- 09:00h: Se completa la restauración de datos críticos y se inicia la validación de la integridad de los sistemas.
- 16:00h: GlobTrans emite un comunicado público sobre el incidente, informando a clientes, socios y partes interesadas sobre las acciones tomadas y las medidas implementadas.

1 de marzo:

- 09:00h: Se reanudan parcialmente las operaciones normales de GlobTrans, mientras un buen número de empleados trabajan en labores de continuidad, ante la falta de actualización de los datos obtenidos en las últimas copias limpias disponibles. Se intensifican las medidas de seguridad y se implementan nuevas políticas para prevenir futuros incidentes.

La estrategia de boicot del empleado consigue que la empresa compradora sufra pérdidas millonarias por semanas de inactividad o actividad parcial. La víctima, aunque dispone de un plan de respuesta a incidentes, no lo tiene diseñado para una actuación rápida ni tampoco está probado en simulacro. Con cierto retraso y varias pruebas de copias infectadas – lo que beneficia la propagación del wiperware a nivel global – acaban por acceder a la recuperación de sus datos por copias de varias semanas atrás (no afectadas por el malware) y procede a la restauración manual de los datos restantes hasta la fecha. Sin embargo, estas pérdidas no han conseguido poner en jaque la operación de compra al no afectar a la viabilidad del proyecto.

El empleado, satisfecho con el resultado de su acción, espera al desistimiento de la operación y guarda un "as en la manga" por si este no se produce finalmente. Es consciente de que, en caso de seguir adelante, se procederá a la integración de ambas empresas y entonces tendrá incluso un acceso mayor a sus sistemas target para un nuevo ataque, lo que podría afectar a ambas empresas y causar daños adicionales a GlobTrans.

Análisis de cobertura

Cobertura de la póliza de la empresa compradora (GlobTrans):

#	COBERTURA	¿SE PUEDE ACTIVAR BAJO ESTE SINIESTRO?	DETALLES
1	Gastos de Asesoramiento y Consultoría		A continuación
	1.1 Gastos forenses:	Si	GlobTrans contacta con la compañía para solicitar los servicios de un experto forense para determinar la causa y gravedad del incidente, así como revisar el sistema en busca de otros malware o vulnerabilidades.
	1.2 Asesoramiento Legal	Si	Aunque el forense no confirmase la ocurrencia de una brecha de datos, se activa la garantía para realizar una sesión informativa sobre posibles responsabilidades con terceros afectados.
	1.3. Asesoramiento Técnico / Consultoría	Si	Los servicios informáticos de respuesta fueron igualmente consultados para la recomendación de medidas de restauración y mejoras de la seguridad que serían necesarias para mitigar nuevos incidentes de seguridad.

#	COBERTURA	¿SE PUEDE ACTIVAR BAJO ESTE SINIESTRO?	DETALLES
1	Gastos de Asesoramiento y Consultoría		A continuación
	1.4 Asesoramiento Reputacional	Si	Con el fin de evitar los efectos que una publicidad negativa pueda tener sobre la reputación de la empresa, y que eso suponga una pérdida de clientes actuales o falta de confianza en nuevos clientes, se activó esta cobertura, la cual pone a disposición del asegurado expertos en relaciones públicas que le ayuden a realizar las campañas o acciones publicitarias necesarias para minimizar el daño reputacional, incluyendo el coste de las mismas.
2	Daños y Costes Propios		A continuación
	2.1 Gastos de Restauración	Si	También tendrían cobertura por la póliza todos los costes en los que incurriera la empresa para restablecer la funcionalidad de los sistemas, permitiendo la puesta en marcha nuevamente de la actividad empresarial.
	2.2 Gastos de Mejora	Si	Con el fin de mejorar la seguridad de cara a futuros incidentes, se utiliza esta cobertura, que suele presentarse sublimitada, para resolver vulnerabilidades. También se restaura un sistema para la detección de vulnerabilidades obsoleto que ha sido dañado, sustituyéndolo por una versión superior.
	2.3 Pérdida de Beneficio	Si	Como consecuencia de la paralización de la actividad, se produce una diferencia significativa con el beneficio esperado, por lo que se activa la cobertura de pérdida de beneficios para contrarrestar esa diferencia en la cuenta de resultados. Asimismo, la compañía se hace cargo de todos los gastos que se hayan generado para agilizar la vuelta a la normalidad de la actividad de la empresa, así como el incremento de costes de operación.

#	COBERTURA	¿SE PUEDE ACTIVAR BAJO ESTE SINIESTRO?	DETALLES
2	Gastos de Asesoramiento y Consultoría		A continuación
	2.4. Extorsión Cibernética	No	Al no existir petición de rescate y entenderse el incidente como un acceso no autorizado con el consecuente impacto, aunque la póliza tuviese esta cobertura, no se activa esta cláusula de la póliza.
3	Responsabilidad con terceros		A continuación
	3.1. Responsabilidad por Privacidad	No	No se detecta ninguna exfiltración de información, por lo que no se espera activar esta cobertura.
	3.2. Responsabilidad Cibernética	No	No se detecta ningún perjuicio a terceros como resultado del uso no autorizado de la red, por lo que no es espera activar esta cobertura.
	3.3. Responsabilidad Multimedia	No	No aplicable por no estar relacionada con el siniestro
	3.4. Regulación / Sanciones	No	No se detecta ninguna exfiltración de información, por lo que no se esperan posibles investigaciones y/o sanciones administrativas.
	3.5. Costes de Notificación	No	Cobertura que tampoco aplicaría, ya que está orientada a las notificaciones obligatorias por Ley en un caso de violación de datos personales.
4	Posibles exclusiones aplicables		A continuación
	4.1 Responsabilidad Contractual		Aunque es posible que haya contratos que tengan una penalización por el retraso en la entrega, los afectados deberán demostrar ese daño para poder activar la cobertura, que no amparará las cantidades contractuales acordadas entre ambas partes, ya que la responsabilidad civil contractual suele estar excluida.
	4.2. Deshonestidad de Empleados		El empleado de OrienTrans aún no se entiende como empleado de la empresa compradora, por lo que no se entiende esta cláusula como aplicable.

