La Comisión presenta un plan de acción para proteger al sector sanitario de los ciberataques

Brussels, 15 de enero de 2025

La Comisión ha presentado hoy un plan de acción de la UE destinado a **reforzar la ciberseguridad de los hospitales y los prestadores de asistencia sanitaria.** Este plan de acción se anunció en las orientaciones políticas **de la presidenta Von der Leyen** como prioridad clave en los primeros cien días del nuevo mandato. La iniciativa es un paso importante para proteger al sector de la salud de las amenazas cibernéticas. Al mejorar la detección de amenazas, la preparación y las capacidades de respuesta de los hospitales y los proveedores de salud, se creará un entorno más seguro para los pacientes y los profesionales de la salud.

La digitalización está trayendo una revolución a la asistencia sanitaria, **permitiendo mejores servicios a los pacientes a través de innovaciones** como los historiales médicos electrónicos, la telemedicina y los diagnósticos impulsados por la IA. Sin embargo, los ciberataques pueden retrasar los procedimientos médicos, crear bloqueos en las salas de emergencia e interrumpir los servicios vitales que, en casos graves, podrían tener un impacto directo en la vida de los europeos. Los Estados miembros notificaron 309 incidentes significativos de ciberseguridad que afectaron al sector sanitario en 2023, más que en cualquier otro sector crítico.

El plan de acción propone, entre otras cosas, que ENISA, la agencia de la UE para la ciberseguridad, establezca un **Centro paneuropeo de apoyo a la ciberseguridad** para hospitales y proveedores de asistencia sanitaria, proporcionándoles orientación, herramientas, servicios y formación a medida. La iniciativa se basa en el marco más amplio de la UE para reforzar la ciberseguridad en todas las infraestructuras críticas y marca la primera iniciativa sectorial específica para desplegar toda la gama de medidas de ciberseguridad de la UE.

En pocas palabras, el plan de acción se centra en cuatro prioridades:

- **Mejora de la prevención**. El plan ayuda a desarrollar las capacidades del sector sanitario para prevenir incidentes de ciberseguridad a través de medidas de preparación mejoradas, como orientaciones sobre la aplicación de prácticas críticas de ciberseguridad. En segundo lugar, los Estados miembros también pueden introducir bonos de ciberseguridad para proporcionar asistencia financiera a los micro, pequeños y medianos hospitales y proveedores de asistencia sanitaria. Por último, la UE también desarrollará recursos de aprendizaje sobre ciberseguridad para los profesionales sanitarios.
- **Mejor detección e identificación de amenazas.** El Centro de Apoyo a la Ciberseguridad para hospitales y proveedores de asistencia sanitaria desarrollará un servicio de alerta temprana a escala de la UE, que ofrecerá alertas casi en tiempo real sobre posibles ciberamenazas, de aquí a 2026.
- **Respuesta a los ciberataques para minimizar el impacto.** El plan propone un servicio de respuesta rápida para el sector sanitario en el marco de la Reserva de Ciberseguridad de la UE. Establecida en la Ley de Cibersolidaridad, la Reserva proporciona servicios de respuesta a incidentes de proveedores de servicios privados de confianza. Como parte del plan, los ejercicios nacionales de ciberseguridad pueden llevarse a cabo junto con el desarrollo de libros de jugadas para guiar a las organizaciones de atención médica a responder a amenazas

específicas de ciberseguridad, incluido el ransomware. Se anima a los Estados miembros a que soliciten a las entidades la notificación de los pagos de rescate, para poder proporcionarles el apoyo que necesitan y permitir el seguimiento por parte de las autoridades policiales.

- **Disuasión: Proteger los sistemas sanitarios europeos** disuadiendo a los agentes de ciberamenazas de atacarlos. Esto incluye el uso del conjunto de instrumentos de ciberdiplomacia, una respuesta diplomática conjunta de la UE a las actividades informáticas malintencionadas.

