Aprendizajes para el contexto empresarial ante ciberataques por *ransomware*: el caso del *Colonial Pipeline*

Fuente: Shred-it.com (2021)

Por Raquel Jorge Ricart[1]

Dirigido a la Fundación ESYS

[1] Raquel Jorge Ricart es especialista asesora en gobernanza y política tecnológica y digital, desde la perspectiva de estrategia e incidencia. Fulbright Fellow en la Elliott School of International Affairs (GWU) en Washington, DC, Estados Unidos, ha trabajado en el *Berkman Klein Center for Internet & Society* en la Universidad de Harvard, así como en una firma de consultoría del Reino Unido encargada de la realización de informes de prospectiva para gobiernos organizaciones multilaterales. Forma parte de la lista "35 Under 35" de Líderes Emergentes de Europa por Banco Santander-CIDOB.
Contacto: raqueljorgericart@hotmail.com

CONTENIDO

1. Problemática

El ciberataque al *Colonial Pipeline*, uno de los oleoductos más largos de Estados Unidos, que transporta alrededor de tres millones de barriles de combustible al día a través de 8,850 kilómetros de Houston a Nueva York, se ha considerado el ataque por *ransomware* más importante de la Historia. También representa el primer caso en que se recupera el pago realizado por una empresa víctima de un ataque informático producido por *ransomware*, aunque la recuperación haya sido parcial.

Sin embargo, el caso del *Colonial Pipeline* muestra una serie de retos, deficiencias y "vacíos" que abren serios **debates acerca de la gestión organizativa** y la **protección cibernética de una infraestructura crítica** tan esencial como esta, así como las **deficiencias en las modalidades de respuesta a crisis cibernéticas** y la **naturaleza de colaboración público-privada** en eventos como el que ocurrió en los días 6 y 7 de mayo de 2021.

Este informe presenta **factores relevantes a tener en cuenta** a la hora de abordar una situación similar a la ocurrida con el *Colonial Pipeline* **por parte de una empresa del sector privado**, cuya sostenibilidad y continuidad dependen de su **madurez cibernética en el contexto empresarial**, su organización, sus sistemas y sus servicios.

2. Antecedentes del *Colonial Pipeline* y el escenario del ciberataque

El *Colonial Pipeline* da servicio a la mayoría de los estados del Sur de Estados Unidos y tiene ramificaciones desde la costa Este hasta el interior en estados como Tennessee. Actualmente, el oleoducto, de naturaleza privada, pertenece a Royal Dutch Shell, Koch Industries, así como a varias firmas de inversión estadounidenses y de origen extranjero.

La criticidad del *Colonial Pipeline* es elevada, ya que la mayoría de los aeropuertos del este de Estados Unidos depende en su mayoría del combustible de este oleoducto. Los aviones precisan recargar suficiente suministro por períodos de cuatro a cinco días de operación. El ciberataque se produjo en un contexto de preocupación sobre la vulnerabilidad cibernética de las infraestructuras críticas, tras el ataque *SolarWinds* de 2020, que consiguió acceder a bases de datos y sistemas mediante *spyware* (software malicioso para espiar y recolectar información una vez se accede al sistema) de agencias gubernamentales, como el Pentágono, el Departamento de Seguridad Nacional, el Departamento de Estado, el Departamento del Tesoro y de una cantidad elevada de usuarios individuales cuyos datos residían en los sistemas de compañías como Microsoft o Intel, entre otras.

A diferencia de *SolarWinds*, que supuso la entrada silenciosa de un *spyware* al software Orion de la compañía, el ciberataque al *Colonial Pipeline* no fue un *spyware*, sino un *ransomware*, desplegado por la red Darkside. En el caso *SolarWinds*, a partir de una actualización del software Orion, y el envío a sus clientes (unos 33,000 aproximadamente), el spyware accedió a una gran cantidad de sistemas de entidades, entre ellas agencias gubernamentales y del sector privado. El spyware continuó recopilando información hasta

ser descubierto. Sin embargo, en el caso *Colonial Pipeline*, el ataque buscaba robar datos del sistema del oleoducto para, posteriormente, exigir un pago por su rescate para desbloquear el sistema. El 6 de mayo de 2021 se produjo el robo de datos, y al día siguiente, 7 de mayo, se produjo el ataque de *malware* pidiendo el rescate.