Cobertura de la póliza de la empresa vendedora (OrienTrans):

En caso de demostrarse que ha sido un empleado de la empresa comprada el responsable del ataque, OrienTrans podría ser reclamada por GlobTrans por los daños causados a través de la garantía de responsabilidad con terceros, si bien la aseguradora podría aplicar la exclusión de dolo.

#	COBERTURA	¿SE PUEDE ACTIVAR BAJO ESTE SINIESTRO?	DETALLES
3	Responsabilidad con terceros		A continuación
	3.1. Responsabilidad Cibernética	No	• **Gastos forenses** – Aunque es una cobertura pensada principalmente para daños propios, entendemos que se podría activar en este caso, con el fin de que un experto informático pudiera determinar las causas del incidente y poder utilizar esa información en una mejor defensa del asegurado. • **Gastos de mitigación de reclamaciones –** En este caso, no se esperan reclamaciones de perjudicados particulares por lo que, al haberse recibido ya la reclamación del perjudicado principal, es una garantía que no tendría sentido activar. • **Gastos de asesoramiento legal –** En este incidente no interviene ningún regulador ni existen unas obligaciones legales específicas, más allá de las propias del contrato de compraventa, por lo que entendemos que no se activaría esta cobertura. • **Daños reclamados –** OrienTrans recibe reclamación de GlobTrans por los perjuicios sufridos por la paralización de su actividad y le reclama tanto la pérdida de beneficios como los costes en los que ha tenido que incurrir para restaurar el sistema y reanudar la actividad. • **Gastos de defensa –** Se activa la cobertura de Gastos de Defensa, en los que la aseguradora pondrá a disposición del asegurado su panel de expertos en la defensa jurídica de sus intereses, haciéndose cargo de la posible investigación, respuesta, defensa y/o apelación.

#	COBERTURA	¿SE PUEDE ACTIVAR BAJO ESTE SINIESTRO?	DETALLES
4	Posibles exclusiones aplicables		A continuación
	4.1 Responsabilidad Contractual		En este caso, como el siniestro no ha ocurrido durante la actividad normal de la empresa si no durante una operación de compra, la penalización derivaría del contrato de compra-venta y entraría en juego la póliza de W&I.
	4.2. Deshonestidad de Empleados		El hecho que ha generado el incidente es un acto deliberado, criminal y deshonesto de un empleado. No obstante, ¿no sería la empresa responsable subsidiaria por la actuación de su empleado? En estos casos, se debe revisar la póliza aplicable, ya que esta exclusión presenta diferencias de redacción. Algunas cláusulas "separan" al empleado de la compañía asegurada, otras hacen excepciones con los empleados, pero no con puestos directivos. En este caso, la redacción de esta cláusula puede ser definitiva.

Cobertura póliza W&I de la operación

- Hechos que activan la póliza: La póliza de W&I da cobertura a toda pérdida de valor de la empresa comprada, derivada de un hecho desconocido que suponga un incumplimiento de las manifestaciones dadas por el vendedor al comprador bajo el contrato de compraventa. Para determinar si habría cobertura bajo la póliza de W&I, serían relevantes los siguientes elementos:

  - Que exista una manifestación del vendedor bajo el contrato de compraventa que fuese incorrecta a fecha de firma por traer causa de un hecho anterior a la fecha de firma (acciones del empleado). Por ejemplo "Ningún empleado ha realizado ninguna acción que pueda comprometer la ciberseguridad de la compañía".
  - Que el incumplimiento de esta manifestación (i.e. que en la fecha de firma un empleado haya realizado trabajos encaminados a

realizar un ataque de ciberseguridad) genere un daño al comprador (vía daño a la compañía).

- Que sea un hecho desconocido para el comprador a fecha de firma (que no esté en su conocimiento ni esté revelado en las Due Diligence).

La póliza de W&I entra en vigor en la fecha de la firma dando cobertura a los hechos que son desconocidos en firma y se manifiestan después (incumplimiento de manifestación por hechos ocurridos antes de firma). Sin embargo, en las operaciones de compra-venta con signing y closing diferido, también podrían cubrirse daños derivados de un incumplimiento de las manifestaciones del vendedor por hechos ocurridos después de firma que se descubran después de closing.

Quedarían excluidos los daños derivados de hechos ocurridos después de firma que se descubran antes de closing (hechos ocurridos y descubiertos en el periodo interino).

En este caso, el "grueso" del ataque ocurre después de firma y el comprador tiene conocimiento después de firma. Por tanto, se podría buscar cobertura sobre la base de lo ocurrido antes de firma (es decir, los trabajos preparatorios del empleado llevados a cabo antes de firma), pero no sobre lo ocurrido después de la misma.

- Cobertura de ciberseguridad: En general, los hechos cibernéticos constituyen una exclusión estándar de las pólizas de W&I en las que este riesgo sea material. Normalmente, se puede eliminar esta exclusión y dar cobertura sujeto a una revisión satisfactoria en materia de ciberseguridad, que puede combinar una revisión técnica, así como una DD de seguros. Normalmente, los aseguradores requieren que los informes estén realizados por asesores externos, pero es posible negociar cobertura sobre la base de informes internos, siempre que obtengan confort del equipo interno que lleve a cabo la revisión.
- Pérdida: Si se determina que existe un daño indemnizable bajo la póliza de W&I, la empresa comprada podría tener que soportar gastos por responsabilidades de cualquier tipo, demandas, multas, costes reputacionales u otros, o podría sufrir una disminución en su

valor que tendría que soportar el comprador, que es quién contrata normalmente la póliza. El daño indemnizable bajo la póliza de W&I suele incluir el importe del daño derivado del incumplimiento (no se incluyen daños morales o reputacionales), así como la pérdida de beneficios (lucro cesante) derivada del hecho que causó el daño.

