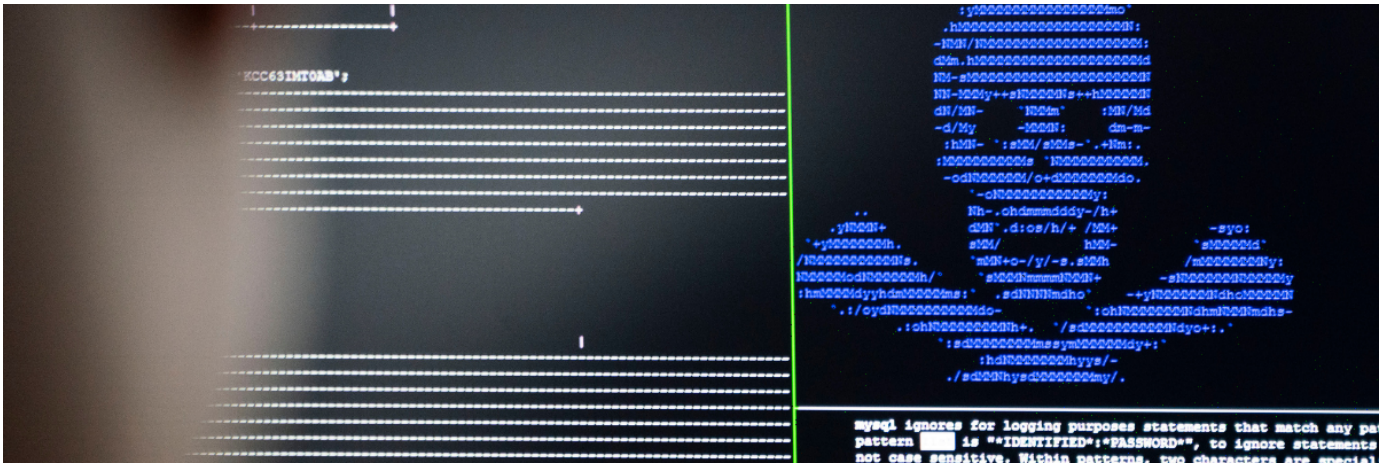
La ciberseguridad en las infraestructuras críticas

Iván Giménez Chueca



Especialistas de seguridad aprenden cómo los programas de "Ransomware" se pueden volver inofensivos en la sala "Cyber ??Range" del nuevo centro de seguridad cibernética "Athene" en el instituto nacional de investigación de Fraunhofer-Gesellschaft (Frank Rumpenhorst/Picture Alliance via Getty Images).

Los ataques de* hackers *han proliferado contra estas instalaciones estratégicas, pero también se ha avanzado mucho en las medidas de protección.

“Las amenazas a la ciberseguridad contra los sistemas que controlan y operan las infraestructuras críticas, de las que todos dependemos, se encuentran entre los problemas más importantes y crecientes a los que se enfrenta nuestra nación”, así rezaba el memorando aprobado por la Casa Blanca a finales de julio de 2021. Toda una muestra de cómo una de las grandes potencias del planeta ponía en primera línea la ciberseguridad de las instalaciones estratégicas del país.

¿Qué se entiende por infraestructura estratégica? Serían todas aquellas que se consideran esenciales para garantizar el normal funcionamiento de los servicios que proporcionan las diferentes administraciones de un país, incluso también aquellas que abarcan ámbitos muy sensibles para el sector privado.

Para entrar más en detalle en estas categorías, Cipher, empresa dedicada a la ciberseguridad, ha identificado hasta 16 sectores clave que pueden ser objeto de amenazas a través de la Red. Bajo esta definición, entrarían ámbitos tan variados, pero fundamentales, como el energético (desde centrales nucleares hasta presas), suministro de agua, finanzas, sanidad, gestión de emergencias, etcétera.

Más allá de estas definiciones genéricas que pueden ayudar a situarse en la cuestión, se han

producido casos concretos recientes que ponen de manifiesto las vulnerabilidades de estos sectores. Por ejemplo, el citado memorando del gobierno de EE UU no hacía referencia solo a teóricas amenazas, sino que era la respuesta antes algunas acciones concretas que había sufrido el país. La más reciente fue el ciberataque contra Colonial Pipeline, la principal red de oleoductos de Estados Unidos.

Tuvo lugar a principios de mayo de 2021, un ataque con *ransomware*, un *software* que infecta una red de ordenadores. A partir de ahí, el virus informático evita que los equipos se utilicen con normalidad, a no ser que se pague un rescate a los responsables de la acción. Es decir, un chantaje en toda regla.

En el caso concreto de Colonial Pipeline, el ciberataque detuvo todas las operaciones de un oleoducto que era la principal fuente de suministro de crudo para la costa Este de EE UU. Causó importantes problemas de abastecimiento en gasolineras de lugares como la misma Washington DC y en los estados de Alabama, Georgia, Florida, Carolina del Norte y Carolina del Sur. Incluso el aeropuerto de Charlotte tuvo que retrasar un buen número de vuelos.