Colonial pagó a la red *Darkside* el rescate. Sin embargo, antes de que *Darkside* desbloqueara el sistema, el Departamento de Defensa pudo interceptar parte del rescate pagado: alrededor de unos 2,3 millones de dólares en bitcoins se recuperaron del total de 4,4 millones de dólares. Este escenario representa el primer caso en que se recupera el pago realizado por una empresa víctima de un ataque informático producido por *ransomware*.

Las actuaciones del *Colonial Pipeline* permitieron desbloquear el sistema, recuperar la normalidad y minimizar los daños. Sin embargo, se pueden identificar deficiencias, errores y algunos "vacíos", que imposibilitaron que la respuesta fuera más efectiva y más cohesionada. De este caso surgen aprendizajes que no pueden dejarse pasar, y que se presentan a continuación.

3. ¿Deben pagarse los rescates? La trampa del *ransomware* para las empresas

De acuerdo con el informe *Cyberason Global Ransomware Study* publicado por *Cybersecurity Ventures* (2021), y que estima el impacto financiero y reputacional de los ciberataques en los negocios, el 80% de las empresas que pagaron por un rescate producido por *ransomware* fueron atacadas de nuevo, y casi la mitad de estas fueron atacadas por el mismo grupo de ciberdelincuentes.

Es cierto que la forma de abordar un ciberataque por *ransomware* es complejo y costoso. Más aún cuando los ciberataques a nivel general ocurren cada 11 segundos de media, y en concreto las pérdidas causadas por *ransomware* en Estados Unidos, por dar un dato específico, aumentaron en un 225% solo en el año 2020.

De media, las empresas víctimas de esta modalidad sufren un impacto significativo en sus negocios. Aproximadamente, el 66% de las compañías pierden ingresos, el 53% sufre daños reputacionales y de marca, el 29% reduce su plantilla a causa de dichas pérdidas, y el 25% de las firmas ha cerrado su negocio tras el ataque.

Cuando se produjo el ataque al *Colonial Pipeline*, surgió un debate importante acerca de si es necesario pagar rescates para poder recuperar rápidamente el sistema, o si no hay que ceder ante este tipo de presiones y esperar a dar una contraofensiva cibernética. En este debate, también entraba el rol gubernamental: ¿debe intervenir el gobierno? ¿solo en situaciones de crisis, o debería tener mayor presencia incluso en períodos de estabilidad?

En esta cuestión, el problema no es que, por pagar un rescate, se incentiva el volver a atacar a la misma empresa, dado que el grupo de ciberatacantes asumirá que es probable

que la entidad vuelva a ceder ante el cibersecuestro. **Uno de los problemas principales es que la empresa víctima no abandona la "lista de objetivos" de las personas que acceden a redes y emiten ataques de *ransomware*.** La lista de objetivos se comportaría de forma similar a la lista Robinson de llamadas o correos comerciales abusivos.

Los ciberdelincuentes tienen extensas listas de correos electrónicos para acceder a sistemas de entidades y rara vez eliminan nombres, independientemente de que ya hayan realizado un ciberataque *ransomware*. Esto plantea cuestiones sobre el grado de concienciación y cultura de ciberseguridad en la Alta Dirección de las empresas, más allá de la figura del CISO (*Chief Information Security Officer*). También plantea cuestiones sobre la coordinación, comunicación e intercambio de información público-privada ante escenarios como este que, quizás no han ocurrido todavía, pero frente a los cuales hay que estar preparado y disponer de protocolos comunes para afrontarlo.

4. Modelos de gestión ante un ataque *ransomware*: entre lo público y lo privado

Algunos sectores apuestan por la autogestión, como es el caso de las asociaciones bancarias privadas más importantes de los países de América Latina y el Caribe, quienes encuentran en FELABAN (la Federación Latinoamericana de Bancos, una institución privada sin ánimo de lucro) el punto de referencia para poder intercambiar información de forma inmediata y rápida ante ciberataques significativos producidos por fraude (FELABAN, 2021).

Este modelo consiste en que, cuando una asociación bancaria miembro ha sido víctima de un ciberataque, recurre a la "ventanilla única" de FELABAN para enviar información anonimizada. Esta información es automáticamente compartida con el resto de los miembros a través de la plataforma *Fraud Information Control.* De esta forma se incrementa y garantiza la seguridad cibernética de sus socios, emitiendo alertas de puntos rojos, ataques de tarjeta no presente, ataques en punto de materialización y tendencias latentes en materia de ciberseguridad.