- Cobertura en exceso: las Pólizas de W&I dan cobertura en exceso de otras pólizas más específicas. En este caso, una vez agotado el límite de cobertura de la póliza de ciberseguridad, si la póliza de W&I da cobertura de acuerdo con los supuestos explicados más arriba, se activaría la cobertura de W&I en exceso de la póliza de ciber.
- Costes de defensa o procesales: La póliza de W&I incluye cobertura de gastos de defensa y gastos procesales. En el caso que nos ocupa entendemos que la póliza ciber cubriría estos costes y, en exceso, como hemos explicado antes, cubriría la póliza de W&I.

Lecciones aprendidas / Conclusiones

Tras el desarrollo del caso se considera importante resaltar las siguientes cuestiones:

- La importancia de la realización de una Ciber DD, útil herramienta que permite detectar riesgos durante la operación de compraventa. Para la realización de esta DD se recomienda el uso de herramientas inside/out que analicen en tiempo real la empresa objetivo de la transacción.
- Se recomienda que esta Ciber DD sea realizada por asesores externos, aunque, poniéndolo de manifiesto al principio del proceso, el bróker de M&A puede negociar con los aseguradores que acepten una DD interna. Tras este paso previo, el seguro de W&I podría ofrecer cobertura siempre que sea en exceso de una póliza de ciberriesgos en vigor y en el proceso de DD de seguros se confirme que dicha póliza cumple con unos determinados estándares de cobertura y adaptación conforme al riesgo de la entidad.
- Más allá del desarrollo de planes de respuesta, estos deben estar correctamente diseñados y ser probados regularmente. Ésta es la manera más eficiente de garantizar que, en caso de siniestro, van a funcionar como se espera.

- En las operaciones de compraventa de empresas el componente humano es un riesgo importante. En este tipo de procesos se debe poner atención especial en limitar la visibilidad que tienen de la empresa compradora los empleados de la empresa comprada y, en general, no es una buena praxis el iniciar los trabajos de integración de ambas empresas antes del cierre de la operación. De cualquier forma, si se realizan trabajos cruzados entre empresas, la monitorización de los accesos se convierte en un elemento crucial a la hora de evitar problemas como el que nos ocupa.
- Revisar la póliza con especial atención a la consideración de empleado dentro de la misma, ya que las ciberamenazas no solo provienen del exterior, sino también desde el interior de la propia compañía. Uno de los aspectos importantes a considerar al contratar pólizas de ciberriesgo es la definición de "empleado". Este detalle puede ser determinante en la cobertura de un siniestro en casos de actos deshonestos perpetrados por miembros de la organización.

  La amenaza interna, o insider threat, se está volviendo cada vez más común y sofisticada, y hace que los empleados actúen en coalición con atacantes externos, facilitando su acceso a los sistemas corporativos. Este fenómeno ha venido creciendo por las iniciativas de bounties, donde incluso se ofrece a los empleados una parte del botín a cambio de acceder a los sistemas con sus credenciales o a través de sus sesiones.

  La gran mayoría de las pólizas Cyber incluyen exclusiones específicas para actos deshonestos. Una definición desacertada de "empleado" puede resultar en la denegación de cobertura en casos donde un miembro de la entidad esté involucrado en actividades fraudulentas o deshonestas.
- Negociar con el asegurador la cláusula de "Cambio de Control". Otra cláusula común en las pólizas de ciberriesgo, así como en otros ramos, es la de "Cambio de Control", por la cual el asegurador puede dejar sin efecto la cobertura del contrato en caso de que la empresa tomadora cambie su órgano de gestión y/o propiedad, con algunos detalles a aplicar según la póliza. Como antes se mencionaba, es importante destacar que la póliza de W&I actuaría en exceso de la póliza de ciberriesgos de la entidad adquirida, pero, ya que ésta cambia de gestión, podríamos sufrir un escenario en el cual el asegurador rehúse la cobertura de un siniestro refiriéndose a esta cláusula, dejando igualmente sin efecto la póliza de W&I en exceso.

6. TERCER CASO – FILTRACIÓN DE DATOS

Descripción del negocio

Descripción del Negocio

Entertainment Suites Hotels* (de ahora en adelante ESH) es un líder global en entretenimiento familiar, enfocado en crear y brindar experiencias inmersivas y memorables para millones de huéspedes. ESH generó ingresos de €1.423 millones para el año 20xx, y su EBITDA subyacente fue de €450 millones. Al Q4 de 20xx, ESH operaba más de 100 atracciones en 12 países en cuatro continentes, y en ese mismo año, ESH dio la bienvenida a 10 millones de huéspedes y aproximadamente 48 millones de visitantes a sus atracciones. ESH es uno de los mayores operadores de atracciones para visitantes y parques temáticos de Europa. ESH también ha sido líder del mercado en el Reino Unido y Alemania por número total de visitantes, con una presencia ya significativa y creciente en los Estados Unidos y la región de Asia Pacífico.

