Foto: iStock.com/lucadp

Ocho lecciones aprendidas de un ciberataque combatido por MAPFRE

Guillermo Llorente // Director Corporativo de Seguridad de MAPFRE

"MAPFRE tenía las medidas de seguridad adecuadas para hacer frente a ciberataques, lo que permitió actuar diligentemente y minimizar sus efectos y, además, lo hizo con una comunicación transparente con todos los grupos de interés."

Estos tres mensajes, que forman parte de las conclusiones de la investigación desarrollada por la Agencia Española de Protección de Datos, y su decisión consecuente de archivo de las actuaciones, ponen punto final a un episodio que no sabría calificar como negro o brillante, pero que, sin duda, ha sido el de mayor alto impacto, en términos de riesgo para la entidad, que ha vivido MAPFRE en su historia reciente.

Todos conocemos las teorías de los cisnes negros, esos eventos de muy baja probabilidad de ocurrencia y muy alto impacto, y hasta algunos estamos cansados de leer sobre ellos, pero la mayoría de nosotros, aunque racionalmente los entendamos e incorporemos a nuestro discurso, emocional y personalmente, los mantenemos lejos como algo sobre lo que hay que trabajar, pero sin asumir que nos pueda suceder. Ello es resultado lógico de nuestra condición de seres humanos y por naturaleza positivos y optimistas *¿qué sería de nosotros si no lo fuéramos?* quienes tratamos de alejar de nuestra mente y de nuestros pensamientos, aquellos más tristes o desagradables.

Pero la realidad es tozuda, y el año 2020 será, para toda nuestra generación, buen ejemplo de ello, pues una pandemia global como la que atravesamos, con más de un año ya de persistencia, estará en los libros y en los modelos teóricos de riesgo. Era, sin duda, el cisne negro que todos nos negábamos a interiorizar y a asumir que nos podría pasar.

En el caso de MAPFRE, en medio del sobrevuelo de ese cisne negro por todos vivido, sobrevino otro aún peor, un ciberataque de *ransomware* que afectó a miles de servidores y estaciones de trabajo en España, en el peor momento posible del año.

¿Qué sucedió?

La noche del viernes 14 de agosto los sistemas informáticos de MAPFRE en España sufrieron el despliegue de un *ransomware* que cifró ficheros de miles de servidores y puestos de usuario Windows.

¿Qué es un ataque de *ransomware*?

Atacantes utilizando diversas técnicas, acceden a una red, se expanden por ella desplegando un virus en equipos y servidores, y tras un tiempo dentro, mandan una orden de cifrado a los dispositivos a los que han alcanzado, imposibilitando el acceso a las aplicaciones y a la información contenida en dichos equipos, así como al uso de estos.

¿Cómo fue el ataque? Tras la laboriosa y detallada reconstrucción de los hechos, gracias al análisis forense, descubrimos que:

Fue un ataque LARGAMENTE PREPARADO, los dominios (algo así como las direcciones de internet) que se utilizaron, fueron comprados un año antes del lanzamiento de la orden de cifrado.

Fue un ataque muy PROFESIONAL y SOFISTICADO, en el que, junto a otras técnicas, los atacantes utilizaron herramientas de *hacking* de escalada de privilegios, no conocidas previamente en el mercado.

Fue un ataque ESPECÍFICAMENTE DISEÑADO contra MAPFRE, los atacantes utilizaron y probaron diferentes versiones de virus, que fueron detectadas y bloqueadas por los sistemas de seguridad, hasta conseguir una versión del virus indetectable por la plataforma de seguridad.

Fue un ataque REFORZADO por el entorno COVID, pues su impacto fue ampliamente favorecido por el hecho de que la empresa, como todas las que tuvieron capacidad, estaba funcionando con la mayoría de sus trabajadores en remoto.

Fue un ataque ENORMEMENTE PRECISO para lograr el mayor impacto, lanzado en mitad del mes de agosto en España, fecha en que se concentra el mayor porcentaje de ciudadanos de vacaciones y, por tanto, uno de los periodos de mayor demanda de servicios de asistencia en carretera; y lanzado una noche de fin de semana, cuando menos personal hay de servicio en cualquier empresa.

¿Cómo empezó el ataque?

A través de la captura, de las credenciales de acceso de un usuario a la red de MAPFRE, en su equipo personal previamente infectado.

¿Como se reaccionó?

