

S2 Grupo advierte de las consecuencias de un ciberataque a un hospital

Desde S2 Grupo se ha asegurado que el sector de la salud es actualmente uno de los más críticos, desde el punto de vista de la ciberseguridad. Actualmente, más allá de los dispositivos que se utilizan para cuestiones administrativas, tanto monitores, como respiradores y otros aparatos como bombas de suministro de medicamentos, están conectados a la red y una posible acción de ciberdelincuentes podría sabotearlos poniendo en riesgo la salud de los pacientes

S2 Grupo, compañía especializada en ciberseguridad y gestión de sistemas críticos, ha asegurado que el ámbito sanitario es en los últimos años uno de los más afectados en el ámbito de la ciberseguridad.

El objetivo de los ciberdelincuentes suele ser económico y su forma de proceder puede ser desde un ransomware que incapacite el acceso a las máquinas de los pacientes, ordenadores, historiales, etc., hasta el robo y venta de información de pacientes, entre otros.

“Los hospitales representan un objetivo estratégico importante para los ciberatacantes y es muy importante que estas instalaciones contemplen la ciberseguridad desde su fase más inicial. El problema reside en que, a pesar de que cada vez se tiene más en cuenta la seguridad a la hora de diseñar cualquier tipo de dispositivo conectado a la red, ningún sistema es seguro al 100% y, menos, si están conectados a máquinas antiguas”, ha explicado José Rosell, socio-director de S2 Grupo.

“Las máquinas de un hospital tienen un coste elevadísimo, por lo que no pueden cambiarse al mismo ritmo que crecen las herramientas utilizadas por los ciberdelincuentes. Por tanto, el objetivo de las empresas de ciberseguridad debe ser estudiar las redes de comunicaciones que utilizan éstas y buscar todas las puertas por donde podría entrar un ciberdelincuente y cerrarlas”, ha asegurado Miguel A. Juan, socio-director de S2 Grupo.

Actualmente, más allá de los dispositivos que se utilizan para cuestiones administrativas, tanto monitores, como respiradores y otros aparatos como bombas de suministro de medicamentos, están conectados a la red y una posible acción de ciberdelincuentes podría sabotearlos poniendo en riesgo la salud de los pacientes.

Para trabajar en este objetivo de securizar al máximo los entornos hospitalarios, S2 Grupo ha creado una Unidad de Cuidados Intensivos (UCI) en su laboratorio para definir sistemas avanzados de ciberprotección que permitan minimizar la acción de los ciberdelincuentes en el ámbito sanitario. Su finalidad es conocer exhaustivamente todos los canales por los que se pueden intentar infiltrar, para asegurarlos y evitar que lo consigan.

Algunos de las formas que los ciberdelincuentes han utilizado para sabotear los sistemas de centros

sanitarios son el bloqueo de las máquinas, alterar su funcionamiento, del flujo de información para que no pueda ser recopilada correctamente, el robo de información de pacientes para venderla posteriormente, o secuestrar equipos a cambio de dinero.

Datos de contacto:

Luis Núñez
667574131

Nota de prensa publicada en: [Madrid](#)

Categorías: [Medicina Programación Ciberseguridad](#)

NotasdePrensa

<https://www.notasdeprensa.es>