Problemas de salud en la asistencia sanitaria debido a los incidentes de ciberseguridad: momento de hacer un chequeo.

ENISA emite recomendaciones clave para proteger los servicios e infraestructuras de la salud en línea (eHealth).

El impacto potencial de una interrupción en los sistemas de información de un hospital puede ser devastador. La pérdida de un servicio o un fallo de un dispositivo médico debido a un ataque informático remoto (por ejemplo, a través de la fuerza bruta y ataques DoS) puede tener importantes repercusiones. Este tipo de incidentes de seguridad cibernética han tenido un gran impacto en los servicios de salud, con riesgos para la vida y las extremidades de los pacientes, exponiendo a las instituciones y los sistemas de atención sanitaria a un riesgo para su reputación. La asistencia sanitaria está ganando espacio en la agenda política. De hecho, los Estados miembros de la UE[1] la suelen considerar como una infraestructura crítica. ENISA, en colaboración con más de quince Estados miembros y dos países de la AELC, ha elaborado un estudio para identificar medidas que los responsables políticos y el sector privado deberían tomar para mejorar la seguridad y la resistencia de los sistemas de salud en línea . Este estudio se centra en tres casos reales de amplio uso, a saber, la historia clínica electrónica, los servicios nacionales de salud en línea (por ejemplo, la receta electrónica) y los sistemas de salud en línea que cuentan con el respaldo de servicios en la nube.

> ***El Director Ejecutivo de ENISA, Udo Helmbrecht, comentó sobre este informe: «La complejidad y la interdependencia de los sistemas de salud en línea han aumentado de manera constante. Garantizar la disponibilidad, integridad y confidencialidad en la salud en línea es una tarea difícil tanto para los proveedores como para los beneficiarios. ENISA busca cooperar con todos los interesados para mejorar la seguridad y la privacidad de todas las infraestructuras y servicios de salud en línea ».***

Dicho informe recomienda tomar, entre otras, las siguientes medidas:

- Las autoridades nacionales de ciberseguridad deberían identificar los activos críticos de la salud en línea y llevar a cabo evaluaciones con el fin de mitigar los riesgos
- Los responsables políticos deberían introducir directrices de seguridad cibernética de referencia para las infraestructuras y los servicios de salud en línea
- Los profesionales de la salud en línea, junto con los agentes del sector público, deberían configurar un mecanismo de intercambio de información para compartir buenas prácticas y conocimientos sobre las amenazas y vulnerabilidades.

Estos resultados fueron validados por numerosos expertos de los sectores público y privado en un taller abierto[2] organizado junto con la Comisión Europea el 30 de octubre de 2015.

Las nuevas tecnologías, como la computación en la nube, los dispositivos inteligentes y el Internet de las cosas, ya representan el motor de innovación que necesita la salud en línea. En 2016, los desafíos de la ciberseguridad

[1] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/Methodologies-for-identification-of-ciis
[2] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/workshops-1/2015/ehealth-workshop

seguirán aumentando junto con los servicios, por lo que ENISA se centrará en la adopción de la computación en la nube por parte de los proveedores de salud y en llevar a cabo un análisis sobre los hospitales inteligentes.

El informe completo se puede leer aquí:

Información técnica: Dimitra Liveri, experta en NIS, Dimitra.liveri@enisa.europa.eu

Para entrevistas y consultas relacionadas con la prensa, póngase en contacto con: **press@enisa.europa.eu, Tel.** +30 2814 409576