Operatividad e Interconexión

Esta cartera única de marcas y activos valiosos entrelazados, cada uno de los cuales posee una sólida herencia dentro de sus mercados originales, además de ser globalmente escalable y respaldado por su amplia experiencia técnica y creativa. El modelo operativo de ESH consiste en una combinación de funciones internas y subcontratadas. El equipo de gestión interna proporciona las funciones corporativas, financieras, de adquisiciones, de recursos humanos y gestión de riesgos, de TI, de facturación y de atención al cliente. El mantenimiento y respaldo del sistema informático son gestionados a nivel global a través de un equipo de TI y algunas funciones tecnológicas son subcontratadas a terceros.

Proceso de Reservas

El área de reservaciones se encarga de efectuar las reservas y venta de habitaciones de cada establecimiento, así como la gestión de las actividades recreativas y de esparcimiento de los diferentes hoteles. También esta área es responsable de aplicar las políticas del hotel referentes a su geografía, y de elaborar los reportes e información que se deben proporcionar a otros departamentos y a su jefe inmediato superior. Este proceso se inicia a través de una plataforma de registro global la cual lleva el control de los depósitos a cuenta, reembolsos, comisiones, descuentos, etc.

Datos de la plataforma de reserva y facturación

- La información requerida en la plataforma para una exitosa reserva incluye nombre del hotel, fecha de llegada y salida, nombre y apellidos del huésped o huéspedes, número de identificación, número de teléfono, correo electrónico, tarifa y cantidad de depósito entre otros datos.
- La facturación se hace a través de una pasarela de pago que entra en funcionamiento una vez ingresados los datos de tarjetas de crédito/debito en la plataforma hotelera.

Antecedentes del incidente

Incidente

El 15 de febrero el equipo de Global de TI de ESH detectó en sus sistemas de información archivos cifrados de forma masiva lo que podía indicar la infección con un malware de tipo Ransomware. El equipo de Respuesta ante Incidente empezó de inmediato con la contención y recuperación de la infraestructura de la compañía, activando la ciberpóliza y contactando al equipo destinado para realizar un análisis en profundidad y ayudar en las tareas de investigación, contención, erradicación y recuperación sobre la infraestructura de ESH.

En base a la información proporcionada por el cliente, el impacto sobre la infraestructura de ESH fue de 94 servidores en 4 países y de 114 equipos de usuario. A partir de la nota de rescate, se identificó el grupo de cibercriminales que realizó el ataque, conocido como BlackCat Ransomware. En base a las fuentes de inteligencia de los investigadores se pudo constatar que el grupo BlackCat empezó a operar en octubre del año anteriory que utilizan un método de doble extorsión, exfiltrando datos confidenciales, cifrándolos y extorsionar a sus víctimas para recibir un rescate. Al ser conocido que este grupo de cibercriminales exfiltraba datos confidenciales, se estableció un equipo de Vigilancia Digital para detectar exfiltraciones de datos en Dark Net, Deep Web y foros “underground” utilizados por los cibercriminales para traficar con información robada. En la nota de rescate, establecían un periodo de tiempo para la realización de un pago en bitcoins el cual si no era cumplido se verían en la necesidad de publicar información personal de huéspedes incluidos sus datos de tarjetas de crédito.

El equipo de investigación analizó distintas evidencias para esclarecer cual fue el acceso inicial y como se produjo el ataque. En base a las evidencias analizadas se pudo concluir que los atacantes accedieron por primera vez el día 22/10 del año anterior utilizando una vulnerabilidad no conocida tipo “Zero Day” en unos de los sistemas utilizados para el acceso remoto a servidores, aunque no fue hasta el día 12/02 que realizaron movimien-

tos laterales hacía uno de los equipos de "procesamiento de datos" ubicado en una de las ciudades clave de almacenamiento de datos y procedieron a desplegar diferentes herramientas de reconocimiento en este equipo, que permitieron al atacante realizar el descubrimiento de la red, de usuarios, y demás información importante para realizar el ataque de tipo Ransomware.

Una vez los atacantes obtuvieron la información necesaria sobre cómo estaba estructurada la red de ESH, fueron pivotando entre distintos equipos con credenciales válidas hasta conseguir acceso a diferentes servidores, dando como resultado el cifrado de los sistemas durante el día 14/02.

