Estado de la Unión 2017 – Ciberseguridad: la Comisión intensifica la respuesta de la UE a los ciberataques

Bruselas, 19 de septiembre de 2017

.

El 13 de septiembre, en su discurso anual sobre el Estado de la Unión, el presidente de la Comisión, **Jean-Claude Juncker**, ha declarado lo siguiente: «*En los tres últimos años, hemos realizado progresos en lo que respecta a la seguridad de los europeos en línea. Pero Europa sigue sin estar adecuadamente equipada para defenderse de los ciberataques. Por ese motivo, la Comisión propone hoy nuevas herramientas, entre las que figura la Agencia Europea de Ciberseguridad, que nos ayuden a repeler esos ataques.*»

Los ciudadanos europeos depositan una gran confianza en las tecnologías digitales. Estas brindan nuevas oportunidades para que los ciudadanos estén conectados, facilitan la difusión de información y constituyen la columna vertebral de la economía de Europa. Sin embargo, también han traído consigo nuevos riesgos a medida que ciertos agentes, tanto estatales como no estatales, han multiplicado sus tentativas de robar datos, cometer fraudes e incluso desestabilizar gobiernos. El año pasado se produjeron más de 4 000 ataques con programas de secuestro de archivos al día y el 80 % de las empresas europeas se vio afectado por al menos un incidente de ciberseguridad. El impacto económico de la ciberdelincuencia se ha multiplicado por cinco en los últimos cuatro años.

A fin de dotar a Europa de las herramientas adecuadas para hacer frente a los ciberataques, la Comisión Europea y la alta representante proponen un amplio conjunto de medidas para fortalecer la ciberseguridad en la UE. Entre ellas figura la propuesta de una nueva **Agencia Europea de Ciberseguridad** que ayude a los Estados miembros en la lucha contra los ciberataques, así como un nuevo **régimen europeo de certificación** que garantice un uso seguro de los productos y servicios en el mundo digital.

Federica **Mogherini**, alta representante y vicepresidenta, ha declarado: «*La UE seguirá trabajando en pos de una ciberpolítica internacional que fomente un ciberespacio abierto, libre y seguro, y apoyará los esfuerzos por elaborar normas de conducta responsable por parte de los Estados y aplicar el Derecho internacional y medidas de fomento de la confianza en materia de ciberseguridad.*»

Andrus **Ansip**, vicepresidente responsable del Mercado Único Digital, ha declarado lo siguiente: «*Ningún país puede hacer frente, por sí solo, a los retos de ciberseguridad. Nuestras iniciativas refuerzan la cooperación de forma que los Estados miembros de la UE puedan acometer juntos estos desafíos. Proponemos también nuevas medidas que potencien la innovación y fomenten la «ciberhigiene».*»

Julian **King**, comisario de la Unión de la Seguridad, ha declarado: «*Hemos de trabajar codo a codo para desarrollar resiliencia, impulsar la innovación tecnológica, potenciar la disuasión, reforzar la rastreabilidad y la obligación de rendir cuentas y encauzar la cooperación internacional hacia el fomento de nuestra ciberseguridad colectiva.*»

Mariya **Gabriel**, comisaria de Economía y Sociedad Digitales, ha declarado: «*Tenemos que afianzar la confianza de los ciudadanos y las empresas en el mundo digital, especialmente en estos tiempos en los que los ciberataques a gran escala son cada vez más comunes. Es mi deseo que la existencia de estándares elevados de ciberseguridad se convierta en la nueva ventaja competitiva de nuestras empresas.*»

Habida cuenta de los recientes ataques con programas de secuestro de archivos, el aumento drástico de la ciberdelincuencia, el creciente uso de ciberherramientas por agentes estatales para sus fines

geopolíticos y la diversificación de los incidentes de ciberseguridad, la UE necesita robustecer su resiliencia ante los ciberataques y desarrollar una estrategia de ciberdisuasión a escala de la UE y una respuesta del Derecho penal efectivas a fin de proteger mejor a los ciudadanos, las empresas y las instituciones públicas de Europa. De esto trata el paquete de ciberseguridad anunciado hoy.

