La España sanitaria, ciber-atacada

Manuel Pérez // Director de Ciberriesgos (Howden Iberia, S.A.U.)
José J. Martínez // Universidad de Alcalá

Una portada de ABC del 14 de enero de 2018 dedicaba accidentalmente un reflejo del estado de la ciberseguridad en nuestro país. El titular mostraba un *"España reclutará dos mil hackers contra las ciberamenazas"*, reconociendo así una contingencia de escala nacional y la consecuente respuesta que se pretendía dar ante tal peligro. El problema de aquella portada, motivo por el cual se hizo tan popular ayer y hoy en este artículo, es que la imagen de fondo tras ese titular mostraba lo que parecía ser un profesional de sonido más que un cracker. La reflexión entonces quedaría resumida en que España conoce que tiene un problema en este ámbito y que está decidida a ponerle una solución, pero que lamentablemente acaba fallando en el análisis y enfoque de esta ansiada y necesaria respuesta.

> Sin preparación, planificación e inversión en ciberseguridad, es cuestión de tiempo que veamos más pantallas bloqueadas en oficinas, más megafonías pidiendo que se apaguen los ordenadores y más noticias sobre nuevos ataques que paralizan a nuestras empresas, sin importar tamaño ni condición

Años más tarde, la situación ha cambiado, pero ni mucho menos se ha revertido. De nuevo, frente a cientos de ataques cibernéticos diarios, seguimos haciendo gala de nuestro ya conocido internacionalmente *"mañana, mañana"*, y es esa procrastinación la que nos hace seguir en el podio de la condena digital a nivel global. Claro ejemplo de este fenómeno han sido los continuos ataques a entidades relacionadas con el sector salud en este 2020, mientras muchos siguen preguntándose el porqué. Según leemos y oímos a expertos informar que todo es debido a la intención oscura del *cracker* en dirigir sus ataques sobre las entidades sanitarias, dada la alta dependencia que tiene la sociedad para con ellas debido a la presente pandemia, volvemos a menospreciar a la figura del *ciber-delincuente* y a recurrir a argumentos manidos basados en películas americanas sobre el cracker y su amor por el caos. Ya en los mejores cines.

Está claro que los datos son el nuevo oro. Y tras la llegada del Reglamento General de Protección de Datos, sabemos que dentro de esta etiqueta, los datos sobre la salud de los usuarios ocupan una categoría superior en cuanto a la sensibilidad de esta información. Dicho esto, y siendo conscientes del gran valor que tendría esta categoría para los ciberdelincuentes de todo el mundo, no podemos olvidar una nueva variable de la ecuación: ¿Cuánto ha aumentado el valor de estos datos médicos durante la pandemia del Covid-19? ¿Cuánto más con la carrera por una vacuna que ha tenido en vilo a personas de todos los rincones del mundo?

Reflexionemos un momento sobre qué información sobre pacientes pueden contener las bases de datos de un grupo hospitalario. Hagamos lo mismo con la cartera de clientes de seguro de salud de un asegurador. ¿Qué información encontraríamos?: diagnósticos, número de positivos, días de internamiento, tratamientos seguidos, respuesta ante esos tratamientos, efectos del virus, efectos secundarios tras pasar la enfermedad… y un buen número de etcéteras.

Introduzcamos ahora estos datos en una herramienta de tratamiento que sea capaz de sacar conclusiones sobre el conjunto. ¿Qué información tenemos delante?: Porcentaje de positivos por el total de pruebas realizadas, soluciones más efectivas, patrones comunes de síntomas y efectos secundarios, respuesta de los pacientes a tratamientos… una información de alto valor para ofrecerla en el mercado negro de la *Deep Web* y sacar un notable rendimiento económico por su venta. Una venta que siguiendo esta explicación se podría efectuar en varias ocasiones y con sencilla rapidez, ya que no debemos olvidar que el dinero, una vez gastado, se elimina, pero los datos una vez vendidos, pueden volverse a vender. De ahí su etiqueta del "nuevo oro". Conocedores de este gran negocio, los *crackers* de todo el mundo han apuntado sus tácticas fraudulentas hacia aquellas entidades que pueden tener esta información, desde hospitales a clínicas, pasando por aseguradores del ramo de la salud. En cuestión de semanas vemos a hospitales bloqueados y a dos aseguradores líderes en sector salud con sus sistemas en jaque. La carrera por los datos había comenzado, y a España la habían *pillado* buscando fotos de técnicos de sonido en Google.

Un nivel de respuesta notable de estas entidades y sus proveedores de ciberseguridad, dejaron a día de hoy estos ataques en una simple anécdota, pero las barbas del vecino ya se han cortado, y seguimos echando de menos acciones que impidan un remojo inevitable en las demás firmas que comparten el sector. Los que estamos dentro del sector compartimos que el proceso de "evangelización" sobre la ciberseguridad en nuestro país se está haciendo más largo de la cuenta, y que seguimos dándonos de bruces con presupuestos limitados, desconocimiento en la materia por parte de la dirección general y con el ya tan nuestro "*mañana, mañana*".

Sin preparación, planificación e inversión en ciberseguridad, es cuestión de tiempo que veamos más pantallas bloqueadas en oficinas, más megafonías pidiendo que se apaguen los ordenadores y más noticias sobre nuevos ataques que paralizan a nuestras empresas, sin importar tamaño ni condición.

Parte de esta preparación pasa por la contratación de seguros de ciberriesgos. Este tipo de contratos garantiza la transferencia de este riesgo y cada vez más, están equipados con amplias redes de colaboradores en materia de respuesta a incidentes y asesores legales en brechas de datos que se ponen a disposición del asegurado de forma permanente (24/7) durante el periodo de póliza acordado. Nacidos a partir de las antiguas pólizas de Protección de Datos, estos seguros han ido evolucionando para incluir coberturas de daños propios a la víctima del ciberataque, que pasan desde la indemnización de los costes de recuperación de sistemas y accesos, hasta la pérdida del beneficio perdido durante la interrupción. Todo ello contando con las coberturas propias de responsabilidad civil con terceros afectados tras el incidente (en el caso que veíamos antes, los propios pacientes o clientes cuyos datos son revelados), así como las posibles repercusiones en materia de investigaciones y sanciones de la AEPD. Retomando el aspecto de esa planificación necesaria en este riesgo, el bróker de seguros adquiere incluso una responsabilidad mayor de la que acostumbra, ya que debe inmiscuirse en la recuperación del incidente para ayudar al cliente a dar los pasos recomendados para resolver el evento y más tarde, ser indemnizado por el asegurador. Esta ayuda se vuelve vital en estas situaciones.

En conclusión, tardamos años en construir una buena reputación, y en los últimos años parece que basta un *click* para arruinarla. Ya que conocemos el problema y sabemos que debemos ponerle solución, trabajemos en cómo enfocar la respuesta y preparémonos para lo que se supone, será la siguiente gran guerra. ●

Foto: iStock.com/metamorworks