Respuesta ante incidente cibernético

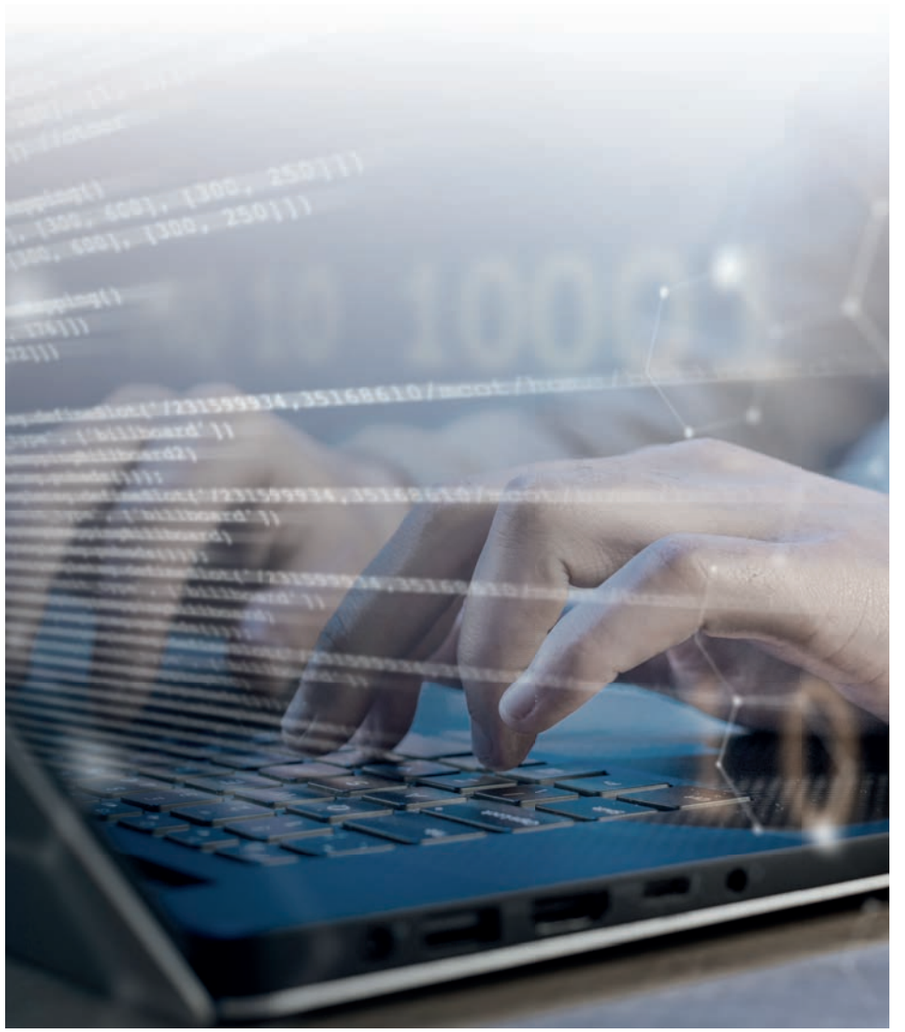
Identificación

El principal objetivo del equipo de investigación durante un incidente cibernético de este tipo es poder reconstruir la cadena de ataque utilizada con el fin de poder apoyar tanto a la identificación como contención del incidente, apoyando también durante este proceso tanto a la defensa activa de la compañía como en la recuperación de los sistemas afectados.

Las actividades identificadas durante este proceso incluyeron las siguientes:

- Apoyo en la respuesta ante el incidente, generando documentación y procedimientos en base a buenas prácticas, así como asesoramiento técnico durante todo el proceso.
- Identificar al grupo/atacante, así como identificar y analizar las diferentes herramientas o malwares utilizados durante el incidente.
- Identificar tipología de ataque, así como vectores de entradas utilizados.
- Identificar técnicas, tácticas y procedimientos utilizados por el atacante.

- Identificar cuentas comprometidas, herramientas o malware utilizado por el atacante.
- Identificar dispositivos afectados, así como cuentas de usuarios comprometidas.
- Identificar las evidencias que puedan sugerir la fuga de información.
- Apoyar en la defensa activa de la compañía proporcionado IOCs e información de contexto para la creación de reglas de detección.



IDENTIFICACIÓN DE INCIDENTE				
DETECCIÓN INICIAL	**Monitorizar**: Utilizar herramientas de monitoreo de seguridad (SIEM, IDS/IPS) para detectar actividades inusuales en la red o sistemas.	**MUY ALTA**	IT	Software de Monitoreo de Seguridad: Splunk, AlienVault, IBM QRadar.
	Alertas de Seguridad: Prestar atención a las alertas de seguridad emitidas por software antivirus, soluciones EDR (Endpoint Detection and Response) o plataformas de monitoreo de redes.	**MUY ALTA**	IT	
	Notificaciones de Usuarios: Estar atento a los informes de usuarios sobre comportamientos extraños en sus equipos, como archivos inaccesibles, mensajes emergentes de ransomware, o rendimiento inusualmente lento.	**ALTA**	IT	
RECOLECCIÓN DE INFORMACIÓN INICIAL	**Capturar Mensajes de Ransomware**: Documentar y capturar imágenes de cualquier mensaje de rescate que aparezca en las pantallas de los sistemas afectados.	**MUY ALTA**	IT	
	Registro de Sintomatología: Anotar todos los síntomas observados, como archivos cifrados con nuevas extensiones, cambios en nombres de archivos, o archivos de texto/HTML que contienen las notas de rescate.	**ALTA**	IT	
	Identificación de Patrones: Buscar patrones en la extensión de archivos o nombres de archivo alterados que puedan indicar un tipo específico de ransomware.	**ALTA**	IT	
ANÁLISIS INICIAL DE LA AMENAZA	**Verificar el Alcance del Impacto**: Determinar cuántos y cuáles sistemas están afectados, y si el ransomware se está propagando.	**MUY ALTA**	IT	
	Examinar los Archivos Afectados: Analizar los archivos cifrados para identificar la extensión añadida, que a menudo puede dar pistas sobre la familia de ransomware.	**MUY ALTA**	IT	
	Revisión de Logs: Examinar los registros de eventos de los sistemas afectados para identificar la actividad sospechosa que precedió al cifrado.	**MUY ALTA**	IT	