El Plan de Acción se aplicará de la mano de los prestadores de asistencia sanitaria, los Estados miembros y la comunidad de la ciberseguridad. Para afinar aún más las acciones más impactantes para que los pacientes y los proveedores de asistencia sanitaria puedan beneficiarse de ellas, la Comisión pondrá en marcha en breve una consulta pública sobre este plan, abierta a todos los ciudadanos y partes interesadas.

Próximos pasos

El plan de acción es el inicio de un proceso para mejorar la ciberseguridad en el sector sanitario. Las acciones específicas se desplegarán progresivamente en 2025 y 2026. Los resultados de la consulta se tendrán en cuenta en otras recomendaciones para finales de año.

Antecedentes

La UE trabaja en varios frentes para promover la ciberresiliencia y proteger a sus ciudadanos y empresas de las ciberamenazas en una Europa cada vez más digital y conectada. Este plan de acción responde a la urgencia de la situación y a las amenazas únicas a las que se enfrenta el sector. Se basa en el marco legislativo existente en el ámbito de la ciberseguridad. Los hospitales y otros prestadores de asistencia sanitaria están establecidos como un sector de gran criticidad en virtud de la Directiva SRI 2. El marco de ciberseguridad de la SRI 2 trabaja de la mano con la Ley de Ciberresiliencia, la **primera legislación de la UE** que establece requisitos obligatorios de ciberseguridad para los productos que incluyen elementos digitales, que entró en vigor el 10 de diciembre de 2024. La Comisión también ha puesto en marcha un Mecanismo de Ciberemergencia en virtud de la Ley de Cibersolidaridad que refuerza la solidaridad de la UE y las acciones coordinadas para detectar, preparar y responder eficazmente a las crecientes amenazas e incidentes de ciberseguridad.

Garantizar una infraestructura digital resiliente y segura es esencial para el pleno despliegue del Espacio Europeo de Datos Sanitarios, que situará a los ciudadanos en el centro de su asistencia sanitaria, otorgándoles un control total sobre sus datos.

Para más información

Plan de acción sobre la ciberseguridad de los hospitales y los prestadores de asistencia sanitaria

Preguntas y respuestas

Ficha informativa

IP/25/262

Cita(s):

"La atención médica moderna ha logrado avances increíbles a través de la transformación digital, lo que ha significado que los ciudadanos se hayan beneficiado de una mejor atención médica. Desafortunadamente, los sistemas de salud también están sujetos a incidentes y amenazas de ciberseguridad. Es por eso que estamos lanzando un Plan de Acción para garantizar que los sistemas de salud, las instituciones y los dispositivos médicos conectados sean resilientes. Es mejor prevenir que curar, por lo que debemos evitar que ocurran ciberataques. Pero si suceden, necesitamos tener todo en su lugar para detectarlos y responder y recuperarse rápidamente."
Henna Virkkunen, vicepresidenta ejecutiva para la Soberanía Tecnológica, la Seguridad y la Democracia - 15/01/2025

"Las tecnologías digitales y las soluciones basadas en datos sanitarios han abierto oportunidades sin precedentes en el ámbito de la asistencia sanitaria. Permiten la medicina de precisión, el monitoreo de pacientes en tiempo real y la comunicación fluida entre los proveedores de atención médica a través de las fronteras. Pero la digitalización es tan fuerte como la confianza que inspira y resistente a los ciberataques. Los pacientes deben sentirse seguros de que su información más sensible es segura. Los profesionales de la salud deben tener fe en los sistemas que utilizan a diario para salvar vidas. El Plan de Acción de hoy es un paso importante para garantizar esa confianza y salvaguardar un ecosistema sanitario más resiliente para el futuro."
Olivér Várhelyi, comisario de Salud y Bienestar de los Animales - 15/01/2025

Personas de contacto para la prensa:

Thomas REGNIER (+32 2 29 91099)
Eva HRNCIROVA (+32 2 29 88433)
Nika BLAZEVIC (+32 2 29 92717)
Anna GRAY (+32 2 29 80873)

Solicitudes del público en general: Europe Direct por teléfono 00 800 67 89 10 11 , o por e-mail

Medios de comunicaci&#65533;n relacionados

Cybersecurity of hospitals - St. Michael's Hospital in Bratislava