European Commission

ESTADO DE LA UNIÓN 2017

CIBERSEGURIDAD

"Los ciberataques pueden ser más peligrosos para la estabilidad de las democracias y las economías que las pistolas y los tanques. […] Los ciberataques no conocen fronteras y nadie es inmune. Por ello, hoy la Comisión propone nuevas herramientas, incluyendo una Agencia Europea de Ciberseguridad, para ayudarnos a defendernos contra esos ataques."

Presidente de la Comisión Europea Jean-Claude Juncker, Estado de la Unión Europea, 13 Sept. 2017

Resiliencia, disuasión y defensa: Construyendo una fuerte ciberseguridad en Europa

La Comisión Europea y la Alta Representante han propuesto una amplia gama de medidas concretas que reforzarán las estructuras y capacidades de ciberseguridad de la UE con una mayor cooperación entre los Estados Miembros y las diferentes estructuras de la UE. Estas medidas garantizarán que la UE esté mejor preparada para hacer frente a los, cada vez mayores, problemas de ciberseguridad.

Los ciudadanos europeos y las empresas dependen de los servicios y tecnologías digitales:

Los europeos creen que las tecnologías digitales tienen un impacto positivo en[1]:

75% Nuestra economía

64% Nuestra sociedad

67% Nuestra calidad de vida

86% de los europeos creen que el riesgo de convertirse en víctima de la ciberdelincuencia está aumentando.[2]

Sectores como el transporte, la energía, la salud y las finanzas se han vuelto cada vez más dependientes de la red y los sistemas de información para dirigir sus negocios

El Internet de las Cosas (IoT) es ya una realidad. Habrá decenas de miles de millones de dispositivos digitales conectados en la UE en 2020.[3]

Los ciberataques están en aumento:

+4,000 ataques ransomware por día en 2016.

En algunos Estados Miembros el 50% de todos los delitos cometidos son ciberdelitos.

Los incidentes de seguridad aumentaron un 38% en 2015, el mayor incremento en los últimos 12 años.

80% de compañías europeas sufrieron, al menos, un ciberincidente el pasado año.[4]

+150 países y +230,000 sistemas de los distintos sectores y países se vieron afectados con un impacto sustancial en los servicios esenciales conectados a Internet, incluyendo hospitales y ambulancias

La magnitud del problema hace necesario actuar a nivel europeo. Las cifras recientes muestran que las amenazas digitales están evolucionando rápidamente: los ataques de ransomware han aumentado en un 300% desde 2015. Según varios estudios, el impacto económico de la ciberdelincuencia se quintuplicó de 2013 a 2017, y podría aumentar aún más en un factor de cuatro para 2019.[5] Las evidencias sugieren que personas de todo el mundo identifican los ciberataques de otros países entre las principales amenazas a la seguridad nacional.

Además, a raíz de los ataques de "Wannacry" y "(Non) Petya", un informe reciente ha estimado que un ciberataque grave podría costar a la economía mundial más de 100.000 millones de euros.

Concienciación y formación

A pesar de la creciente amenaza, la concienciación y la formación de las cuestiones de ciberseguridad siguen siendo insuficiente

69% de las compañías

no tienen ni un conocimiento básico de su exposición a los riesgos cibernéticos

60% de las compañías

nunca han estimado la posibles pérdidas financieras de un gran ciberataque[6]

51% de los ciudadanos

Europeos no se sienten bien informados sobre las ciberamenazas[7]

LA RESILIENCIA DE LA UE A LOS CIBERATAQUES

La UE necesita estructuras más sólidas y eficaces para garantizar una fuerte resiliencia, promover la ciberseguridad y responder a los ciberataques dirigidos a los Estados Miembros y a las propias instituciones, agencias y organismos de la UE. También necesita una ciberseguridad fuerte para su Mercado Único, importantes avances en la capacidad tecnológica de la UE y una comprensión más amplia del papel de todos en la lucha contra las ciberamenazas. Como respuesta a esto, la Comunicación conjunta sugiere nuevas iniciativas para seguir mejorando la resiliencia y respuesta de la UE en tres áreas clave:

- Construyendo una UE resiliente a ciberataques y reforzando las capacidades de ciberseguridad de la UE
- Creando una respuesta efectiva del derecho penal
- Fortaleciendo la estabilidad mundial mediante la cooperación internacional

Por tanto, la Comisión y la Alta Representante proponen reforzar la capacidad de resiliencia, la disuasión y la respuesta de la UE mediante:

- El establecimiento de una Agencia Europea de Ciberseguridad más sólida basada en la Agencia para la Seguridad de las Redes y la Información (ENISA), para asistir a los Estados Miembros a hacer frente a los ciberataques.
- Creando un sistema de certificación de ciberseguridad a nivel de la UE que incremente la ciberseguridad de productos y servicios en el mundo digital.
- Un plan (Blueprint) para responder rápida, operativamente y al unísono cuando ocurra un ciberataque a gran escala.
- Una red de centros competentes en los Estados miembros y un Centro Europeo de Investigación y Competencia en Ciberseguridad que ayudará a desarrollar y difundir las herramientas y la tecnología necesarias para mantenerse al día con una amenaza constante y asegurarse de que nuestra defensa sea lo más fuerte posible.
- Una nueva Directiva para combatir relativa a la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo para prever una respuesta penal más eficaz a los ciberdelitos.
- Un marco para una respuesta diplomática conjunta de la UE a actividades cibernéticas maliciosas y medidas para reforzar la cooperación internacional en materia de ciberseguridad, incluyendo avanzar en la cooperación entre la UE y la OTAN
- La UE pretende impulsar el desarrollo de competencias 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 de entrenamiento para la ciberdefensa y para la educación.

1 *Attitudes towards the impact of digitisation and automation on daily life,* Eurobarometer, 2017.
2 Eurobarometer on Cybersecurity (EBS 464).
3 *Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination*, IDC and TXT, study carried out for the European Commission, 2014.
4 PWC, Global State of Information Security Survey, 2016 and http://news.sap.com/pwc-study-biggest-increase-in-cyberattacks-in-over-10-years/.
5 *How to protect your networks from ransomware*, CCIPS, 2016 https://www.justice.gov/criminal-ccips/file/872771/download.
6 *Continental European Cyber Risk Survey* 2016 Report.