IDENTIFICACIÓN DE INCIDENTE				
CONFIRMACIÓN DEL INCIDENTE	**Análisis de Herramientas de Seguridad**: Utilizar herramientas de análisis de malware para confirmar la presencia del ransomware en los sistemas afectados.	**ALTA**	IT	Soluciones de Respuesta a Incidentes: CrowdStrike, Carbon Black, FireEye.
	Consulta con Fuentes de Inteligencia: Comparar las notas de rescate, extensiones de archivos y patrones de cifrado con bases de datos de inteligencia de amenazas (como ID Ransomware) para identificar el tipo específico de ransomware.	**ALTA**	IT	Plataformas de Inteligencia de Amenazas: ID Ransomware, VirusTotal.
AISLAMIENTO DEL INCIDENTE	**Desconexión de la Red**: Aislar los sistemas afectados de la red para prevenir la propagación del ransomware a otros dispositivos.	**MUY ALTA**	IT	
	Deshabilitar Servicios Comprometidos: Detener cualquier servicio o proceso que esté relacionado con la propagación del ransomware.	**MUY ALTA**	IT	
NOTIFICACIÓN Y ESCALAMIENTO	**Desconexión de la Red**: Aislar los sistemas afectados de la red para prevenir la propagación del ransomware a otros dispositivos.	**MUY ALTA**	IT	
	Comunicación a la Dirección: Mantener informada a la alta dirección sobre el incidente y las acciones que se están tomando.	**MUY ALTA**	IT	
INVESTIGACIÓN DETALLADA	**Análisis Forense**: Iniciar un análisis forense completo de los sistemas afectados para comprender cómo se introdujo el ransomware y cómo se propagó.	**MUY ALTA**	IT	Herramientas de Análisis Forense: EnCase, FTK (Forensic Toolkit), Autopsy.
	Revisión de Logs y Tráfico de Red: Analizar los logs de eventos de seguridad y el tráfico de red para identificar los vectores de ataque y cualquier comunicación con los servidores de comando y control (C2).	**MUY ALTA**	IT	
DOCUMENTACIÓN Y REGISTRO DEL INCIDENTE	**Registrar Todo el Proceso**: Documentar detalladamente cada paso tomado desde la detección inicial hasta la confirmación del incidente.	**ALTA**	IT	
	Mantenimiento de Evidencias: Asegurar la conservación de todas las evidencias digitales para futuros análisis o posibles procedimientos legales.	**ALTA**	IT	

IDENTIFICACIÓN DE INCIDENTE				
EVALUACIÓN DE IMPACTO	**Evaluar los Datos Comprometidos**: Determinar qué datos han sido cifrados o comprometidos y evaluar el impacto en las operaciones de negocio.	**MUY ALTA**	IT	**MUY ALTA**
	Priorizar la Recuperación: Identificar los sistemas y datos críticos que necesitan ser recuperados primero.	**ALTA**	IT	

Restauración del sistema

Una de las necesidades inmediatas a este tipo de eventos es la continuidad de la actividad y por supuesto el soporte es el sistema, la restauración del mismo implicaría las siguientes acciones en este caso:

RESTAURACIÓN DE SISTEMAS		
ACCIONES		**IMPORTANCIA**
ACCIONES GENERALES	**ACCIONES ESPECÍFICAS (el líder y área principal involucrada IT)**	
Verificar la Autenticidad de la Herramienta de Desencriptación	**Evaluar los Datos Comprometidos**: Determinar qué datos han sido cifrados o comprometidos y evaluar el impacto en las operaciones de negocio.	**MUY ALTA**
	Validar con Expertos: Consultar con especialistas en ciberseguridad para confirmar la autenticidad y seguridad de la herramienta.	**ALTA**
Realizar una Copia de Seguridad de los Datos	**Copiar los Datos Cifrados**: Hacer una copia de seguridad de todos los datos cifrados antes de iniciar el proceso de desencriptación. Esto es crucial en caso de que algo falle durante el proceso de desencriptación.	**MUY ALTA**
	Documentar Todo: Registrar qué archivos estaban cifrados y su estado antes de la desencriptación.	**ALTA**

RESTAURACIÓN DE SISTEMAS		
ACCIONES		**IMPORTANCIA**
ACCIONES GENERALES	**ACCIONES ESPECÍFICAS (el líder y área principal involucrada IT)**	
Ejecutar la Herramienta de Desencriptación en un Entorno Seguro	**Utilizar un Entorno Aislado**: Ejecutar la herramienta en un sistema aislado, preferiblemente en una máquina virtual o un equipo separado, para minimizar el riesgo de que la herramienta contenga malware.	**ALTA**
	Supervisar el Proceso: Observar el proceso de desencriptación cuidadosamente para detectar cualquier comportamiento anómalo.	**ALTA**
Verificar la Integridad de los Datos Desencriptados	**Comprobar los Archivos Recuperados**: Asegurarse de que los archivos desencriptados estén completos y no corruptos. Comparar con copias de seguridad previas, si están disponibles.	**ALTA**
	Realizar Pruebas: Ejecutar aplicaciones y archivos desencriptados para confirmar que funcionan correctamente.	**ALTA**
Analizar y Limpiar el Sistema	**Escaneo Completo**: Realizar un escaneo completo del sistema con herramientas de seguridad para asegurarse de que no quedan rastros del ransomware u otras amenazas.	**ALTA**
	Eliminar Software Inseguro: Borrar cualquier software o archivo relacionado con los atacantes una vez confirmada la recuperación de los datos.	**ALTA**
Reforzar la Seguridad	**Actualizar Software y Sistemas**: Instalar las últimas actualizaciones de software y parches de seguridad.	**MUY ALTA**
	Cambiar Credenciales: Cambiar todas las contraseñas y credenciales del sistema para prevenir futuros accesos no autorizados.	**MUY ALTA**
	Revisar Políticas de Seguridad: Evaluar y mejorar las políticas de seguridad existentes para evitar incidentes similares en el futuro.	**ALTA**

