CIBERSEGURIDAD PARA SALUD: protección en un mercado digitalizado
Fuente: El Hospital | Fecha: Abril.2022
Medio: Revista | Página: 51-22

CIBERSEGURIDAD PARA SALUD: protección en un mercado digitalizado

Además de robo o secuestro de información con datos sensibles, el cese de operaciones es el mayor riesgo al que se pueden enfrentar las instituciones de salud con un ciberataque.

POR: JORGE IVÁN PARADA HERNÁNDEZ
periodista

POR: ALEJANDRA LEGUIZAMÓN
editora de El Hospital

A medida que el sector salud opta por soluciones en digitalización y servicios de nube, hoy más que nunca se necesita un fuerte esquema de protección de datos y equipos en instituciones clínicas. Recientemente el Instituto Nacional de Vigilancia de Medicamentos y Alimentos (Invima) de Colombia, sufrió un ciberataque debido a un ransomware que afectó su sistema informático, afectando, por más de 30 días, la capacidad operativa en los servicios prestados por la entidad.

El INVIMA debió 'apagar' su sitio web y ha tenido varios retrasos en permisos de importación y exportación de productos, entre otras labores de vigilancia y autorizaciones que realiza la institución. Esta crisis tecnológica, llevó a la entidad a realizar sus procesos de forma manual.

Este es un ejemplo que realza la importancia detener soluciones de protección de datos y equipos interconectados a redes hospitalarias. Hoy, la información digital es un valioso activo para hackers, ya que puede ser vendida a terceros o ser parte de secuestro de datos. De igual forma, los equipos médicos pueden ser intervenidos y dejados fuera de operación, afectando el flujo de trabajo en instituciones de salud. Para profundizar en el tema, el experto en seguridad Oswaldo Palacios, Director de Guardicore para Latinoamérica, habló en exclusiva con revista El Hospital.

El Hospital: ¿A qué se debe la falta de acción de las instituciones de salud para protegerse de ciberataques?

Oswaldo Palacios: La primera razón es qué no es falta de interés, sino falta de información. En instituciones de salud siempre están buscando cómo innovar la operación, pero no siempre tienen la información adecuada a mano. Por otro lado, existe una cultura de protección reactiva y no proactiva. Nosotros ejecutamos una solución antes de que pase un ataque, pues una vez la información es cifrada, no hay nada que se pueda hacer. Lo que recomendamos a los tomadores de decisión de instituciones médicas es que nos permitan explicar y mostrar las solucio-

nes que tenemos, porque hay diferentes procesos y fases de protección para cada uno.

EH: ¿Cuál es el mayor riesgo que afrontan las instituciones y cuál debería ser la ruta de operación para contrarrestarlo?

OP: Para el sector salud no es solo el robo, secuestro o pérdida de los datos, sino la alteración en la operación del sistema; ese es el objetivo principal. Un paciente no debería llegar a un hospital que no le funcionen los equipos de rayos X o algún otro dispositivo que esté conectado a la red informática porque fue atacado.

Si le dicen que no pueden acceder a sus datos o a sus resultados, el paciente se iría a otra institución médica. Esto impacta en las finanzas de la institución, en el flujo de trabajo, en los procesos programados, en general en la operación habitual del centro médico. Esto supondría volver a los equipos antiguos [que sirven como reserva en algunas instituciones] que no están conectados y no tienen todas las ventajas de los equipos de última generación.

Además del robo de información, hay un problema y es el mal uso de los perfiles que tienen acceso a esa información. Se debe ver a la red informática como un todo. Debemos asegurarnos que los profesionales tengan los perfiles adecuados para acceder a la red de información que requieren. También recomendamos un software de visibilidad para ver cómo se están transmitiendo los activos críticos, como un expediente virtual.

EH: ¿Cuál es el protocolo básico para actuar de manera preventiva y no reactiva ante estas amenazas?

OP: La seguridad se debe llevar en capas. Una amenaza de este tipo, no se soluciona con tan solo un antivirus. De acuerdo a quién accede a la información, cómo se hace la información y la disponibilidad de la información, se toman las precauciones y las herramientas que debemos usar para protegerla.

Cada plan de contingencia se debe hacer a la medida de las necesidades de cada empresa, como cada una es diferente, no hay algo estandarizado. Sin embargo, hay casos de usos generales, por ejemplo, la segmentación de una aplicación crítica. Por eso siempre recomendamos empezar con la visibilidad, ya que no puedes proteger lo que no puedes ver. Una vez conoces cómo se comunican tus activos críticos, puedes hacer algo que llamamos *enforcement*, es decir, tomar decisiones frente al tráfico que estamos viendo. Una vez hecho esto, se puede crear un ambiente seguro.

EH: ¿Qué tan perjudicial y/o qué tan beneficioso puede ser el Internet de las Cosas Médicas (IoMT) a la hora de almacenar y proteger los datos de instituciones de salud?

OP: Definitivamente es responsabilidad de quien ejecuta y usa la tecnología. El fabricante de los equipos de IoMT está pensando en la funcionalidad y el beneficio clínico. El problema es que estos equipos se vinculan a la red informática del centro médico y eso los hace vulnerables. Por ejemplo, un equipo de ultrasonido o de rayos X, podría tener los estudios y enviarlos a un servidor central, de ahí las personas adecuadas deberán tener acceso. Nosotros vemos esa brecha y tratamos de blindar comunicaciones, para que los datos no sean accesibles a quien no se debe y que dicho acceso esté segmentado. Esto significa que está aislado del tráfico de la red informática para que el acceso sea selectivo y se reduzca la superficie de ataque.

EH: ¿Cuáles son las tendencias en ciberseguridad para 2022 según el comportamiento actual del mercado de salud digital en América Latina?

OP: La primera es el resguardo de información. Hay muchos datos comerciables de hospitales, instituciones de salud, laboratorios, etc. y todos son susceptibles de ser sustraídos y vendidos. Algo que no están haciendo, es tener una superficie preventiva para que sepan cómo protegerse. Entendemos que por la naturaleza de la operación, están enfocadas en temas de salud y prevención; pero a la par que están en la transformación digital, deben informarse [y adoptar] sobre las opciones en el mercado que les permite anticipar y evitar los riesgos de ciberataques.