CIBERSEGURIDAD EN LA ERA DE LA TRANSFORMACIÓN DIGITAL

IVAN SÁNCHEZ
Director de Seguridad de la Informacion (CISO) y responsable de la definición y ejecución del Plan de Seguridad de la información de las distintas unidades de negocio de la compañía y abarcando áreas como Ciberseguridad, Cumplimiento normativo, Protección de Datos, Seguridad Tecnológica o Continuidad de Negocio.
GRUPO SANITAS

Vivimos tiempos de transformación digital en las compañías. Se dice que no es una época de cambios, sino un cambio de época. Cuestiones como el Internet de las Cosas (IoT, *Internet of Things*) [1], el coche autónomo, el *Big Data* o las máquinas inteligentes han dejado de ser meros conceptos a ser una realidad en nuestro día a día y a convertirse en la pieza angular de la *Economía 4.0*. Del mismo modo que asociamos la Primera Revolución Industrial a la invención de la máquina de vapor, la Segunda al uso de la electricidad y la Tercera a la era de las comunicaciones e Internet, la Cuarta Revolución Industrial viene de la mano de la *Ciberindustria* en la que la digitalización y la hiperconectividad son los protagonistas.
Pero toda revolución también supone la aparición de una serie de factores de riesgo, que abordaremos a lo largo de este artículo y que englobaremos en lo que ahora se conoce como *Ciberseguridad*.

PANORAMA ACTUAL

Pocos sectores son ajenos a esta nueva transformación digital, aunque no son tantos los que han definido una agenda en materia de ciberseguridad. Y ello a pesar de que, hoy en día, la pregunta que los expertos en ciberseguridad han de hacerse no es si una compañía será o no atacada, sino cuándo será atacada.
Los números hablan por sí solos; el Informe Anual de Seguridad Nacional 2016 [2], publicado recientemente por el Departamento de Seguridad Nacional del Gabinete de la Presidencia del Gobierno destaca el incremento en el número de ataques cibernéticos hasta el punto de haberse triplicado desde 2013 (7.263 incidentes) hasta 2016 (21.000 incidentes) ver Figura 1.

El propio contenido del informe deja claro la importancia que las cuestiones en materia de ciberseguridad están adquiriendo para la Seguridad de nuestros intereses nacionales sobre otros tradicionalmente presentes en nuestro país: se dedican 11 páginas sobre la lucha en el ámbito de la ciberseguridad por 10 páginas dedicadas a la lucha contra el terrorismo.

Pero esta tendencia no es una cuestión exclusiva de nuestro país, sino que se trata de una tendencia global. Ya en 2012 el Foro Económico Mundial identificó un riesgo, por aquel entonces aún no tan presente, en el top 5 de riesgos "probables" de afectar la estabilidad mundial. Este riesgo era el de ciberataque [3]. En ese momento, muchos comenzaron a considerar seriamente el impacto que una ciber-disrupcion podría llegar a tener para las compañías, los ciudadanos o las naciones. Desde entonces, el riesgo de ciberataque no ha salido del cuadrante alto (alta probabilidad, alto impacto) de la matriz de riesgos globales que ela-

CYBERSECURITY IN THE DIGITAL TRANSFORMATION AGE

Cyberthreats are a reality in today's digital environment. Companies, Governments and Citizens are affected by first-digital then-physical events like power outages, data theft or malware infections. In such a changing environment, a business model where both attackers obtain financial benefit and state-sponsored attackers work, it's imperative to develop Cybersecurity strategies in order to uplift Companies and Government capabilities on protecting their infrastructure against Cyberthreats.