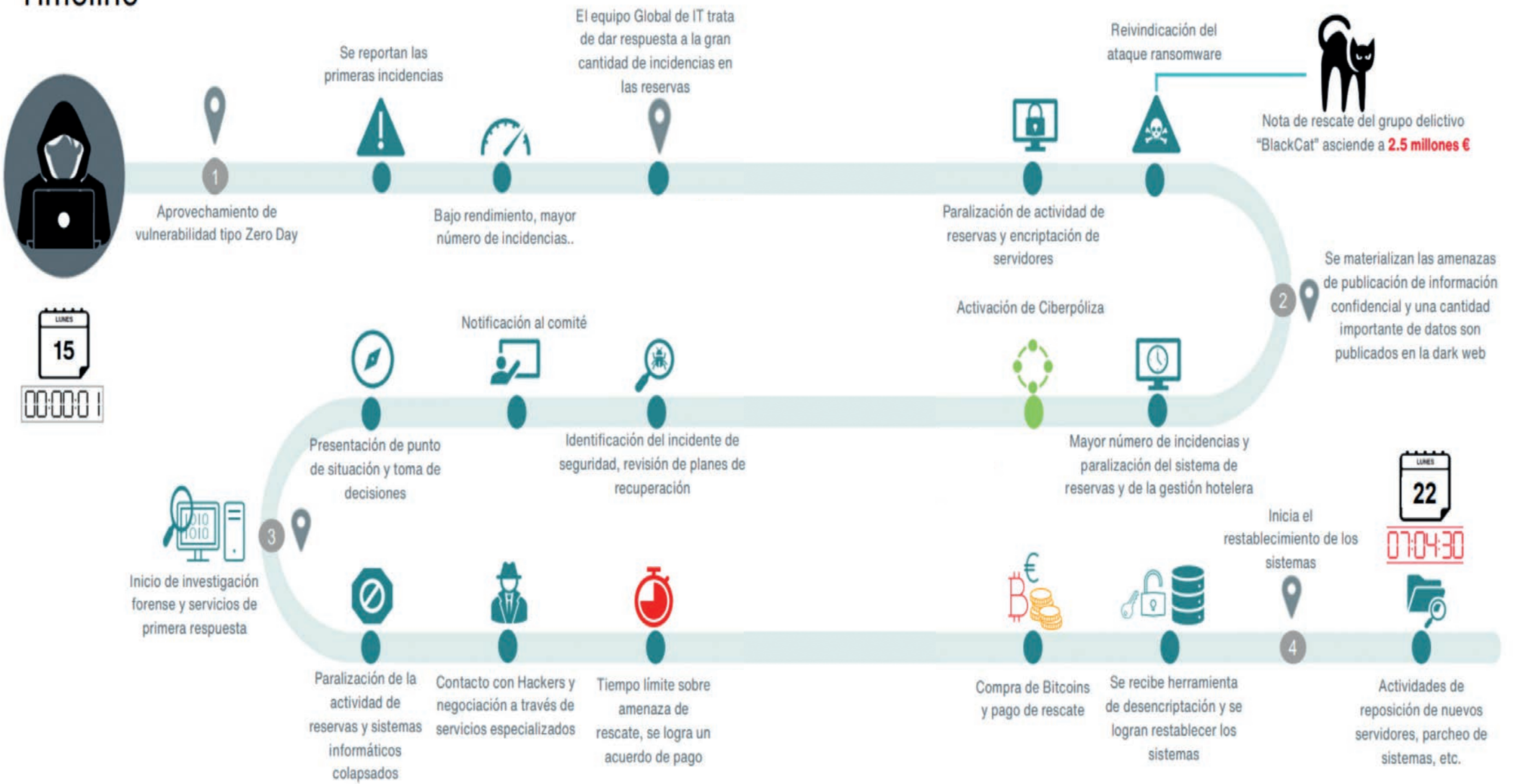
RESTAURACIÓN DE SISTEMAS		
ACCIONES		**IMPORTANCIA**
ACCIONES GENERALES	**ACCIONES ESPECÍFICAS (el líder y área principal involucrada IT)**	
Evaluar el Impacto y Tomar Medidas Legales	**Documentar el Incidente**: Registrar todos los detalles del ataque, incluyendo cómo ocurrió y cómo se manejó.	**ALTA**
	Consultar con Abogados: Evaluar las obligaciones legales y considerar involucrar a las autoridades o cumplir con requisitos de notificación según la legislación.	**MEDIA**
Evaluar el Impacto y Tomar Medidas Legales	**Investigar el Ataque**: Llevar a cabo un análisis forense para comprender cómo se produjo el ataque y qué vulnerabilidades fueron explotadas.	**MUY ALTA**
	Recopilar Evidencias: Recopilar toda la información posible que pueda ser útil para futuras investigaciones o medidas legales.	**ALTA**
Revisar y Mejorar Planes de Respuesta a Incidentes	**Actualizar Procedimientos**: Revisar los procedimientos de respuesta a incidentes y actualizar el plan para incluir las lecciones aprendidas.	**ALTA**
	Capacitar al Personal: Asegurarse de que todo el personal esté capacitado en las mejores prácticas de seguridad y en el manejo de incidentes.	**ALTA**
Considerar la Asistencia de Expertos en Recuperación	**Contratar Profesionales**: Si es posible, trabajar con expertos en recuperación de ransomware que puedan ayudar a navegar el proceso de recuperación de manera segura y eficiente.	**ALTA**

Toma de decisiones

Con la plataforma de reservas sin funcionar, fue evidente para los clientes que había una paralización general y empezaron a publicar en redes sociales su crispación. Se procedió a realizar un comunicado público sobre la situación que atravesaban. El ataque fue más grave de lo que se había anticipado y generó un daño reputacional significativo para la compañía. Además de la encriptación de sistemas, se descubrió que se había exfiltrado una cantidad importante de información personal incluyendo número de tarjetas de crédito que fue puesta a la venta en uno de los foros de la dark web.

La preocupación por la pérdida de más información valiosa y la inoperatividad de los sistemas informáticos supuso un gran contratiempo para la organización, por lo que se optó por la única posibilidad de recuperar los datos, y restituir los sistemas, esto significó el pago del rescate. Con esta acción, se iniciaron las labores de recuperación y restablecimiento de sistemas a través de una herramienta para la desencriptación provista por los atacantes.

