La seguridad en datos de salud, algo imprescindible

Con el desarrollo de los objetos capaces de coenctarse a Internet para mantener un registro de la rutina de los ciudadanos, el sector de la salud es uno de los que más cambios está viviendo. El hecho de poder conectar los aparatos a una red para monitorizar a cada paciente, va a revolucionar los tratamientos y cuidados a las personas que sufren alguna dolencia. Pero esto también lleva a que los ciberdelincuentes sientan atracción por estos datos, tan íntimos de los ciudadanos.

SiliconWeek ha hablado con voceros de **Mkit, Kaspersky Lab, SonicWall y ESET Latinoamérica** para analizar cómo estos datos sanitarios están en el punto de mira de los ciberdelincuentes que quieren sacar dinero con sus fechorías y cómo los hospitales y centros sanitarios en general deben hacer para protegerlos.

Cabe mencionar aquí, como explica Vladimir Alem, Marketing Leader de SonicWall en América Latina, que **los ataques de ransomware crecieron en 2017 alrededor de 160 veces comparado con el año anterior,** lo que ocasionó grandes estragos en empresas de salud que por diversos motivos no contaban con la infraestructura de seguridad adecuada, es decir, no estaban preparadas para enfrentar amenazas de día cero.

Recuerdan desde Mkit que los datos sanitarios para los ciberdelicuentas ya que un registro médico electrónico (Electronic Health Record, “EHR”) tiene un valor en el mercado negro de entre 1,000 y 50,00 dólares, según quien sea la persona o que tan único sea el perfil. Para comprender la dimensión, una tarjeta de crédito vale entre 5 y 50 dólares en el mercado negro, muchísimo menos. Los expertos de esta empresa recuerda que en Enero de 2015 se robaron 80 millones de registros de la empresa Anthem Health Insurance, incluyendo informaciones tan privadas como historial de enfermedades de los pacientes y de los procedimientos llevados a cabo. “Esa información es crítica y absolutamente privada para los pacientes. Por supuesto, una vez que el hecho se hizo público no hay margen de acción. Es posible resolver si te capturan un password, se recupera y queda solucionado. Pero ¿cómo cambias tu DNI, o tu historial de enfermedades?”, explica Christian Amicelli desde Mkit.

¿Qué es lo que más atrae a los ciberdelincuentes de los datos sanitarios?

Como nos recuerda Cristian Amicelli, Chief Operating Officer de Mkit, compañía especializada en servicios de seguridad informática, “los registros medicos son datos de mucho valor en el **mercado negro,** ya que permiten realizar diversas actividades ilícitas, sea compra de drogas legalmente e introducirlas el mercado negro”, por ejemplo. Además, recuerda el directivo que “los datos medicos poseen mucha información más allá de los datos filiatorios, **algo que es importante saber es que los registros medicos poseen distintos niveles** cuando más alto sean mayor información se

obtiene".

Por su parte, Miguel Ángel Mendoza, especialista en seguridad informática de ESET Latinoamérica, recuerda que las instituciones de salud como hospitales, clínicas y laboratorios se han convertido en un blanco atractivo para los cibercriminales, "debido a que manejan información personal, financiera y médica de sus pacientes, así como del personal". Es decir, vemos que "**ya no solo se trata de datos como nombre, teléfono, dirección o número de seguridad social, sino que también entran en juego las dependencias a medicamentos**, las necesidades de determinados tratamientos o prácticas".

De este modo, cabe recordar que "dentro de los datos relacionados con la salud, se pueden identificar la valoración, preservación, cuidado, mejoramiento y recuperación sobre el estado de salud físico o mental, información genética, historias clínicas, patentes y fórmulas de medicamentos, sin dejar de lado los datos personales y bancarios de pacientes y personal. Un registro médico robado que contenga muchos detalles puede venderse mucho más caro que datos no correlacionados; sin embargo, es un mercado mucho más especializado que el mercado general de los datos personales".

¿Cómo un robo de datos puede afectar a un centro y a los pacientes?

Alfonso Ramírez, director general de Kaspersky Lab Iberia, recuerda que la empresa de seguridad ha observado que, aunque muchos dispositivos médicos están expuestos en Internet, por lo que cualquier cibercriminal puede encontrar escáneres, equipos de cardiología y de radiología conectados a la red, "muchos de ellos siguen teniendo las mismas contraseñas predeterminadas de fábrica, pudiendo ser averiguadas fácilmente por los ciberdelincuentes". Además, muchos de estos dispositivos médicos utilizan versiones obsoletas de sistemas operativos con innumerables vulnerabilidades. Según el experto, "**en la mayoría de las ocasiones, los parches para reparar esas vulnerabilidades no son tan fáciles de implementar,** además se necesitan ingenieros cualificados que ayuden a actualizar los sistemas. Como esto supone mucho dinero y tiempo, en la mayoría de las ocasiones, se desatiende la seguridad, haciendo que estos dispositivos sean una puerta de entrada fácil para las actividades delictivas de los cibercriminales".

Kaspersky alerta de que las consecuencias d este tipo de prácticas ineficientes pueden ser muy graves. "No sólo pone los datos personales al alcance de los ciberdelincuentes, sino que también podría afectar de forma directa la salud y hasta las vidas de los pacientes".

Desde **ESET**, Miguel Ángel Mendoza, Especialista en seguridad informática, recuerda que en muchos casos, esta información es utilizada para llevar a cabo delitos, como el robo de identidad, extorsiones o fraudes. "Ahora, si nos enfocamos en datos personales relacionados con la salud,

pensemos en un caso donde un atacante puede recopilar el nombre, número de seguridad social, teléfono, dirección, correo electrónico y otros datos personales; con esta información tendrá una oferta potencial mucho más amplia que el hecho de averiguar si un paciente se sometió o no a un procedimiento médico en particular", concreta el experto.

Alem, desde SonicWall añade que si miramos al aspecto legal, diversos países incluyendo México han determinado la forma en que deben ser protegidos los datos, teniendo un impacto directo en las empresas o instituciones, incluso en los administradores de TI. "Por el lado de los pacientes **el robo de información personal puede llegar a tener graves implicaciones en el aspecto laboral, personal,** profesional y hasta financiero, en caso de darse a conocer información confidencial a la que sólo tiene acceso la institución donde están o han sido atendidos".

Consejos para evitar estos robos y sus consecuencias

El primer elemento a considerar es que "no existe una empresa en el mundo cien por ciento protegida, en un escenario tan complicado como el que implica estar conectado a Internet la opción es buscar herramientas y capas de seguridad complementarias que puedan ser gestionadas de forma centralizada", como explica el vocero de **SonicWall**.

Por su parte, Cristian Amicelli, Chief Operating Officer de Mkit, añade que "siempre es necesario estar atento" y que "**como principales medidas es muy recomendable realizar auditorias de seguridad constantes a plataformas, servicios y recursos humanos ya que todos son parte de la cadena de la seguridad informátic**a, sumar contramedidas para evitar la fuga de información también ayuda a elevar la seguridad".

Lo primero de todo es contar con una infraestructura fuerte en cuanto a seguridad para proteger los equipos. Además de eso, desde **Kaspersky** recomiendan excluir del acceso externo a todos los sistemas de información que procesen los datos médicos y demás información sobre los pacientes: cambiar las contraseñas predeterminadas de los sistemas de atención médicas por unas más complejas que incluyan números, símbolos y letras; formar y concienciar a todo el personal del hospital sobre los peligros de las ciberamenazas y cómo hacerles frente; y actualizar los sistemas médicos y parchear siempre las distintas vulnerabilidades; además de hacer una copia de seguridad con la información crítica.