Esta modalidad es de naturaleza privada, de carácter intra-sectorial (solamente dentro de las asociaciones bancarias grandes de los países de la región), garantiza el anonimato, y funciona con rapidez ante escenarios de crisis.

El sector gubernamental no participa, lo cual plantea retos acerca de cómo promover la colaboración público-privada ante situaciones graves como la del *Colonial Pipeline*, o cómo generar confianza entre ambos sectores en escenarios sin crisis. Siempre debe tenerse en cuenta la dependencia que hay, no solamente entre entidades de un mismo sector, sino también de varios sectores al mismo tiempo, dentro de una misma cadena de valor.

Mientras que esta primera opción, caracterizada por la autogestión, garantiza efectividad e inmediatez ante situaciones de crisis, pero no tanto en escenarios regulares, **una segunda opción es la de la coordinación por parte del sector público**. El caso del *U.S. CISA* (la Agencia de Seguridad de las Infraestructuras y Ciberseguridad), componente operativo del

Departamento de *Homeland Security*, es reseñable. Si bien no ha creado un Grupo de Trabajo –como sí ha hecho con la higiene cibernética-, sí publicó en septiembre de 2020 la primera guía (*NEW Ransomware Guide*) que incluye las mejores prácticas de la industria y una lista de verificación de respuestas personalizadas que sirve como apéndice específico sobre *ransomware* para incorporar esta perspectiva como un protocolo único y diferenciado dentro los planes de respuesta a incidentes cibernéticos de la compañía (U.S. CISA, 2021). Esta guía –operativa y orientada a crisis- es fruto del trabajo del U.S. CISA así como del MS-ISAC (*Multi-State Information Sharing and Analysis Center*). A él le acompañan campañas específicas, una de ellas desplegada en enero de 2012 con el fin de reducir el riesgo de *ransomware*, que se orientaba a crear esfuerzos coordinados y sostenidos en el tiempo entre las organizaciones del sector público y privado.

En el contexto de esta crisis, el 9 de mayo –dos días después de desplegar el ataque-, el presidente Joe Biden declaraba el estado de emergencia y eliminaba las limitaciones de transporte de combustible por carreterera. Los Secretarios de Estado de Transporte –Pete Buttigieg- y de Energía –Jennifer Granholm- anunciaban soluciones frente al acaparamiento de combustible por parte de la ciudadanía, reiterando que Estados Unidos sufría una parada de suministro pero no un escenario de escasez de gasolina.

Pese a esta coordinación en el ámbito del combustible, lo cierto es que hubo críticas en lo que se refiere al lado del ciberataque. Tras el *ransomware*, se reveló en una audiencia del Subcomité de Ciberseguridad del Comité de Servicios Armados del Senado de Estados Unidos que el Departamento de Seguridad Nacional no había sido alertado del ataque de *ransomware*, ni tampoco el Departamento de Justicia había sido informado sobre el pago del rescate, lo que provocó un tenso debate sobre la limitada capacidad de recopilación de información por parte del gobierno y las dificultades para compartir datos entre los sectores público y privado.

Pese a todo, el 7 de junio el Departamento de Justicia anunciaba que había recuperado 63,7 de los 75 bitcoins del pago de rescate a través de trabajo del FBI. El valor era solo de 2’3 millones de dólares del total de 4’4 millones, en gran parte debido a una caída progresiva en el valor de mercado del bitcoin desde la fecha de pago del rescate.

Lo cierto es que ninguno de los dos modelos anteriormente citados en materia de gestión de *ransomware* tiene resultados totalmente efectivos. Cada uno tiene sus ventajas y sus deficiencias. Sin embargo, un modelo híbrido –coordinación pública en la gestión con descentralización ejecutiva en lo privado- podría dar lugar a un modelo más efectivo para escenarios de crisis, como fue el caso del *Colonial Pipeline*.

En lo que respecta al grado de actuación de una compañía dentro de su propio contexto empresarial, la solución más efectiva, temprana y de largo plazo es la de incorporar en su arquitectura institucional una serie regular de formaciones tanto a la Alta Dirección como a los cuadros intermedios sobre habilidades en la toma de decisiones y gestión de crisis ante ciberataques, que apelen a la figura del CISO, pero también sean una dimensión que esté en los protocolos diarios y en la forma cotidiana de trabajar del resto de equipos directivos y de gobierno.