Timeline


Se reportan las primeras incidencias
El equipo Global de IT trata de dar respuesta a la gran cantidad de incidencias en las reservas
Reivindicación del ataque ransomware
Nota de rescate del grupo delictivo "BlackCat" asciende a 2.5 millones €
1
Aprovechamiento de vulnerabilidad tipo Zero Day
Bajo rendimiento, mayor número de incidencias..
Paralización de actividad de reservas y encriptación de servidores
2
Se materializan las amenazas de publicación de información confidencial y una cantidad importante de datos son publicados en la dark web
Activación de Ciberpóliza
LUNES
15
Notificación al comité
Presentación de punto de situación y toma de decisiones
Identificación del incidente de seguridad, revisión de planes de recuperación
Mayor número de incidencias y paralización del sistema de reservas y de la gestión hotelera
Inicia el restablecimiento de los sistemas
LUNES
22
07:04:30
3
Inicio de investigación forense y servicios de primera respuesta
Paralización de la actividad de reservas y sistemas informáticos colapsados
Contacto con Hackers y negociación a través de servicios especializados
Tiempo límite sobre amenaza de rescate, se logra un acuerdo de pago
Compra de Bitcoins y pago de rescate
Se recibe herramienta de desencriptación y se logran restablecer los sistemas
4
Actividades de reposición de nuevos servidores, parcheo de sistemas, etc.

Valoración y Coberturas

TIPOLOGÍA DEL DAÑO	DESCRIPCIÓN DEL DAÑO	COBERTURA DE LA PÓLIZA
Bajada de rendimiento desde el DIA-1	Pérdida de confianza de los clientes Pérdida de volumen de ventas.	* La pérdida de cuota de mercado no está cubierta * Se cubriría la pérdida de beneficios y los gastos incurridos para remediar la bajada de rendimiento.
Paralización de actividad de reservas	Pérdida de confianza de los clientes Pérdida de volumen de ventas	* La pérdida de cuota de mercado no está cubierta * Se cubriría la pérdida de beneficios y los gastos incurridos para remediar la bajada de rendimiento. * El impacto reputacional como caida del valor de la marca o de precio de la acción no tendría cobertura, sí la tendrían los gastos de gestión de la crisis (RRPP).
Cifrado de sistemas de información	Gastos de especialistas informáticos para solventar el cifrado. Posible necesidad de adquirir equipos nuevos. Posible necesidad de adquirir software nuevo (nuevas licencias).	* Gastos de especialistas estarían cubiertos * Gastos de nuevo hardware no estaría cubierto por ser un daño material, salvo que este coste repercutiera en una reducción de la pérdida de beneficio superior * Gastos en licencias o nuevo software podría tener cobertura si no se considera una mejora.
Datos publicados en la Dark Web - DÍA-2	Posibles reclamaciones por vulneración de privacidad y reglamento protección de datos. Posible violación de propiedad intelectual. Posibles incumplimientos detectados por los regularos a causa del incidente fuera del alcance de este.	* Reclamaciones y sanciones del organismo competente estarían cubiertas, siempre que la legislación aplicable lo permita y se hayan cumplido los plazos y requerimientos de notificación. No se contemplan sanciones de los reguladores por incumplimientos revelelados por el incidente fuera del alcance de este (Ej.: No cifrado de datos de carácter personal, usos de licencias de software que infringen los derechos de autor, etc.) * Gastos de notificación de la brecha de privacidad según legislación vigente tendrían cobertura. * La violación de propiedad intelectual no estaría cubierta en una póliza ciber al uso (requiere un producto específico).
Inicio de investigación forense y servicios de primera respuesta	Gasto especialistas informaticos, de RRPP y Legales	Los gastos de los especialistas están cubiertos.
Pago rescate	Pago de en criptomoneda a los cibercriminales	Si la póliza cuenta con esta cobertura, el pago del rescate estaria cubierto siempre que se haga acorde a las directrices marcadas por la aseguradora (con un experto definido por la aseguradora).
Interrupción de comunicación, parada de producción	Pérdida confianza de los clientes Pérdida de volumen de ventas Posible fuga de información, delitos contra los datos	La pérdida de cuota de mercado Perdida de beneficios, gastos incurridos Medidas de comunicación por la fuga de info Pérdida de beneficio
Daño en los servidores	Daños económicos por inutilización de los sistemas de información. Inversión en nuevos equipos, CPD, tecnología, etc.	Coste económico de la restitución de los servicios exclusivamente.

Esta guía, elaborada por la Comisión de Riesgos Tecnológicos de AGERS, se centra en proporcionar pautas prácticas para la gestión de riesgos cibernéticos. Destaca la importancia de abordar el ciberriesgo desde una perspectiva integral, que incluye prevención, detección, respuesta y recuperación. Subraya que la transferencia del riesgo al mercado asegurador es viable solo si se implementan medidas adecuadas de ciberseguridad, y detalla las expectativas de las aseguradoras sobre políticas de gestión y cultura organizacional relacionadas con la ciberseguridad.

Se propone un modelo basado en las etapas del marco NIST (identificación, protección, detección, respuesta y recuperación) adaptado a las necesidades empresariales. Cada etapa describe medidas específicas, desde la gestión de activos y el establecimiento de políticas de seguridad, hasta la implementación de sistemas de monitorización y simulacros de respuesta ante incidentes. También incluye herramientas para garantizar la seguridad de los datos, como la autenticación multifactor, segmentación de redes y uso de sistemas de copia de seguridad.

La guía concluye enfatizando que la ciberseguridad no solo es responsabilidad de los departamentos técnicos, sino que requiere un enfoque interdisciplinario con el apoyo de toda la organización, incluyendo la alta dirección. También subraya la importancia de la formación continua y el cumplimiento normativo para minimizar los riesgos y garantizar la continuidad operativa ante ciberataques o incidentes tecnológicos.

agers