

El director ejecutivo de la Agencia de la Unión Europea para la seguridad de las redes y de la información (ENISA) habla en la conferencia del PE sobre un enfoque equilibrado respecto a la privacidad en línea, así como de un sector europeo de las TIC fiable.

En la conferencia de alto nivel del Parlamento Europeo en Bruselas, Udo Helmbrecht, director ejecutivo de ENISA, comentó: «El desafío de los políticos es lograr un enfoque equilibrado respecto a la privacidad, con los menores efectos adversos posibles sobre los intereses de los ciudadanos y el sector empresarial». La conferencia, organizada junto con la Comisión de Libertades Civiles, Justicia y Asuntos de Interior (LIBE) y la Presidencia de Luxemburgo del Consejo de la UE, y copresidida por las Comisiones IMCO e ITRE, se centró en la protección de la privacidad en línea mediante la mejora de la seguridad informática y el refuerzo de las funciones de la TI en la UE.

ENISA acogió favorablemente el debate de cada uno de los ámbitos políticos centrados en estimular la adopción de las tecnologías de protección de la intimidad (PET), en abordar las vulnerabilidades del software y el hardware y la infraestructura de Internet, así como en desarrollar el potencial de la UE para una industria de la TI robusta y vital. ENISA espera que la conferencia tenga un efecto estimulante en el debate político sobre estas políticas estrechamente vinculadas.

Las PET, la estandarización y la certificación son básicas para la industria de la TI

El uso de las PET, como la «privacidad mediante el diseño», es parte de la funcionalidad de la TI que permite ofrecer una protección a la intimidad compatible y que se basa en elementos de seguridad estándares, por lo que se promueve que se apliquen por defecto. Asimismo, las directrices de la UE que abordan el desarrollo de software y hardware seguro, como la estandarización y la certificación, que ENISA también desarrolla, pueden promocionarse y aplicarse en la UE como una forma de hacer frente a las vulnerabilidades.

La implantación del «Internet de las cosas» (IoT) es un ejemplo que demuestra su importancia creciente, ya que supone problemas de seguridad que pueden mitigarse en parte desde la perspectiva de la resiliencia de la red. Sin embargo, la interacción del IoT con componentes de hardware y software representa más riesgos y amenazas. En este sentido, algunos componentes de la arquitectura de Internet desempeñan un papel fundamental. Así pues, es importante establecer protocolos para compartir información sobre incidentes y vulnerabilidades, así como un diálogo entre los agentes que contribuyen a crear un enfoque común sobre la seguridad.

Respecto a afrontar la importancia de la infraestructura de la TI de la UE, los Estados miembros han desarrollado medidas específicas para protegerla. El **nuevo texto acordado** de la directiva NIS supone un avance hacia un enfoque y cooperación más coordinados entre todos los agentes y sectores, que haga frente a la seguridad de la infraestructura digital (ya sea energética, sanitaria, de transporte o finanzas) para garantizar un elevado nivel de seguridad de los sistemas esenciales, la infraestructura y los ciudadanos. ENISA cuenta con una dilatada experiencia en todas estas áreas. Gracias a este conocimiento, se han desarrollado buenos mecanismos de cooperación (a través de los CSIRT y los ejercicios de la serie Ciber Europa), que permiten a las autoridades competentes y al sector privado responder conjuntamente a

los incidentes (artículo 13a, TSP)¹. «Esperamos seguir mejorando y reforzando nuestra colaboración en esta dirección», comentó Helmbrecht.

ENISA subraya el valor añadido del mercado de la ciberseguridad

En el debate se destacó el valor que aporta la ciberseguridad, que podría suponer 640 mil millones² de euros para la economía de la UE. El mercado de la ciberseguridad en la UE está poco desarrollado, con un valor estimado de 20 mil millones de euros y un crecimiento del 6 % TCAC³. Lo que es importante es que la UE establezca la ciberconfianza entre los ciudadanos y la industria para crear una UE competitiva basada en el sector de las TIC, reforzando así la posición de la UE.

Para saber más y realizar consultas relacionadas con la prensa, póngase en contacto con:

press@enisa.europa.eu, Tel.+30 2814 409576

Para saber más sobre la reunión del PE, puede visitar los siguientes enlaces:

<http://www.europarl.europa.eu/committees/en/libe/events.html?id=20151208CHE00191>

<http://www.stoa.europarl.europa.eu/stoa/cms/home/events/workshops/privacy>

¹ TSP (Trust Service Providers o proveedores de servicios de confianza). ENISA propone **un nuevo plan de información para los TSP**. Artículo 13a: el artículo 13a de la Directiva 2009/140 CE es parte del paquete de telecomunicaciones y pretende garantizar la seguridad e integridad de las redes y servicios de comunicación electrónica (telecom). En este área, ENISA tiene la responsabilidad de recopilar incidentes y acciones llevadas a cabo por los sectores de la telecomunicación en los Estados miembros, y contribuir a la «armonización de las medidas de seguridad técnicas y organizativas apropiadas proporcionando su asesoramiento», además de «promover el intercambio de las mejores prácticas».

² Riesgo y responsabilidad en un mundo hiperconectado –Foro Económico Mundial

³ El tamaño del mercado de la ciberseguridad en Europa, Gartner 2013