El presidente Joe Biden tuvo que recurrir al estado de emergencia en 17 estados para garantizar el suministro. Además, la empresa pagó un rescate de 75 bitcoins (4,3 millones de euros) y poco a poco pudo restablecer el servicio. El FBI identificó al grupo DarkSide como responsable del ataque. Según los investigadores estadounidenses, está integrado por *hackers* rusos y de Europa del Este. Aunque, al contrario que otros grupos de perfil parecido, no están controlados por el Kremlin, sino que son una organización criminal autónoma que se dedica a este tipo de acciones.

Fuentes de la Oficina de Coordinación de Ciberseguridad del Ministerio del Interior de España han detallado a *esglobal* los riesgos de estos ataques *ransomware*: “Cada vez presentan mayor

especialización y, por tanto, son más peligrosos debido especialmente a que el crimen organizado está adoptando la modalidad del *crimen como servicio*, donde es posible contratar personal especializado para diseñar un ataque *ad hoc* en base al objetivo fijado".

Por su parte, Andrea G. Rodríguez, investigadora de CIDOB, ha explicado a *esglobal* cómo se puede conocer estas potenciales amenazas en la Red, asegurando que "hay que seguir invirtiendo en saber qué está pasando en el ciberespacio, quiénes son los actores, cómo actúan, cómo están evolucionando y cómo pueden atacarte".

La cuestión se remonta a hace años. Antes del caso de Colonial Pipeline y del memorando de la Casa Blanca, las altas esferas estadounidenses ya habían manifestado su preocupación por los riesgos en los canales digitales. El teniente general Paul Nakasone, comandante del mando de ciberdefensa de Estados Unidos, declaró en 2018 ante el Comité de Inteligencia del Senado que "nos enfrentamos a un entorno de amenazas desafiante y volátil, y las ciberamenazas a nuestros intereses de seguridad nacional y a las infraestructuras críticas ocupan el primer lugar de la lista".

Ya sea a través de *ransomware* o de virus informáticos ya hace unos cuantos años que los ciberataques marcan las relaciones internacionales. Solo hay que recordar que hace más de una década el virus Stuxnet causó daños en las instalaciones del programa nuclear iraní, aunque luego se extendió a ordenadores de otros países. Fue diseñado por Israel y Estados Unidos, según informó el diario *The New York Times*. Para la analista del CIDOB, la magnitud del ataque "provocó un antes y un después" en el ámbito de la ciberseguridad.

Otro caso llamativo fue el ciberataque que sufrió Ucrania en pleno invierno de 2015. Un cuarto de millón de habitantes del país se quedó sin suministro eléctrico durante seis horas. Otro ataque con *ransomware* fue el que sufrió el sistema de salud de Reino Unido en 2017 y que paralizó 16 hospitales.

Más allá de la espectacularidad de los hechos o cómo los enfoca la prensa, lo cierto es que se ha producido una evolución de la ciberseguridad en infraestructuras críticas durante los últimos años. Por ejemplo, en el mencionado caso del memorando de Estados Unidos, destaca que se implica al sector privado que opera estos sectores clave para el desarrollo de las medidas frente a los ataques digitales.

De hecho, seis meses antes de que lo hiciera la Casa Blanca, la Unión Europea presentó a finales de 2020 su nueva estrategia de ciberseguridad. El documento menciona específicamente como infraestructuras críticas los hospitales, las redes de energía, los ferrocarriles, los centros de datos, las administraciones públicas, los laboratorios de

investigación y la fabricación de medicamentos y productos sanitarios críticos.

Tomar medidas coordinadas en este campo es importante para los integrantes de la Unión debido a que se ha producido la interconexión de infraestructuras esenciales entre varios Estados miembros. Así lo apunta Adolfo Hernández Lorente, subdirector de Thiber, un *think tank* sobre ciberseguridad, quien explica que “un incidente de seguridad en una de las infraestructuras críticas de un estado de la UE podría afectar a otros países”.

Un visitante mira una pantalla electrónica que muestra datos de red en una exposición de ciberseguridad, parte de la Semana de Ciberseguridad de China del 11 al 17 de octubre de 2021 en Xi’an, provincia de Shaanxi en China (Zhang Yuan/China News Service via Getty Images).

Hernández Lorente también destaca que las nuevas tecnologías vinculadas a la Industria 4.0 (*big data*, *cloud computing,* Internet de las cosas…) "hacen que, amenazas típicamente asociadas a estas tecnologías, hayan irrumpido en los sistemas industriales, aumentando pues la superficie de ataque y abriendo este mercado a nuevas vulnerabilidades y exponiéndolo a unas amenazas crecientes". Pero el responsable del *think tank* no solo señala lo negativo, y apunta que "han aumentado las amenazas, pero también el sector de soluciones dirigidos a estos entornos, así como la inversión".

Volviendo a las actividades de ciberdefensa de la UE, estas se vehiculan a través de la Agencia Europea de Defensa. Europa define estas amenazas como "cambiantes" y "complejas". En el terreno práctico, la nueva estrategia apuesta por la creación de una red de Centros de Operaciones de Seguridad basados en la inteligencia artificial para lograr una mayor eficiencia frente a estas amenazas.