Desarrollo de la resiliencia de la UE: una Agencia Europea de Ciberseguridad fuerte

La Agencia Europea de Ciberseguridad: basada en la actual Agencia de Seguridad de las Redes y de la Información de la Unión Europea (ENISA), recibirá un mandato permanente para ayudar a los Estados miembros a prevenir y responder con eficacia a los ciberataques; mejorará la capacidad de reacción de la UE mediante la organización anual de **ejercicios paneuropeos de ciberseguridad** y la mejor **puesta en común de la información y la inteligencia sobre las amenazas** a través de la creación de centros de intercambio de información y análisis; y contribuirá a la aplicación de la **Directiva sobre la seguridad de las redes y sistemas de información**, que contiene obligaciones de notificación a las autoridades nacionales en caso de incidentes graves.

Asimismo, la Agencia de Ciberseguridad ayudaría a establecer y aplicar el **marco de certificación a escala de la UE** que propone la Comisión para garantizar que los **productos y servicios sean «ciberseguros»**. Del mismo modo que los consumidores pueden confiar en lo que comen gracias al etiquetado de alimentos de la UE, los nuevos certificados europeos de ciberseguridad asegurarán la fiabilidad de miles de millones de dispositivos («internet de las cosas») con los que se manejan infraestructuras fundamentales de nuestro tiempo, como las redes de energía y transporte, pero también de nuevos dispositivos destinados a los consumidores, como los automóviles conectados. Los certificados de ciberseguridad serán reconocidos en todos los Estados miembros, con lo que se reducirán los trámites administrativos y los costes[1] para las empresas.

Refuerzo de la capacidad de la UE en materia de ciberseguridad

Redunda en el interés estratégico de la UE velar por que las herramientas tecnológicas de ciberseguridad se desarrollen de forma que la economía digital pueda prosperar, protegiendo al mismo tiempo nuestra seguridad, nuestra sociedad y nuestra democracia. Ello incluye la protección de elementos de *hardware* y *software* esenciales. A fin de reforzar la capacidad de la UE en materia de ciberseguridad, la Comisión y la alta representante proponen:

- **Un Centro europeo de investigación y competencias en materia de ciberseguridad** (proyecto piloto que se pondrá en marcha en 2018). En colaboración con los Estados miembros, este centro ayudará a desarrollar y desplegar las herramientas y tecnologías necesarias para hacer frente a una amenaza en constante cambio y a velar por que nuestras defensas sean tan punteras como las armas que utilizan los ciberdelincuentes. También complementará los esfuerzos de desarrollo de capacidades en este ámbito a escala nacional y de la UE.
- **Un Plan rector para que Europa y los Estados miembros puedan responder rápidamente**, con operatividad y al unísono cuando se produzca un ciberataque a gran escala. El procedimiento propuesto se establece en una Recomendación adoptada la semana pasada. Asimismo, esta Recomendación pide a los Estados miembros y a las instituciones de la UE que definan un marco de respuesta a las crisis de ciberseguridad de la UE para que el Plan rector sea operativo. Posteriormente, se pondrá a prueba periódicamente en ejercicios de gestión de crisis, tanto cibernéticas como de otros tipos.
- **Mayor solidaridad**. Más adelante, se podría estudiar la posibilidad de crear un Fondo de Respuesta en casos de Emergencia de Ciberseguridad para aquellos Estados miembros que hubiesen puesto en marcha de forma diligente todas las medidas de ciberseguridad exigidas por el Derecho de la UE. El Fondo podría facilitar ayuda de emergencia a los Estados miembros, del mismo modo que el Mecanismo de Protección Civil de la UE se moviliza para ofrecer apoyo en los casos de incendios forestales o catástrofes naturales.
- **Capacidades de ciberdefensa más sólidas**. Se anima a los Estados miembros a incluir la ciberdefensa en el marco de la cooperación estructurada permanente y el Fondo Europeo de Defensa, con el fin de apoyar los proyectos en materia de ciberdefensa. En el diseño del Centro europeo de investigación y competencias en materia de ciberseguridad, podría contemplarse añadir una dimensión de ciberdefensa. Para resolver el déficit de competencias en la materia, la UE creará en 2018 una plataforma de formación y educación en ciberdefensa. La UE y la OTAN fomentarán de forma conjunta la cooperación en materia de investigación e innovación sobre ciberdefensa. Se reforzará la cooperación con la OTAN, especialmente la participación en ejercicios paralelos y coordinados.
- **Aumento de la cooperación internacional**: la UE endurecerá su respuesta a los ciberataques

