Publicado en Madrid el 21/04/2021

Los ciberataques a las organizaciones sanitarias, los más temidos por el sector de la ciberseguridad

Los ciberataques a las organizaciones sanitarias son los más tenidos entre los profesionales de la ciberseguridad, porque pueden poner en riesgo la seguridad de los pacientes. Según informa S2 Grupo, en este tipo de incidentes los ciberdelincuentes incluso "pueden llegar a tener que coordinarse con personal sanitario en intervenciones sobre máquinas de soporte vital". Por ello, los expertos en ciberseguridad advierten de la necesidad de "establecer fuertes protocolos de ciberseguridad en los hospitales"

La empresa española S2 Grupo, especializada en ciberseguridad y gestión de sistemas críticos, ha destacado en un comunicado que la gestión de la ciberprotección de las organizaciones sanitarias es uno de los grandes retos del sector en 2021. De hecho, la compañía subraya que los ciberataques a las organizaciones sanitarias son de los más “temidos” por los expertos en ciberseguridad, debido a que puede ponerse en riesgo la seguridad de los pacientes.

En relación a las prácticas que debe poner en marcha un centro sanitario para hacer frente a un ciberataque, Rafael Rosell, director comercial de S2 Grupo, ha indicado que "la ciberseguridad es un proceso continuo, un conjunto de proyectos que deben formar parte de un Plan Director de Seguridad que deberán ejecutarse a lo largo del tiempo".

En este sentido, el experto en ciberseguridad añade que es clave la figura de un CISO o de una oficina técnica de seguridad externa, para que priorice las iniciativas en función de las riesgos de la organización. “Uno de los puntos clave para mantener de forma continua la seguridad es la creación o la contratación del servicio de un SOC, un centro de operaciones de seguridad, especializado en salud. Desgraciadamente los ciberataques actuales no se centran de forma exclusiva en los sistemas de información, afectan también, en muchas ocasiones, al equipamiento médico propio de una infraestructura sanitaria. Esto obliga a desplegar sistemas de cibervigilancia específicos para el sector”, explica Rosell.

¿Qué hacer en caso de ciberataque a un centro sanitario?
“Lo primero que debemos hacer es estar preparados para sufrir un ciberincidente adoptando las medidas de prevención y de continuidad de negocio adecuadas”, afirma Rafael Rosell.

Junto a esto, S2 Grupo ha resaltado que, a pesar de estar preparados y protegidos, es importante trabajar con la hipótesis de que el ciberataque se va a producir para estar preparados en todos los contextos.

“Si esto sucede, lo primero que debemos hacer es convocar un gabinete de crisis y ponernos en manos de un equipo especialista de gestión de incidentes de ciberseguridad. Es muy importante, para poder responder de forma adecuada tanto legal como técnicamente, que en los primeros momentos

del ciberincidente participen especialistas en gestión de incidentes de ciberseguridad, no en tecnología, y si es posible con experiencia en entornos sanitarios. Si hacemos esto podremos responder con las máximas garantías al incidente", ha asegurado.

Ante el actual contexto de la ciberseguridad en el ámbito sanitario, S2 Grupo ha señalado que es muy importante tener en cuenta que nadie está libre de sufrir un ciberataque. Por otra parte, la compañía ha destacado en su comunicado que se debe tener en cuenta que la preparación para responder al ciberincidente es clave. Por último, S2 Grupo concluye que "nunca se debe pagar a los delincuentes porque, además de ser delito, si se paga se entra en la lista de 'clientes que pagan' y posiblemente sea la garantía de sufrir el próximo incidente".

Datos de contacto:
Luis Núñez
667574131

Nota de prensa publicada en: Madrid

Categorías: Medicina Ciberseguridad