NOTA DE ACTUALIDAD 17/2017

21 de noviembre de 2017

*Ana García y Felipe Mañanes*[*]

Ciberseguridad en la Unión Europea

## Nota de actualidad: Ciberseguridad en la Unión Europea

El presidente de la Comisión Europea Jean Claude Juncker reconoció que, a pesar de los avances realizados en los últimos tres años, Europa no está preparada para hacer frente a los ciberataques. La Comisión Europea y el Alto Representante han propuesto una serie de medidas para reforzar las estructuras de ciberseguridad de la UE.

La tecnología es cada vez más importante en la administración europea: al depender más de ella surgen nuevas amenazas. Varios datos demuestras esta afirmación: en 2016 el 80% de las empresas experimentaron al menos uno de estos ataques; el 86% de los europeos cree que el riesgo de convertirse en víctima del cibercrimen va en aumento, especialmente en sectores como transporte, energía, salud y finanzas; en algunos Estados miembro, el 50% de todos los delitos cometidos son delitos cibernéticos. Las cifras recientes muestran que las amenazas digitales están evolucionando rápidamente: los ataques de ransom-ware han aumentado en un 300% desde 2015; los impactos económicos se multiplicaron por cinco desde 2013 hasta 2017. Los ataques cibernéticos son las principales amenazas para la seguridad nacional, a pesar de esto, la conciencia y el conocimiento aún son insuficientes: el 69% de las empresas no comprende o no entiende su exposición a los riesgos cibernéticos.

Las propuestas para reforzar la seguridad incluyen el fortalecimiento de la Agencia de la Unión Europea para la Seguridad de las Redes y la Información (ENISA); la Comisión propone ahora transformar a ENISA en una Agencia de Seguridad Cibernética más sólida de la UE con un mandato permanente y con mayores recursos operativos. El objetivo principal de la Agencia es ayudar a los Estados miembro a aplicar las nuevas directivas para modernizar el marco de acción. También proponen la creación de un marco común para gestionar la ciberseguridad en toda la Unión. En este sentido, se hace hincapié en la colaboración entre países para lograr un alto grado de competitividad en la respuesta a los ciberataques: se debe aplicar el derecho internacional ante ellos, así como establecer una serie de normas que garanticen el comportamiento responsable de los Estados.

[*] Alumnos en prácticas de la Universidad Pontificia de Comillas

## Desarrollar la resistencia de la UE ante los ciberataques: una firme Agencia Europea de Ciberseguridad

La Agencia deberá amparar a los Estados miembro cuando estos tengan que lidiar con ciberataques. La UE necesita estructuras más sólidas y eficaces, la comunicación conjunta sugiere nuevas iniciativas para mejorar aún más la ciber resistencia y la respuesta de la UE en tres áreas clave:

- Desarrollar la resistencia de la UE a los ciberataques y aumentar la capacidad de ciberseguridad de la UE.
- Crear una respuesta efectiva del derecho penal.
- Fortalecimiento de la estabilidad global a través de la cooperación internacional.

Por lo tanto, la Comisión y el Alto Representante proponen reforzar la resiliencia, la disuasión y la respuesta de la UE a los ciberataques mediante:

- Establecimiento de una Agencia de Ciberseguridad de la Unión Europea más sólida, basada en la Agencia para la Seguridad de las Redes y la Información (ENISA), para ayudar a los Estados miembro a abordar los ciberataques.
- Creación de un esquema de certificación de ciberseguridad en toda la UE que aumente la ciberseguridad de los productos y servicios en el mundo digital.
- Un plan detallado de cómo responder de manera rápida, operativa y al unísono cuando ocurre un ciberataque a gran escala.
- Una red de centros de competencia en los Estados miembro y un Centro Europeo de Investigación y Competencia en Ciberseguridad, que ayudará a desarrollar y desplegar las herramientas y la tecnología necesarias para mantenerse al día con una amenaza en constante cambio y garantizar que nuestra defensa sea lo más fuerte posible.
- Una nueva Directiva sobre la lucha contra el fraude y la falsificación de los medios de pago distintos del efectivo para proporcionar una respuesta más eficaz del Derecho penal al delito cibernético.
- Un marco para una respuesta diplomática conjunta de la UE a actividades cibernéticas maliciosas y medidas para reforzar la cooperación internacional en ciberseguridad, incluida la profundización de la cooperación entre la UE y la OTAN.
- El objetivo de impulsar el desarrollo de habilidades de alto nivel para los profesionales civiles y militares a través de la provisión de soluciones para los esfuerzos nacionales y la creación de una plataforma educativa y de capacitación en defensa cibernética.

La gestión de crisis involucrará a actores a nivel de los Estados miembro y de Europa. Las autoridades nacionales competentes y los puntos únicos de contacto establecidos por la Directiva NEI, los equipos de respuesta a incidentes de seguridad informática (CSIRT) y las agencias de seguridad cibernética participarán en los Estados miembro. ENISA y Europol/EC3 (el Centro Europeo de Ciberdelincuencia de Europol), la Comisión Europea, el Servicio Europeo de Acción Exterior y, en particular, sus servicios encargados de la gestión de crisis, así como el Consejo participarán a nivel europeo. Estos organismos cooperarán juntos a nivel técnico, operativo y estratégico.