A las **21:04** Se lanzó la orden de cifrado de los equipos. Cualquier compañía de nuestro tamaño detecta y neutraliza cada día miles de ataques que de distintas maneras buscan acceder al interior de los sistemas. Con equipos testados y personas entrenadas, el Centro de Operaciones de Seguridad de Mapfre emitió la primera señal de alarma apenas siete minutos más tarde, a las 21.11h, desencadenando la activación del Comité Corporativo de Crisis, y los procesos de seguridad y tecnología previstos frente a este tipo de escenarios, entre ellos:

> Por muchas herramientas que despleguemos, al final, la seguridad depende de las personas, del usuario, del desarrollador. Debemos reforzar nuestra Cultura Corporativa de Seguridad

Contención del ataque mediante, entre otras, órdenes urgentes de apagado de los equipos, corte de comunicaciones con las entidades MAPFRE en otros países y terceras empresas, así como de aislamiento de nuestro Data Center Alternativo para caso de contingencia.

Garantizar el Servicio a los clientes por procedimientos alternativos. Esa primera noche MAPFRE ya disponía de un refuerzo de personas y canales aislados que permitieron dar continuidad al servicio.

Análisis Forense, elemento básico para entender que había pasado y como, así como el alcance de la afectación, y poder construir, desde ese conocimiento, tanto la respuesta al ataque, como la restauración de los sistemas.

Restauración de los sistemas, orientada a la recuperación del servicio, sujeta a los requisitos de seguridad, y posibilitada por la calidad y seguridad del *backup*.

Refuerzo, desplegando de forma urgente un conjunto de medidas y herramientas para robustecer el entorno de seguridad, prevenir, detectar y ganar en capacidad de respuesta, en caso de un nuevo ataque, tanto por el atacante inicial como por otros. Desgraciadamente, cuando se hacen públicas este tipo de situaciones, grupos de cibercriminales de todo el mun-

do, focalizan su atención sobre la compañía afectada, de forma similar a como hacen los tiburones cuando huelen la sangre.

Comunicación, rápida y transparente a todos los grupos de interés e instituciones relacionadas. MAPFRE decidió actuar con plena transparencia desde el primer momento. Esa transparencia, de la que nos sentimos tan orgullos, también motivó, que reguladores y clientes del todo el mundo se dirigieran a nosotros interesándose por lo sucedido y obligando a un esfuerzo en la respuesta, muy significativo.

Lecciones aprendidas

Las lecciones aprendidas del ciberataque son muchas, tanto sobre lo que ha funcionado bien, como de los aspectos a mejorar, ya sean de carácter técnico como organizativo, pero hay algunas que creo oportuno resaltar:

- **Riesgo de Ciberseguridad al alza:** las amenazas son cada vez mayores y no van a desaparecer, por lo que debemos prepararnos para una nueva normalidad en la que los Ciberataques sofisticados contra nosotros se sucedan.

Foto: iStock.com/DigitalStorm

- Ningún **Plan de Continuidad de Negocio**, podrá responder a todos los escenarios posibles, pero disponer de ellos, actualizarlos y entrenar reiteradamente el sistema de gestión de crisis, es imprescindible.
- El perímetro tradicional ha desaparecido y la **identidad digital** se ha convertido en **el nuevo perímetro de las compañías**, que hay que blindar.
- Hay que aumentar la **exigencia de cumplimiento de los "básicos" de seguridad** a todos los entornos conectados a nuestra red. El símil de la fortaleza de la cadena está más que manido, pero, lamentablemente, sigue estando totalmente vigente.
- Debemos reforzar nuestras **capacidades de monitorización y respuesta**. Tenemos que adaptarnos al nivel de sofisticación de la amenaza. La colaboración público –privada y privada– privada, se demuestra más necesaria que nunca.
- **No hay alternativa a la de integrar eficientemente la seguridad en los nuevos sistemas y aplicaciones**. La seguridad debe ser parte nuclear del proceso de transformación de nuestras organizaciones y de nuestra sociedad.
- **Por muchas herramientas que despleguemos**, al final, la seguridad depende de las personas, del usuario, del desarrollador. Debemos reforzar nuestra Cultura Corporativa de Seguridad. Hay que llevar la Seguridad al ADN de la compañía.
- Cuando un ataque de este tipo sucede, los recursos ofrecidos y disponibles en el mercado pueden ser infinitos, pero la auténtica diferencia estará en la capacidad real previamente instalada, que establecerá cual es el límite de la capacidad de absorber recursos adicionales para gestionar esa crisis.

Por último, y como colofón, permítanme trasladarles la que para mí ha sido también la gran lección aprendida del pasado año, y es la enorme resiliencia de MAPFRE, que no fue solamente capaz de afrontar con éxito la pandemia, sino que, adicionalmente, y en el peor momento posible, víspera del día más desafiante del año, fue capaz de responder y sobreponerse al peor ataque que hubiéramos podido imaginar, y seguir cumpliendo con su misión y el compromiso con sus clientes. Por ello, estoy convencido de que, aunque aquellas noches fueron negras, el futuro es brillante. ●