mediante la aplicación del Marco para una respuesta diplomática conjunta de la UE a las actividades informáticas malintencionadas, marco estratégico de prevención de conflictos y aumento de la estabilidad en el ciberespacio. Esta iniciativa irá acompañada de nuevos esfuerzos de ampliación de la cibercapacidad para ayudar a los terceros países a hacer frente a las ciberamenazas.

Desarrollo de una respuesta de Derecho penal eficaz

Para desincentivar efectivamente la comisión de este tipo de delitos, es fundamental que la respuesta policial y judicial sea más eficaz y se centre en la detección, el rastreo y la persecución de los ciberdelincuentes. La Comisión propone, por tanto, reforzar la disuasión con nuevas medidas de **lucha contra el fraude y la falsificación de los medios de pago distintos del efectivo**.

La propuesta de **Directiva** reforzará la capacidad de las autoridades judiciales y policiales para luchar contra esta forma de delincuencia **ampliando el alcance de las infracciones** relativas a los sistemas de información a todas las operaciones de pago, incluidas las operaciones con monedas virtuales. Este acto jurídico también introducirá **normas comunes en relación con las sanciones aplicables** y aclarará **a qué supuestos se extiende la jurisdicción de los Estados miembros** en este tipo de infracciones.

Con el fin de potenciar la investigación y el enjuiciamiento efectivos de la delincuencia favorecida por el entorno cibernético, la Comisión también presentará propuestas a principios de 2018 para facilitar el acceso transfronterizo a las **pruebas electrónicas**. Por otro lado, la Comisión presentará en octubre sus reflexiones sobre la importancia del **cifrado** en las investigaciones penales.

Antecedentes

Según cifras recientes, las amenazas digitales evolucionan con rapidez y los ciudadanos perciben la ciberdelincuencia como un grave peligro: los ataques con programas de secuestro de archivos han aumentado un 300 % desde 2015 y el impacto económico de la ciberdelincuencia se ha multiplicado por cinco entre 2013 y 2017, y todavía podría cuadruplicarse de aquí a 2019, según los estudios. El 87 % de los europeos consideran la ciberdelincuencia como un importante desafío para la seguridad interior de la UE.

La Agenda Europea de Seguridad y la revisión intermedia de la Estrategia para el Mercado Único Digital guían la actividad de la Comisión en este ámbito, ya que exponen las principales medidas de refuerzo de la ciberseguridad. Las medidas que hoy se proponen complementan las normas en vigor y colman los resquicios que la evolución de la amenaza ha abierto desde la adopción de la Estrategia de Ciberseguridad de la UE de 2013, atendiendo con ello la prioridad esencial de garantizar la seguridad interior con arreglo a la Declaración y la Hoja de Ruta de Bratislava.

Para más información

Preguntas y respuestas – Estado de la Unión 2017 – Ciberseguridad: la Comisión intensifica su respuesta a los ciberataques

Ficha informativa sobre propuestas en materia de ciberseguridad

Ficha informativa sobre la Agencia Europea de Ciberseguridad

Ficha informativa sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo

Documentos adoptados el 13 de septiembre

[1] El coste de la certificación de los contadores inteligentes en el Reino Unido y Francia, por ejemplo, ronda los 150 000 EUR.

IP/17/3193

Personas de contacto para la prensa:

Natasha BERTAUD (+32 2 296 74 56)
Nathalie VANDYSTADT (+32 2 296 70 83)
Tove ERNST (+32 2 298 67 64)
Maja KOCIJANCIC (+32 2 298 65 70)
Inga HOGLUND (+32 2 295 06 98)

Solicitudes del público en general: Europe Direct por teléfono 00 800 67 89 10 11 , o por e-mail

Attachments

20170919-cybersecurity factsheet non-cash payments-en.pdf
Cybersecurity-EU agency and certification framework.en.pdf
Cybersecurity.en.pdf