5. Nivel de sofisticación y equilibrio entre las medidas *ex ante* y *ex post* ante un *ransomware*

Se han indicado anteriormente las consecuencias de un ataque por *ransomware* en materia de reputación, ingresos, plantilla y confianza, entre otros. Ante este impacto significativo, las empresas que han sido víctimas de un ciberataque de esta modalidad suelen implantar cinco medidas específicas (*VentureBeat*, 2021):

- Un 48% de estas empresas contratan talleres de formación en concienciación de seguridad;
- Un 48% integra sus servicios en Centros de Operaciones de Seguridad (SOC);
- Un 44% implanta la protección de *endpoints*;
- Un 43% implementa sistemas de apoyo y recuperación de datos;
- Un 41% genera escaneos de correos electrónicos.

Sin embargo, las soluciones menos implementadas, muchas de ellas esenciales para ataques de una naturaleza tan híbrida entre lo virtual y lo humano como es el *ransomware*, son:

- Escaneo de web (solo un 40% de las empresas);
- Detección y respuesta de *endpoints* (EDR) y tecnologías de detección y respuesta extendidas (XDR), en solo el 38% de las empresas. Estos sistemas son, sin embargo, esenciales para responder ante amenazas combinadas para las cuales el enfoque convencional de seguridad ya no es suficiente;
- Software antivirus (solo el 38% de las compañías);
- Soluciones de seguridad móvil y SMS (36%), dado que el *ransomware*, que puede llegar a exigir grandes cantidades de dinero, accede fácilmente por cualquier vía, incluso aquella concebida como la más sencilla y de menor penetración en el sistema de la compañía;
- El 3% de las firmas encuestadas afirmó que no hizo ninguna inversión en seguridad tras un ataque de *ransomware*.

En el caso del *Colonial Pipeline*, un fallo importante fue no disponer de una segmentación concreta de sus entornos de red, permitiendo así que los ciberdelincuentes pudieran actuar con mayor facilidad.

Otro debate de carácter operativo para las empresas, es el que se plantea ante situaciones en donde la capacidad financiera es limitada y no permite invertir en una amplia cantidad de sistemas de seguridad. En este escenario, ¿qué deberían primar: las medidas *ex ante* para prevenir posibles accesos a la red y consecuentes solicitudes de rescate, o las medidas *ex post* para saber responder rápidamente ante este tipo de *ransomware*?.

No existe una respuesta única. Cada contexto empresarial es particular y requiere de unas soluciones personalizadas. Para ello, se requiere formación sobre las virtudes y deficiencias de ambos tipos de medidas, no solamente desde un punto de vista técnico y operativo, sino también en la dimensión organizativa, de gestión de la reputación y de

cumplimiento con la regulación, entre otros. Olvidar esta segunda dimensión –la que está menos vinculada con lo puramente operativo- es perder un gran margen de maniobra.

6. Desmitificar al atacante: el caso del *RaaS*

Cuando el 7 de mayo *Colonial Pipeline* tuvo que cerrar durante seis días sus 8,850 kilómetros de tuberías, se buscó rápidamente atribuir la autoría. Inicialmente se apuntó a *DarkSide* como una entidad apoyada por el gobierno ruso con el fin de desestabilizar las infraestructuras críticas del país. Sin embargo, el 9 de mayo, solo dos días más tarde del ciberataque, *DarkSide* publicó un comunicado en donde no mencionaba directamente el ataque, pero afirmaba que su "objetivo era obtener ganancias monetarias, y no crear problemas sociales".

Sin embargo, más allá de que rápidamente se confirmara que era un grupo con fines lucrativos –y no vinculados a asuntos de seguridad nacional o de carácter geopolítico-, lo cierto es que es preciso desmitificar la figura del ciberatacante en este tipo de actuaciones.

DarkSide no era un grupo de ciberdelincuentes que se unieron de forma organizada en una zona de un país para coordinarse e incrementar las ganancias, ni un grupo de especialistas informáticos dispersos por el planeta que se unieron para este proyecto específico. Todo lo contrario, ***DarkSide* es una franquicia de crimen organizado**.