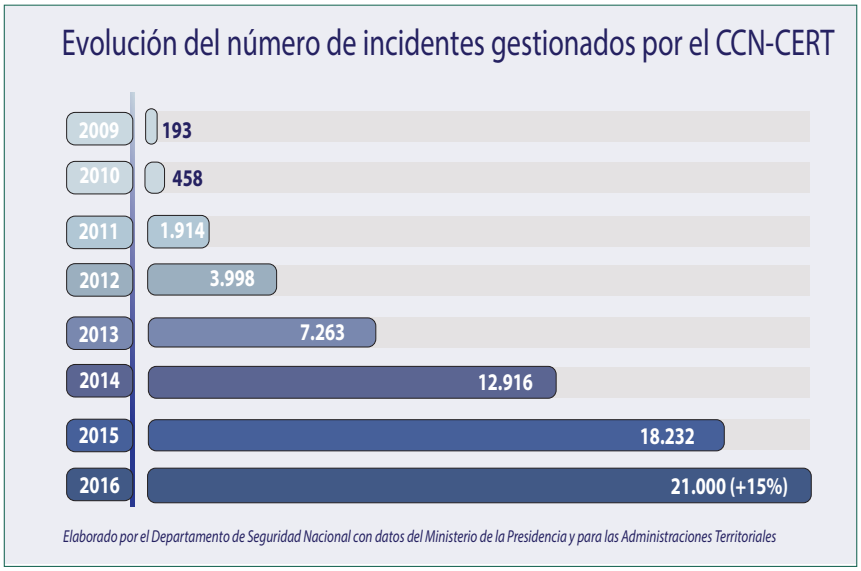

Figura 1. Servicio de vigilancia.

bora anualmente el Foro Económico Mundial. Incluso ha esponsorizado la creación de la llamada Comisión Global sobre la estabilidad del Ciberespacio (GCSC, *Global Commission on the Stability of Cyberspace*), reunida por primera vez en enero de 2017 y con representantes de alto nivel de diferentes compañías privadas y gobiernos.

La evolución de la tecnología y los servicios también implica una evolución de las ciberamenazas y una mayor sofisticación de los atacantes y de sus técnicas. Porque ya no hablamos de simples ataques vía correo electrónico de suplantación de identidad de una entidad bancaria o del *spam* que recibimos diariamente en nuestros buzones de correo, sino de ataques preparados y dirigidos contra objetivos muy concretos y que en muchas ocasiones explotan vulnerabilidades en *software* o en sistemas que son desconocidos por los propios fabricantes (los llamados ataques de día cero o *zero-days*). En el mercado negro de las "ciberarmas" se puede llegar a pagar más de un millón de dólares por llevar a cabo un ataque de este tipo. Hay un floreciente modelo de negocio con compañías y gobiernos que demandan estos servicios y dispuestos a pagar grandes cantidades de dinero, y eso hace aparecer de manera natural un mercado de oferta de *hackers*.

LA CIBERAMENAZA COMO CUESTIÓN DE ESTADO

La mayor dependencia que los gobiernos tienen de la tecnología hace del "ciberespacio" un nuevo campo de actuación. Procesos tan vitales para el funcionamiento de una nación como el mantenimiento de las infraestructuras críticas, la gestión de datos de sus propios ciudadanos o el llevar a cabo procesos electorales con apoyo de sistemas tecnológicos es ya una normalidad.

En este último apartado, son mencionables las últimas elecciones de los Estados Unidos donde las propias agencias de inteligencia del Gobierno (NSA, CIA, FBI) han acusado formalmente al gobierno ruso de haber influido proactivamente en el proceso electoral mediante una serie de ciberataques a sus sistemas. Este conflicto no fue el primero; ya en 2015 y 2016 la tensión entre EE.UU. y China llegó a alcanzar cotas muy elevadas cuando el, por aquel entonces, presidente Obama requirió formalmente al gobierno chino que cesaran las hostilidades y ciberataques ante empresas e intereses norteamericanos [4]. Se llegó a hablar de un posible *Cyber Pearl Harbour* que no llegó a materializarse ya que la presión se redujo tras una cumbre bilateral entre ambos países. En todo caso, las hostilidades no desaparecieron y el propio gobierno estadounidense se ha visto comprometido por las revelaciones del antiguo trabajador de la NSA y actual activista de la libertad en la red, Edward Snowden. En la información revelaba como el gobierno americano cuenta con un enorme arsenal de *ciberarmas* que ha empleado sistemáticamente incluso contra gobiernos extranjeros "aliados" (por ejemplo el caso de las conversaciones telefónicas del gobierno alemán interceptadas por la NSA).

