Un aumento significativo de las ciberamenazas a los servicios e infraestructuras básicas exige una mayor cooperación entre los principales interesados de los sectores público y privado.

En su estudio sobre las infraestructuras básicas de la información (CII por sus siglas en inglés), ENISA analiza las prácticas actuales de protección de infraestructuras básicas de la información (CIIP por sus siglas en inglés) y los modelos de gestión implementados en los Estados miembros. Este estudio contribuye a la divulgación y próxima aplicación de la Directiva NIS.

Los ciudadanos y las empresas dependen de las infraestructuras de la información y de la comunicación para dar apoyo a los servicios básicos en línea (por ejemplo, energía, telecomunicaciones, sanidad). El aumento de las ciberamenazas puede afectar considerablemente la prestación de servicios y conllevar la pérdida de dinero y daños a la reputación de las empresas.

En la actualidad, tanto los Estados miembros de la UE como el sector privado necesitan cooperar entre sí para afrontar de manera efectiva estas amenazas. Sin embargo, solo la mitad de los países analizados ha establecido modelos de cooperación, como asociaciones público-privadas, grupos de trabajo y foros de contacto.

Debido a que algunos sectores, como el financiero, el de las telecomunicaciones y el energético, están regulados más estrictamente que otros, hay grandes diferencias en los requisitos de seguridad entre los diferentes sectores y para distintos tipos de operadores CII. Solo un pequeño número de países ha aplicado requisitos de seguridad obligatorios en todos los sectores.

Este estudio señala que algunos países, especialmente los que tienen un enfoque más descentralizado del la CIIP, delegan la evaluación del riesgo nacional a autoridades sectoriales o a operadores CII. Algunos países consideran que la presión de los mercados dará a los operadores CII suficientes incentivos para invertir en medidas de seguridad adicionales. Sin embargo, casi ninguno de los Estados miembros analizados ha implementado incentivos para que los operadores CII inviertan en medidas de seguridad relacionadas con la CIIP.

Tras los resultados validados del estudio, ENISA propone las siguientes medidas para los Estados miembros y la Comisión Europea:

- realizar una evaluación cuidadosa del riesgo nacional;
- establecer una cooperación entre los sectores público y privado;
- definir requisitos básicos de seguridad en línea para apoyar el desarrollo de medidas CIIP en los Estados miembros;
- implementar incentivos que puedan motivar a los operadores CII a invertir más en medidas de seguridad.

Udo Helmbrecht, director ejecutivo de ENISA, ha comentado: *«Las nuevas amenazas a las infraestructuras básicas de la información constituyen un peligro claro y presente, que solo pueden ser mitigado mediante esfuerzos coordinados. ENISA trabaja con los sectores tanto público como privado para garantizar que la CIIP sea una prioridad a escala europea».*

ENISA ofrece asesoramiento, recomendaciones y asistencia a los Estados miembros en la aplicación de la legislación comunitaria pertinente. La Agencia interactúa con las partes interesadas y la industria para fomentar el intercambio de buenas prácticas, información e ideas para la mejora de la CIIP en Europa.

A la luz de la próxima Directiva NIS y a partir de los resultados de este informe, ENISA continuará trabajando en la CIIP, interactuando con los agentes públicos y privados para definir los requisitos básicos de seguridad en línea y establecer un enfoque armonizado para la notificación de incidentes.

Informe completo: más resultados y más información sobre el estudio
Para obtener información técnica: Ana Sarri, responsable de seguridad de las redes y de la información, Anna.sarri@enisa.europa.eu
Para entrevistas y consultas de la prensa póngase en contacto con **press@enisa.europa.eu, Tel:** + 30 2814 409576