APM 3.9.

Publicación digital. - Asociación Profesional de la Magistratura

María Luisa Gil Meana

Ex Magistrada de TSJM

CIBERSEGURIDAD Y UNIÓN EUROPEA

Se define la Ciberseguridad como la práctica de proteger los sistemas más importantes y la información confidencial ante ataques digitales. También es conocida como seguridad de la tecnología de la formación (TI). Las ciber amenazas más comunes son los programas maliciosos que se refieren a variantes del software malicioso como virus, troyanos y spyware que proporcionan acceso no autorizado o causan daños a un sistema y son cada vez más "sin archivos" y diseñados para eludir los métodos más comunes de detección. Ransomware es un tipo de programa malicioso que, últimamente, se ha dirigido a gobiernos estatales y locales bloqueando archivos, datos o sistemas y amenaza con borrarlos o destruirlos o con publicar datos privados o confidenciales a menos que se pague un rescate a los ciber delincuentes responsables. Phishing es una forma de ingeniería social, consiste en engañar a los usuarios para que proporcionen su propia PII o información confidencial, como datos de tarjeta de crédito o información de inicio de sesión. Los ataques de denegación de servicio distribuido (DDos) tienen como finalidad hacer caer un servidor, un sitio web o una red sobrecargándola con tráfico, generalmente, desde varios sistemas coordinados. Las amenazas persistentes avanzadas (APT) suponen que las personas que hacen el ciberataque se infiltran en un sistema y permanecen sin ser detectadas durante un largo periodo de tiempo en las redes y sistemas, la finalidad es poder expiar la actividad empresarial y robar datos confidenciales. El llamado ataque intermediario (Man -in-the-middle) es un ataque de escuchas no autorizadas donde un delincuente intercepta y retransmite mensajes entre dos partes para robar datos de, por ejemplo, una red wi-fi no segura.

Ante esta situación en diciembre de 2020, la Comisión Europea y el Servicio Europeo de Acción Exterior (SEAE) presentaron una nueva Estrategia de Ciberseguridad de la UE. Su objetivo es reforzar la resiliencia de Europa frente a las ciber amenazas y garantizar que todos los ciudadanos y empresas puedan beneficiarse plenamente de servicios y herramientas digitales seguros y fiables. Así pues, la ciberseguridad incluye las actividades necesarias para la protección de las redes y sistemas de información, de los usuarios de tales sistemas y de quienes se vean afectados por las ciber amenazas.

El 22 de marzo de 2021, el Consejo de Europa adoptó unas Conclusiones sobre la Estrategia de Ciberseguridad en las que destacó que la misma es esencial para construir una Europa resiliente, ecológica y digital. Los ministros de la UE fijaron como objetivo clave lograr la autonomía estratégica preservando al mismo tiempo una economía abierta. Para ello, es necesario aumentar la capacidad de adoptar decisiones autónomas en el ámbito de la ciberseguridad a fin de reforzar el liderazgo digital y las capacidades estratégicas de la UE.

Por otra parte, el Reglamento sobre la Ciberseguridad de la UE, que entró en vigor en junio de 2019, estableció:

-un sistema de certificación para toda la UE,

-un mandato nuevo y reforzado de la Agencia de la UE para la Ciberseguridad.

-Reglamento sobre la Ciberseguridad de la UE (Comisión Europea)

-Sistema de certificación de la ciberseguridad a escala de la UE

Hay que tener en cuenta que la certificación es fundamental a la hora de garantizar unas normas rigurosas en materia de ciberseguridad para los productos, servicios y procesos de TIC. El hecho de que diferentes países de la Unión recurrieran a diferentes sistemas de certificación de la seguridad provocaba una fragmentación del mercado y generaba barreras reglamentarias. Gracias al Reglamento sobre la Ciberseguridad, la UE ha implantado un marco único de certificación a escala de toda ella que genera confianza, aumenta el crecimiento del mercado de la ciberseguridad y facilita el comercio en toda la UE. El marco proporciona un conjunto completo de reglas, requisitos técnicos, normas y procedimientos.

La Directiva sobre la seguridad de las redes y sistemas de información (SRI), adoptada en 2016, fue la primera medida legislativa a escala de la Unión destinada a estrechar la cooperación entre los Estados miembros en lo relativo a la ciberseguridad. En ella se establecieron obligaciones de

seguridad para los operadores de servicios esenciales (en sectores vitales como la energía, el transporte, la sanidad y las finanzas) y los proveedores de servicios digitales (mercados en línea, motores de búsqueda y servicios en la nube).

Fue en 2022 cuando la UE adoptó una revisión de la Directiva SRI (SRI 2) para sustituir a la Directiva de 2016. Las nuevas normas garantizan un elevado nivel común de ciberseguridad en toda la Unión, respondiendo a la evolución del panorama de las amenazas y teniendo en cuenta la transformación digital, que se ha visto acelerada por la pandemia de COVID-19. Así, define nuevas normas mínimas relativas a un marco regulador, establece mecanismos para una cooperación eficaz entre las autoridades competentes de cada Estado miembro y actualiza la lista de sectores y actividades sujetos a las obligaciones de ciberseguridad.

La Directiva SRI 2 entró en vigor el 16 de enero de 2023.

El 18 de abril de 2023, la Comisión propuso una modificación específica de la Ley de Ciberseguridad de la UE La modificación propuesta permitirá la futura adopción de sistemas de certificación europeos para los «servicios de seguridad gestionados» que abarquen ámbitos como la respuesta a incidentes, las pruebas de penetración, las auditorías de seguridad y la consultoría. También con esa fecha la Comisión europea propuso la Ley de Ciber solidaridad de la UE para mejorar la preparación, la detección y la respuesta a los incidentes de ciberseguridad en toda la UE.

Cabe decir también que, el aumento del teletrabajo, el fenómeno de dispositivos conectados, la consolidación tecnológica y la mayor digitalización en sectores más tradicionales han fomentado un masivo ataque, sin precedentes, tanto nivel corporativo como doméstico con los dispositivos digitales, por ello el 15 de septiembre de 2022 la Comisión Europea presentó una propuesta innovadora a nivel mundial para mejorar la seguridad de los dispositivos de hardware .y software . Se trata de la ley de Ciber resiliencia Europea que tiene como objetivo proteger a empresas y usuarios de productos con características digitales que no cumplan con los requisitos de ciberseguridad. Las medidas que se contemplan en dicha ley están aún en proceso de revisión y debate.

Por otra parte, teniendo en cuenta que la ciberdelincuencia adopta diversas formas y el ámbito cibernético facilita numerosos delitos comunes, se ha creado en Europol un Centro Europeo de Ciberdelincuencia para ayudar a los países de la Unión a investigar los delitos en línea y desmantelar las redes delictivas.