LITORALPRESS

Fecha: 10-12-2024
Medio: El Mercurio
Supl. : El Mercurio - Cuerpo B
Tipo: Noticia general
Título: Por qué los hackers quieren su información de salud

Pág. : 8
Cm2: 811,7

Tiraje: 126.654
Lectoría: 320.543
Favorabilidad: No Definida

Las sustracciones de datos se han vuelto comunes:

Por qué los *hackers* quieren su información de salud

HEIDI MITCHELL
THE WALL STREET JOURNAL

Estos registros contienen antecedentes personales que pueden dejar a los pacientes expuestos a riesgos financieros y médicos.

Las violaciones de datos en las organizaciones que ofrecen atención de salud se han vuelto comunes últimamente. Pero, de todos modos ¿qué quieren los *hackers* con su información médica?

Por lo general, los *hackers* irrumpen en las redes de proveedores en busca de un rescate, y hacen cosas como dejar al proveedor fuera de sus propios sistemas computacionales o amenazar con exponer sus datos en línea. Pero también están buscando datos de pacientes.

Los registros de atención de salud tienen información personal de la que los *hackers* siempre quieren apoderarse, como direcciones y números de tarjetas de crédito. Pero los registros también contienen un conjunto de información privada sobre los pacientes, que abarca desde números de pólizas de seguro hasta condiciones médicas y medicamentos; datos que permiten a los delincuentes estafar a las compañías de seguro y a Medicare y Medicaid, dejando a los pacientes expuestos a agudos riesgos financieros y médicos.

MERCADO NEGRO
Un registro médico individual se puede vender entre US$ 500 y US$ 1 mil.

"Le proporcionan a los *hackers* un cuadro completo para cometer fraude de seguros, robo de identidad u otra actividad maliciosa en el futuro", dice John Riggi, asesor nacional de ciberseguridad y riesgo de American Hospital Association, una organización comercial que representa al 90% de los hospitales en EE.UU.

Lo que es más, el robo de registros de salud puede tener un impacto más duradero en las víctimas que el fraude financiero o el robo de identidad habitual, porque la información en esos registros es más difícil de detectar y es un desafío mayor corregirla cuando se ha hecho mal uso de ella.

"Si su tarjeta de crédito está comprometida, su banco lo va a alertar, la va a cancelar y le va a enviar una nueva", indica Geetha Thamilarasu, profesora adjunta de computación y sistemas de *software* de la Escuela de STEM de la Universidad de Washington Bothell. "Pero sus registros médicos tienen una vida muy larga. Se puede hacer mal uso de ellos sin que eso se detecte durante largos períodos de tiempo, porque es más difícil identificar una actividad maliciosa. Eso los hace muy valiosos".

Robo y venta

Según la Oficina de Derechos Civiles del Departamento de Salud y Servicios Humanos de EE.UU., se reportaron 725 incidentes de violación de datos que expusieron 500 o más registros de salud en 2023, frente a 720 en 2022. En febrero, Change Healthcare informó un hackeo gigante que puede haber afectado hasta un tercio de la población estadounidense, según Andrew Witty, jefe ejecutivo de la empresa matriz UnitedHealth Group.

Una vez que se roba el registro de atención de salud, a menudo termina siendo vendido en la 'dark web', los rincones ocultos de internet donde tienen lugar las transacciones ilícitas. Un registro médico individual se puede vender entre US$ 500 y US$ 1 mil, señala Thamilarasu, en comparación con uno o dos dólares que juntan los números del Seguro Social.

Con la información de identificación personal y registros médicos de un paciente, "un tipo malo puede entrar en una cuenta de la persona, suplantar su identidad, luego monetizar esa información en una variedad de formas", explica Rahul Telang, profesor de sistemas de información en el Heinz College de la Universidad Carnegie Mellon.

Los delincuentes podrían, por ejemplo, solicitar beneficios y reembolsos de seguros de aseguradoras privadas o Medicaid y Medicare, dice Telang, y hacer que esos cheques se los envíen a la nueva dirección. Igualmente pueden hacer que el sistema genere recetas ilícitas para dispositivos de salud o sustancias controladas, los que tienen un alto valor de reventa, precisa.

Puede que pasen meses o años antes de que el paciente promedio y la aseguradora descubran estos fraudes, los que pueden provocar una serie de problemas. Las aseguradoras pueden elevar las primas de las personas en base a hackeos anteriores debido a los cuales las compañías de seguro tienen que realizar grandes gastos para corregirlos.

Este tipo de estafa podría no solo perjudicar económicamente a las personas, sino que también provocarles nuevos dolores de cabeza en el futuro. A las víctimas de robo de identidad médica les pueden negar cobertura en el futuro porque sus registros muestran que tiene una condición que realmente no tiene. O les pueden decir que han alcanzado su límite de beneficios. Corregir la información falsa es difícil, puesto que los proveedores de atención de salud y aseguradoras a menudo tienen sistemas complicados para corregir los registros, y estos sistemas no "hablan" entre ellos.