Darkside es una plataforma que **ofrece un portfolio de servicios para que sean otros grupos –sus clientes- quienes cometan el delito informático**. *DarkSide* funciona como un ***marketplace*** para aquellos ciberdelincuentes que buscan comprar herramientas y servicios. Entre estos servicios se pueden encontrar desde mantener una página web donde publicar la información robada, hasta herramientas para hacer llamadas de extorsión a las entidades (CrowdStrike, 2021). Cuando apoya en la realización del *ransomware*, DarkSide gana de un 10% a un 25% del total del pago realizado en el rescate (Bloomberg, 2021). A este negocio se le llama de forma creciente ***Ransomware as a Service (RaaS)***.

DarkSide no se limita a proveer de estos servicios, sino que, en el caso de que la entidad víctima se niegue a realizar el pago por rescate, *DarkSide* ofrece a la víctima la opción de comprar *put options* u "opciones de venta". Cuando *DarkSide* anuncia que ha hackeado a esta empresa, sus acciones bajan, lo cual hace que las *put options* que DarkSide compró le den un beneficio significativo, pues es el mecanismo natural de este instrumento financiero: sube cuando las acciones de la empresa bajan (Harwell, MacMillan, 2020). En cualquier caso, la empresa víctima pierde en ingresos y reputación. Esto hace que muchas víctimas tengan más incentivos en realizar el pago directamente a *DarkSide*, sin informar a las agencias gubernamentales competentes.

7. Conclusiones

No existe una vía única a la hora de responder ante ciberataques por *ransomware*. Tampoco de prevenirse ante ellos. Existen varios modelos de gestión y colaboración entre los sectores público y privado; cada uno con sus virtudes y deficiencias.

Sin embargo, existe un eje común a todo tipo de escenarios que pueden derivarse del caso *Colonial Pipeline*: la necesidad de mejorar la cultura de ciberseguridad actual en las empresas. Este marco de cultura abarca:

- La ampliación del presupuesto medio aplicado en los departamentos de Seguridad de la Información o de Ciberseguridad de la firma.
- El establecimiento de formaciones y talleres continuados según el grado de madurez y concienciación por parte de la Alta Dirección.
- La medición continuada y sostenida de indicadores para realizar un correcto análisis de impacto.
- Un primer cambio de mentalidad de que la ciberseguridad no es solamente una dimensión más dentro del organigrama empresarial, sino que es una realidad que permea en todos los departamentos.
- Un segundo cambio de mentalidad de que la ciberseguridad no se refiere únicamente a cuestiones técnicas u operativas, sino a otras dimensiones como la gestión de la reputación, la incidencia en asuntos públicos, el cumplimiento de la regulación, así como el estrechamiento de alianzas estratégicas con entidades del mismo sector, o grupos de otros sectores y que forman parte de la misma cadena de valor de un producto o servicio.

El caso del *Colonial Pipeline* ofrece aprendizajes interesantes desde estos prismas. Para poder darles efectividad, el siguiente paso será realizar una autoevaluación personalizada para entender las fortalezas y debilidades ante la realidad del ciberataque por *ransomware*.

Referencias

Bloomberg, *DarkSide Hackers Mint Money with Ransomware Franchise* (12 de mayo de 2021). Disponible en https://www.bloomberg.com/news/articles/2021-05-12/darkside-hackers-mint-money-with-ransomware-franchise?sref=1kJVNqnU

CrowdStrike, *Ransomware as a Service (RaaS) Explained* (28 de enero de 2021). Disponible en https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/

Cybersecurity Ventures (2021). *Ransomware: The True Cost to Business*. Cybereason. Disponible en https://www.cybereason.com/ebook-ransomware-the-true-cost-to-business

FELABAN (2021). *Fraud Information Control by FELABAN*. Disponible en https://fic.felaban.com/

Harwell, Drew, & MacMillan, Douglas, *Investors in breached software firm SolarWinds traded $280 million in stock days before hack was revealed* (The Washington Post, 16 de diciembre de 2020). Disponible en https://www.washingtonpost.com/technology/2020/12/15/solarwinds-russia-breach-stock-trades/

U.S. CISA (2021). *The NEW Ransomware Guide,* U.S. Cybersecurity and Infrastructure Agency, U.S. Government.

VentureBeat, *Adopting zero trust architecture can limit ransomware's damage* (14 de mayo de 2021). Disponible en https://venturebeat.com/2021/05/14/adopting-zero-trust-architecture-can-limit-ransomwares-damage/