Por su parte, la OTAN también ha tomado medidas en este ámbito. En su cumbre de junio de 2021, la Alianza aprobó su nueva política de ciberdefensa. En la declaración final del encuentro, se mencionaba expresamente que los recientes ataques contra infraestructuras críticas de sus miembros son amenazas "complejas, destructivas, coercitivas y cada vez más frecuentes". El texto también advertía que estos riesgos "pueden tener efectos sistémicos y causar daños importantes"

La OTAN tiene una experiencia prolongada en contrarrestar estas amenazas. En 2007, Estonia sufrió un importante ciberataque que obligó a la Alianza a actualizar su estrategia para defenderse ante un ataque que la pilló totalmente por sorpresa. La experiencia fue útil y ahora el país báltico es un referente en ciberdefensa.

¿La mejor defensa es un buen ciberataque?

Pero las potencias mundiales no solo se preparan para defenderse. Rusia y China suelen ser sospechosos habituales en estas acciones, junto a otros *Estados canallas* como Corea del Norte o Irán. Pero Estados Unidos ha reconocido que tiene capacidad para golpear las infraestructuras de sus rivales a través del ciberespacio. Además, del mencionado caso de Stuxnet, según informó *The New York Times*, Washington instaló *software* malicioso en la red eléctrica rusa.

En este sentido, conviene recuperar la intervención del teniente general Nakasone ante el Senado estadounidense. A preguntas de los integrantes de la Comisión de Inteligencia sobre si

se estaban "desarrollando activamente capacidades para amenazar la infraestructura crítica de adversarios pares", el comandante del mando de ciberdefensa respondió afirmativamente.

Por su parte, la OTAN advierte que responderá a cualquier ciberataque, siguiendo la filosofía que aplica en su célebre artículo 5, frente a amenazas convencionales. Es decir, la ciberdefensa se integra de manera plena en la estrategia de defensa colectiva de la Alianza. El propio secretario general de la organización, Jens Stoltenberg, ha manifestado en diversas ocasiones que un ataque a través de canales digitales contra uno de sus miembros, es un ataque contra todos.

Más allá del protagonismo que puedan tener los organismos militares y como sucede en tantos otros ámbitos, la prevención suele ser la mejor herramienta. En esta línea se manifiesta también Andrea G. Rodríguez, quien concreta que, para mejorar la resiliencia de las infraestructuras críticas, “hay que seguir mejorando en la detención temprana de las amenazas, la comunicación y la coordinación entre los diferentes sectores interconectados y, por supuesto, los tiempos de respuesta”.

Desde la Oficina de Coordinación de Ciberseguridad del Ministerio del Interior español, se recuerda que “sería más coherente observar la evolución de la seguridad de las infraestructuras críticas desde su aspecto más integral”. Es decir, en la actualidad los países integran estrategias de protección de estos puntos sensibles que contemplen amenazas *online* y *offline.*

El riesgo de una escalada al mundo real

¿Un ciberataque podría provocar una guerra? Es una posibilidad que se ha barajado en algunos foros. El propio presidente Joe Biden reconoció este verano que su país podría acabar inmiscuido en una “guerra real” como resultado de un ciberataque. El mandatario no señaló a ninguna potencia rival, pero poco antes, en junio de 2021 durante una cumbre con su homólogo ruso, Vladímir Putin, elevó el tono al advertir a Moscú que su país respondería si continuaban los ciberataques.

Por su parte, el subdirector de Thiber explica que la respuesta con armas convencionales a un ciberataque ya es una realidad. “Existe el precedente del Ejército de Estados Unidos en 2015 utilizando drones para realizar ataques selectivos contra objetivos, con el fin de repeler ciberataques contra el país”. Fue en el que un aparato no tripulado mató a un *hacker* de Daesh.

El responsable de Thiber también recuerda el caso del ataque de la fuerza aérea israelí contra el cuartel general de ciberinteligencia de Hamás (HamasCyberHQ.exe). Incluso, las IDF hicieron público en Twitter

que habían ejecutado la operación.

En ocasiones, también se ha hablado del concepto de un "Pearl Harbor cibernético". Para Andrea G. Rodríguez, "sería un evento determinante para la seguridad global, como lo fue el ataque japonés". Mientras que desde la Oficina de Coordinación de Ciberseguridad del Ministerio del Interior se considera que "actualmente los sistemas de ciberseguridad de las infraestructuras críticas son muy robustos, por lo que un ataque generalizado que pudiera colapsar un país es bastante improbable".

Por último, el responsable de Thiber considera que el *Pearl Harbor cibernético* "técnicamente si es factible, y hemos tenido casos relevantes en los últimos años". Como casos concretos señala los mencionados ejemplo de la interrupción del sistema de distribución eléctrica en Ucrania en 2015 o el ataque en marzo de 2018 contra la red eléctrica de EE UU, en esa ocasión, las autoridades de Washington volvieron a responsabilizar a Rusia.

Fecha de creación
18 noviembre, 2021