Según la Oficina de Derechos Civiles del Departamento de Salud y Servicios Humanos de EE.UU., se reportaron 725 incidentes de violación de datos que expusieron 500 o más registros de salud en 2023

JON KRAUSE

Los delincuentes también podrían utilizar los registros de los pacientes para hacerse pasar por proveedores de atención de salud; y dejar a los pacientes debiendo dinero. Por ejemplo, los ladrones podrían hacerse pasar por un proveedor y cobrar a las compañías aseguradoras por dispositivos costosos y otros servicios médicos reembolsables, indica Thamilarasu. Luego los deducibles o copagos por servicios jamás prestados llegan a los pacientes, quienes tal vez no los reconozcan como fraudulentos.

"Los tipos malos calcularon que si mantienen la factura bajo una cierta cantidad de dólares, pueden volar bajo el radar un largo tiempo", dice Riggi.

Igualmente se sabe que los *hackers* utilizan registros médicos robados para crear convincentes correos electrónicos o llamadas telefónicas o videollamadas de '*spearphishing*' (suplantación de identidad selectiva), en los que se hacen pasar por proveedores legítimos de atención de salud y les piden a los pacientes que paguen una cuenta, que entreguen su contraseña o den más datos personales, explican expertos. "Esta es un área en que la IA puede multiplicar rápidamente la cantidad de personas que los delincuentes atacan y qué tan astutos pueden ser esos mensajes específicos", señala Telang.

Un uso menos común para los registros médicos hackeados es el chantaje, afirma Riggi. Los *hackers* podrían amenazar con dar a conocer los registros de una persona a un empleador o al mundo en general si no paga un rescate. "Usted no quiere que otra persona sepa si está teniendo problemas de salud mental o si está embarazada", dice Thamilarasu. "No quiere que todos tengan acceso a los datos".

Principalmente, los pacientes individuales no tienen que preocuparse de que los delincuentes vendan sus registros médicos robados a las aseguradoras o a profesionales del márketing. La Ley de Transferencia y Responsabilidad de Seguro Médico permite que las corredoras de datos compren y vendan cierta información de salud de los pacientes; siempre que las características de estos sean anónimas y sigan siendo secretas. Por supuesto, los datos de los delincuentes no cumplirán esas pautas.

"Las compañías aseguradoras se meterían en muchos problemas legales", observa Riggi de AHA, "y la gente de márketing puede encontrar información sobre sus intereses y prácticas de compra en forma legal en base a los datos disponibles públicamente y al historial de búsqueda".

Esté atento

Para evitar el fraude, los pacientes deberían tener las mismas precauciones con su información médica que las que tendrían con cualquier dato sensible en línea. Deberían utilizar autenticación multifactor para tener acceso a los registros médicos, por ejemplo, y nunca deberían hacer clic en enlaces sospechosos.

Las personas también deberían prestar atención a sus facturas médicas en forma tan minuciosa como lo harían con las facturas de la tarjeta de crédito. La Comisión Federal de Comercio precisa que las personas deberían estar atentas a las señales de advertencia como recibir facturas por servicios médicos que no recibieron o que sus planes de salud les informen que han alcanzado sus límites de beneficios.

Aunque la vigilancia individual es importante, las reformas sistémicas son fundamentales para abordar las causas principales de las violaciones de datos médicos, afirma Parham Eftekhari, fundador y presidente de Institute for Critical Infrastructure Technology, un instituto de estudios no partidista y sin fines de lucro. Muchas organizaciones de atención de salud utilizan terceros socios, lo que significa que los registros de los pacientes no están almacenados solo en el hospital, sino que también es posible que estén con docenas de otros proveedores de servicios, indica Eftekhari.

"Eso ofrece más oportunidades para que los datos sean robados debido a trabajadores no maliciosos pero con poca o ninguna capacitación, o debido a actividades delictuales. Igualmente significa que los hospitales dependen de la seguridad de sus socios, sobre las cuales tienen menos control", agrega.

Más de un 85% de registros de atención de salud es robado a terceros y a proveedores no hospitalarios, según Riggi.

Aquellos a cargo de las políticas también tienen un papel que desempeñar. Una aplicación más estricta de estándares a todo el sector de atención de salud, lo que incluye a terceros proveedores, podría motivar a las organizaciones de salud a invertir en medidas preventivas más bien que responder en forma reactiva después de que ocurre un delito, dice Eftekari.

"Los que se encargan de las políticas también tienen que asegurar que las leyes destinadas a mejorar la seguridad de los datos no agreguen en forma inadvertida complejidades con respecto a las violaciones y amenazas cuando se trata de compartir información entre los sectores público y privado", precisa.

Además, agrega Riggi, no todos los hospitales, como aquellos que atienden a áreas rurales y de bajos ingresos, tienen los recursos para cumplir con las regulaciones cada vez más estrictas. Para arreglar el problema de hackeo generalizado se requerirán soluciones creativas.

Hay algunas señales de que las cosas están mejorando. Para mantener la confianza de los clientes, los hospitales han hecho grandes esfuerzos en los últimos años para bloquear sus redes. "Los hospitales han estado reforzando sus sistemas para dificultar la infiltración de extraños", asegura Telang. Pueden hacer esto al segmentar las redes, codificarlas, permitir la autenticación multifactor y poner en marcha otras estrategias de prevención de pérdida de datos.

"Están contratando a más personas especializadas en tecnología de la información, gastando más dinero y capacitando a todo el personal", indica Telang. "Y las cosas han mejorado".

Artículo traducido del inglés por "El Mercurio".