En este contexto de digitalización, las compañías privadas se convierten en objetivo de ataques tanto por parte de atacantes que buscan un beneficio económico en el ataque como de gobiernos extranjeros interesados en el robo de información o en la potencial disrupción de sus actividades. Y todo ello con el agravante de la dependencia que las compañías tienen de sistemas fabricados por terceros que contienen vulnerabilidades de seguridad conocidas pero que en muchas ocasiones no es posible solucionar por las propias limitaciones de los sistemas terceros.

LA APLICACIÓN DEL CIBERATAQUE: ALGUNOS ATAQUES NOTABLES

Con respecto a los ciberataques, hay un factor muy difícil de señalar, que no es otro que la atribución del ataque. En el mundo "físico" es posible identificar un sospechoso por las evidencias que se pueden recoger: huellas, testigos, posicionamiento del sospechoso,... Por el contrario en el mundo "digital", el propio carácter distribuido y global de Internet hace esa recolección de evidencias muy difícil y, en muchas ocasiones, imposible.

Y es por todo esto que los ataques se suceden de manera continua, siendo algunos casos muy interesantes de estudiar bien por su sofisticación o bien por el impacto que han generado. Algunos de ellos son:

- **Stuxnet**, 2010 [5]: fue uno de los primeros con un altísimo grado de complejidad en su programación. Dirigido a interferir directamente en el programa nuclear iraní, consiguió penetrar en la red interna de la central nuclear de Natanz aprovechando vulnerabilidades en sistemas PLC de Siemens (Siemens SIMATIC Step 7 ICS). Una vez desplegado, su objetivo era tomar control de los sistemas para la reprogramación de los parámetros de las centrifugadoras. Se estima que alrededor del 20% de las centrifugadoras de la planta de Natanz quedaron fuera de servicio, y el programa nuclear iraní se vio retrasado por más de dos años.
- **Saudi Aramco**, 2012 [6]: el ataque sobre Aramco, compañía que produce en torno al 10% del petróleo

mundial, tuvo consecuencias muy graves para la operación de la compañía y su suministro de petróleo al mercado. El 15 de agosto de 2012, durante las celebraciones del Ramadán, un sofisticado virus penetró en la red de la compañía, haciendo que en cuestión de horas más de 35.000 equipos se vieran infectados, de modo que ninguna operación pudiera ser llevada a cabo. Mientras que los procesos industriales de extracción se llevaron a cabo con medios mecanizados, el resto de operaciones se vieron interrumpidas. La recuperación de la compañía se logró antes de que pudiera haberse producido un impacto en la cotización mundial del crudo, pero mostró una alerta sobre lo que en la economía puede llegar a producir un ciberataque.

- **Black Energy**, 2015 [7]: en diciembre de 2015 la red eléctrica de Ucrania se vio afectada por un sofisticado ataque que dejó sin suministro eléctrico durante seis horas a más de 250.000 hogares de la región Ivano-Frankivsk, del Oeste de Ucrania. Los atacantes, supuestamente relacionados con el gobierno ruso debido a la coincidencia en el tiempo con el conflicto de Crimea, tomaron el control del sistema de suministro eléctrico y paralizaron la actividad de unas 30 subestaciones eléctricas. Se calcula que dejaron de aportarse a la red 73 MW de electricidad (en torno al 0,015% de la producción diaria en Ucrania), pero lo que reveló es el impacto que un ciberataque puede tener en las infraestructuras críticas de un país.

CIBERSEGURIDAD EN EL SECTOR SANITARIO

El sector sanitario no es ajeno al entorno actual de aumento de los ciberataques a nivel global. Si bien históricamente el objetivo principal de los atacantes era el sector bancario por su capacidad de robo de activos financieros, el ciberataque masivo ocurrido en febrero de 2015 sobre la compañía aseguradora y de salud americana Anthem [8] supuso una evidencia en el cambio de motivaciones de los atacantes. En dicho ataque, se filtraron registros de información de alrededor de 80 millones de ciudadanos; se estima que un registro de información personal con datos sensibles como datos de salud puede estar valorado en alrededor de 200 dólares, con lo que podemos hacernos una idea del gran impacto de esta brecha de seguridad.