Dada la naturaleza global de la amenaza, construir y mantener alianzas sólidas y asociaciones con terceros países es fundamental para la prevención y disuasión de los ciberataques, que son cada vez más fundamentales para la estabilidad y la seguridad internacionales. La UE ha desarrollado diálogos cibernéticos específicos con EE.UU., Japón, India, Corea del Sur y China. También se han celebrado consultas estrechas con organizaciones internacionales, como la OTAN, el Foro Regional de la ASEAN, la OSCE, el Consejo de Europa y la OCDE.

Además, en base al progreso reciente, la UE reforzará su cooperación con la OTAN en ciberseguridad, amenazas híbridas y defensa, como se prevé en la Declaración conjunta de 8 de julio de 2016. Los dos socios también intensificarán el intercambio de información entre sus respectivos órganos de ciberseguridad, es decir, Equipo de respuesta ante emergencias informáticas para las instituciones de la UE (CERT-UE) y la capacidad de respuesta a incidentes informáticos de la OTAN (NCIRC). Otra acción clave será su participación común en ejercicios paralelos y coordinados y una mejor interoperabilidad de los estándares de ciberseguridad. Por primera vez en 2017 y 2018, la OTAN y la UE llevarán a cabo ejercicios paralelos y coordinados en respuesta a un escenario híbrido.

## Marco de certificación de ciberseguridad de la UE

La Comisión propone la creación de un marco europeo de certificación de ciberseguridad que se espera que ofrezca numerosos sistemas europeos de certificación de ciberseguridad individual, es decir, descripciones claras de los requisitos de seguridad que deben cumplir los productos, sistemas o servicios. Cumplir los nuevos requisitos, lo que facilita a las empresas el comercio transfronterizo y que los compradores comprendan las características de seguridad de los productos o servicios. Los ciudadanos y los usuarios finales de los productos, los proveedores de productos y los gobiernos nacionales serán los beneficiados del marco de certificación.

Con el fin de ampliar la respuesta de la UE contra los ciberataques, la Comisión ha propuesto:

- Una Agencia de Ciberseguridad de la Unión Europea: con un fuerte mandato, un estado permanente, recursos adecuados.
- Un marco de certificación de ciberseguridad de la UE: la certificación desempeña un papel fundamental para aumentar la confianza y la seguridad en los productos y servicios que son cruciales para el mercado único digital. Sin un marco común para los esquemas de certificados de ciberseguridad válidos en toda la UE, existe un riesgo creciente de fragmentación y barreras en el mercado único.
- ENISA implementará este proceso de certificación que refrendará que los productos y servicios TIC están certificados y cumplen con los requisitos de ciberseguridad.

El uso del marco de certificación no es obligatorio a menos que esté prescrito en la futura legislación de la UE, sin embargo, habrá un incentivo para certificar la calidad y seguridad.

Existen algunos esquemas de certificación existentes en la UE, tales como el Commercial Product Assurance (CPA), desarrollado en el Reino Unido, la Certificaction Sécuritaire de Premier Niveau (CSPN), en Francia, Dutch Baseline Security Product Assessment (BSPA), en los Países Bajos, y uno donde no puede ser un reconocimiento mutuo entre los miembros SOG-IS MRA que incluye 12 Estados miembro incluyendo a Noruega.

## Abordar el fraude de pagos que no se realizan en efectivo

El fraude de pago no en efectivo puede tomar diferentes formas. Los delincuentes pueden desencadenar la ejecución de pagos utilizando la información del pagador obtenida a través de, por ejemplo, suplantación de identidad, robo u obtención de información en sitios web dedicados que venden credenciales de tarjetas de crédito robadas en la red oscura (deep web). Los pagos también pueden ejecutarse fraudulentamente mediante tarjetas falsificadas o robadas, utilizadas para pagar en tiendas o retirar efectivo en cajeros automáticos o mediante el pirateo de sistemas de información para procesar pagos, por ejemplo, alterando los puntos de venta para transacciones con tarjeta o aumentando ilegalmente los límites de la tarjeta de crédito que permita que los gastos excedentes no sean detectados.

La normativa actual no refleja las realidades del momento y no será suficiente para abordar los nuevos desafíos y desarrollos tecnológicos tales como monedas virtuales y pagos a través del móvil. La nueva Directiva para combatir el fraude y la falsificación de los medios de pago que

no sean en efectivo sustituye a la actual Decisión marco del Consejo y proporciona una respuesta eficaz de ciberdelincuencia y penal de la UE a través de:

- Actualizar el marco legal.
- Eliminar obstáculos operacionales.
- Mejora la prevención.

Además, permitirá a los Estados miembro disuadir y enjuiciar efectivamente tales delitos cibernéticos mediante:

- Expansión del alcance de los delitos, incluidas las transacciones a través de monedas virtuales.
- Introducción de nuevos delitos en línea.
- Introducción del nivel mínimo para las penas más altas de 2 a 5 años.
- Aclaración del alcance de la jurisdicción.
- Garantía de los derechos de las víctimas del delito cibernético.
- Mejora de la cooperación en materia de justicia penal en toda la UE.
- Proporción de datos estadísticos sobre el fraude.