CONSECUENCIAS DE UNA PANDEMIA MUNDIAL EN LAS INFRAESTRUCTURAS CRÍTICAS

JORGE UYÁ. DIRECTOR DE OPERACIONES DE ENTELGY INNOTEC SECURITY

Desde que se declarara la pandemia generada por la COVID-19 se ha registrado un notable aumento de los ciberataques a algunos de los sectores esenciales para hacer frente a la situación. Los hospitales, la industria farmacéutica y los centros de investigación, infraestructuras críticas primordiales para gestionar la enfermedad, han sido objetivo de los ciberdelincuentes durante los últimos meses, poniendo de manifiesto la necesidad de incrementar en ellos las medidas de seguridad.

Las infraestructuras críticas de un país, que en el caso de España abarcan hasta 12 sectores diferentes, sustentan los servicios esenciales para que una sociedad pueda funcionar correctamente. Y estas, asimismo, dependen unas de otras para su normal desenvolvimiento. Ello implica que, de sucederse una alteración en alguna de ellas, tendría lugar una cascada de fallos que afectaría a otras infraestructuras, provocando consecuencias catastróficas para la población.

La situación de pandemia en la que nos encontramos desde hace meses a nivel mundial, como consecuencia de la COVID-19, ha tenido sin duda efectos devastadores a nivel sanitario, social y económico. Estas consecuencias han ido más allá y, desde el pasado mes de marzo, se ha registrado un importante incremento de los ciberataques a estas infraestructuras, particularmente al sector sanitario.

La propia Organización Mundial de la Salud (OMS), un organismo clave en la gestión de la pandemia, ha sido objeto de numerosos ataques a lo largo de estos meses. La organización así lo señalaba a mediados de abril[1], tras ver cómo el número de ciberataques se había multiplicado por cinco, e instaba a incrementar la vigilancia.

EL SECTOR SANITARIO, EN EL PUNTO DE MIRA DE LOS CIBERDELINCUENTES

Una de las peores partes de esta tendencia se la han llevado los propios hospitales, más necesarios ahora que nunca, si cabe. Estos se han visto afectados, e incluso paralizados, en numerosas ocasiones debido a ataques a sus sistemas informáticos. Un ejemplo de ello fue el ataque al hospital universitario de Brno, la segunda mayor ciudad de la República Checa. Este centro estuvo bloqueado durante un tiempo como consecuencia de un ransomware que secuestró los dispositivos electrónicos, provocando que varias intervenciones quirúrgicas de urgencia se tuvieran que posponer.

Uno de los principales protagonistas de esos ciberataques es el virus informático «NetWalker», un

ransomware con un potencial muy dañino que se envía a través de correo electrónico, y que ha estado detrás de muchas de las amenazas a los hospitales españoles, atacando tanto a trabajadores como a organismos sanitarios. Un ciberataque exitoso con este ransomware sobre un centro sanitario tendría consecuencias devastadoras, pues sería capaz de paralizar los sistemas informáticos con solo enviar un e-mail a uno de sus trabajadores y que este pinche en alguno de los enlaces que estos suelen incluir.

Tampoco se libra la industria farmacéutica y los centros de investigación, responsables de la búsqueda de una vacuna para esta y otras muchas enfermedades. Y España ha sido uno de los países a los que han ido dirigidos estos ciberataques, tal y como señalaba recientemente Paz Esteban, directora del Centro Nacional de Inteligencia (CNI), durante un seminario organizado por la Asociación de Periodistas Europeos: «La pugna por la vacuna es un aliciente más que sobrado para que actores, estatales o no, hayan emprendido una campaña de ataques especialmente virulenta no solo en España, sino en todos los países». El objetivo de estos ataques no es otro que el robo de datos relacionados con la vacuna.

Situarse en el ojo del huracán con las tremendas repercusiones que puede llegar a tener un incidente en este tipo de sistemas, ha facilitado este incremento de ciberataques, por lo que ahora es más necesario que

nunca adoptar una serie de medidas para preservar su seguridad.

En este sentido, para evitar al máximo los ataques, riesgos y vulnerabilidades de estas infraestructuras sería necesario, al menos, tener en cuenta las siguientes recomendaciones:

-Realizar una evaluación de riesgos donde se analicen los activos, el valor y el riesgo que tiene cada uno, así como el daño potencial, adoptando las medidas de seguridad a implementar.

-Definir las políticas, procedimientos y alcance del proyecto, y coordinar las tareas del personal.

-Establecer una arquitectura de seguridad de referencia. Realizar un inventariado y clasificación de activos, así como la segmentación de las distintas redes, creando y definiendo niveles de seguridad. Igualmente, será necesario controlar todos los datos que puedan intercambiarse entre estas capas por medio de un firewall de nueva generación.

-Implementación de medidas de seguridad de red, gestión de acceso remoto, firewalls y diodos, monitorización de red, gestión de contraseñas, concienciación del personal, gestión de actualizaciones y despliegue de una solución SIEM y un SOC específico industrial (fundamental en infraestructuras críticas).

Comprobar con frecuencia las capacidades de protección, detección y respuesta mediante pruebas de hacking ético o red team, es decir, llevar a cabo simulaciones de ciberataques para determinar que el nivel de defensa es el correcto de cara a hacer frente a un ataque real.

«Desde el pasado mes de marzo, se ha registrado un importante incremento de los ciberataques a estas infraestructuras, particularmente al sector sanitario»

Estas y otras medidas de seguridad son fundamentales para mejorar la protección de las infraestructuras críticas, independientemente del sector al que pertenezcan. Solo una concienciación y conocimiento de las amenazas a las que se exponen puede mitigar sus efectos y evitar las graves pérdidas que pueden llegar a provocar y, de hecho, provocan. ✱

Referencias

1.- Organización Mundial de la Salud: https://www.who.int/es/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance.estable.