Desde entonces, se han venido sucediendo ataques en el sector, aunque de menor escala, y ello ha revelado la necesidad de contar con elementos de seguridad proactiva para proteger entornos tan críticos como los hospitalarios, donde los sistemas de información están detrás de la vida de pacientes.

El aumento del número de ataques en el sector está por encima de la media global y, combinado con los nuevos procesos de digitalización del sector salud que "expanden" la superficie de ataque, nos obligan a una fuerte inversión en herramientas, procesos y personas para ser capaces de movernos en este entorno tan cambiante y donde las amenazas existen y son reales. Porque la pregunta no es si seremos atacados, sino cuando lo seremos.

REFLEXIONES SOBRE EL FUTURO DE LA CIBERSEGURIDAD

A modo de conclusión, parece importante compartir unas breves reflexiones sobre el futuro de la ciberseguridad ya que, a pesar de los mensajes que se vienen dando, queda mucho por hacer en este ámbito.

Es fundamental que las compañías y los gobiernos dejen de ver la ciberseguridad como algo "improbable", "teórico" o simplemente de las "películas de ciencia ficción" y pasen a la acción lo antes posible. Es cierto que se han dado grandes pasos y cada vez hay mayor concienciación, pero es una realidad el que los ataques continúan ocurriendo y ya no quedan únicamente en el ámbito digital, sino que trascienden al físico. Por ello, es necesario que las compañías que no lo hayan hecho aún, definan un plan estratégico de ciberseguridad y que estos planes cuenten con el apoyo directo de la dirección tanto en medios humanos como materiales. A los gobiernos cabe pedirles también su apoyo tanto institucional como para, por ejemplo, las inversiones en ciberseguridad especialmente en aquellos sectores o compañías que necesitan, pero no pueden permitirse, inversiones en ciberseguridad. Por último, otro aspecto clave es el de la formación de profesionales cualificados en ciberseguridad ya que la escasez actual de personal es preocupante. Es necesario revertir la tendencia actual y ser capaces de cubrir las posiciones para profesionales de la ciberseguridad y que se incorporen a las compañías y entidades donde sean capaces de definir y ejecutar planes de ciberseguridad.

REFERENCIAS

[1] "Internet de las Cosas". Wikipedia, 24/04/2017. url: https://es.wikipedia.org/wiki/Internet_de_las_cosas

[2] "Informe Anual de Seguridad Nacional" , Servicio de Prensa de La Moncloa, Enero 2017. url: http://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/Documents/140217-Informe_Anual_de_Seguridad_Nacional_2016.pdf

[3] "Top 5 Risks in terms of Likelihood", World Economic Forum, Enero 2017. url: http://reports.weforum.org/global-risks-2017/the-matrix-of-top-5-risks-from-2007-to-2017/

[4] "Chinese Curb Cyberattacks on U.S. Interests, Report Finds". New York Times, 20/06/2016. url: https://www.nytimes.com/2016/06/21/us/politics/china-us-cyber-spying.html?_r=0

[5] "El virus que tomó control de mil máquinas y les ordenó autodestruirse". BBC, 11/10/2015. url: http://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet

[6] "The inside story of the biggest hack in history". CNN, 05/08/2015. url: http://money.cnn.com/2015/08/05/technology/aramco-hack/

[7] "Cyber-Attack Against Ukrainian Critical Infrastructure". ICS-CERT (Industrial Control Systems Cyber Emergency Response Team), US Department of Homeland Security. 25/02/2016. url: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

[8] "Cyber security: Attack of the health hackers". Financial Times, 21/12/2015. url: https://www.ft.com/content/f3cbda3e-a027-11e5-8613-08e211ea5317