CIBERSEGURIDAD Y SALUD

CYBERSECURITY AND HEALTH

Julio Fernando Andrade Vintimilla [1]

[1] Instituto Superior Tecnológico con Condición de Universitario "Compou Sur". Ecuador. julioan652@gmail.com, https://orcid.org/0000-0001-9928-846X

RESUMEN

En este artículo se entiende lo que es la ciberseguridad y cómo ella se relaciona con las ciencias de la salud en general y con la salud en particular. Se destaca el por qué la ciberseguridad debe formar parte de las áreas estratégicas de las empresas, no solo de aquellas relacionadas con la salud sino de empresas de todas las áreas. Se analiza los costos relacionados con la recuperación a los ciber-ataques. Mediante el análisis de casos de empresas del área de la salud que han sido afectadas por acciones de los ciber-delincuentes, se van puntualizando las acciones que han debido realizar como resultado del nivel de importancia que han prestado dichas empresas, a la prevención contra los ciberataques, y se determina si han podido o no hacer frente a los mismos. Se aprovecha esta circunstancia para poder realizar recomendaciones de manera general, que permitirán prepararse para frenar y, de alguna manera, mitigar si es del caso, las afectaciones por parte de los ciber-terroristas.

PALABRAS CLAVES: Ciberseguridad, Salud, Ciber-ataques,Ciberdelincuentes, Ciber-terroristas

ABSTRACT

In this article we understand what cybersecurity is and how it relates to the health sciences in general and health in particular. It highlights why cybersecurity should be part of the strategic areas of companies, not only those related to health but companies from all areas. The costs related to recovery to cyber-attacksare analyzed. Through the case analysis of companies in the health area that have been affected by cyber- criminal attacks, the actions that have been carried out as a result of the level of importance these companies have given to the prevention against cyber-attacks are pointed out, and determine whether or not they havebeen able to mitigate them. This circumstance is used to make recommendations in a general manner, whichwill help to prepare to stop and, in some way, mitigate affectations due to cyber-terrorist attacks.

Keywords: Cybersecurity, , Health, Cyber-attacks, Cybercriminals, Cyber-terrorists
.

INTRODUCCIÓN

El presente trabajo presenta un análisis y su relación entre las Ciencias de la Salud en general,la salud en particular, y la Ciberseguridad.

Las Ciencias de la Salud se pueden definir como las ciencias aplicadas que abordan el uso dela ciencia, la tecnología, la ingeniería o las matemáticas en la prestación de asistencia sanitaria a los seres humanos (Wikipedia, 2019).

Según la fuente citada, estas ciencias abarcan el amplio propósito de: mantener, reponer, mejorar la salud y el bienestar, prevenir, tratar y erradicar enfermedades y comprender mejor los complejos procesos vitales de los organismos animales y humanos relacionados con la vida, la salud y sus alteraciones (enfermedad).

La Ciberseguridad, por otro lado, es la protecciónc contra los ataques cibernéticos de los sistemas conectados a Internet, incluidos el hardware, elsoftware y los datos (Rouse, 2018).

En un contexto informático, la seguridad comprende la seguridad cibernética y la

seguridad física; ambas se utilizan para proteger contra el acceso no autorizado a centros de datos y otros sistemas informáticos.

La ciberseguridad está diseñada para mantener la confidencialidad, integridad y disponibilidad de los datos.

La relación entre las ciencias de la salud en general, y la salud en particular, con la ciberseguridad se manifiesta porque las primeras usan el Internet para llevar a cabo casi todas las actividades de su diario accionar, y los ciber-delitos se producen en redes interconectadas, siendo el Internet su campo de acción favorito.

Por tanto,la confidencialidad y resguardo de toda la información relacionada con la salud, uno de los objetivos de la ciberseguridad, es responsabilidad de las empresas relacionadas con el área de salud.

Esto les compromete a incluir dentro de sus áreas estratégicas, a la seguridad de la información como parte de su corebusiness o áreas críticas del negocio.

DESARROLLO

En la figura1 se puede apreciar el costo por industria de violación de datos, ubicando a la salud comola favorita de los ciber delincuentes con cercade 400 millones de dólares.

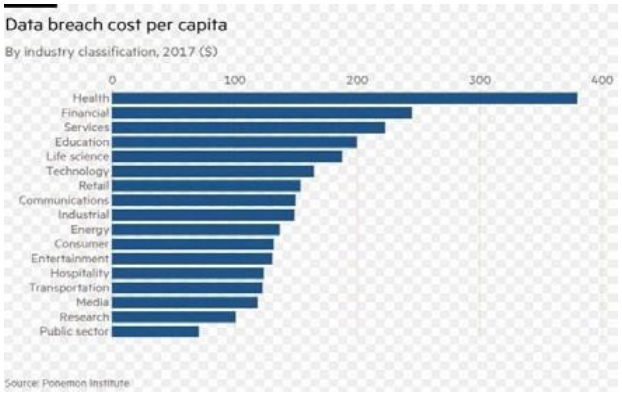

Figura 1. Costo de violación de datos por industria. Fuente: Ponemon Institute. 2017.

Un estudio reciente sobre las mejores prácticasde seguridad cibernética, adoptado por grandes y pequeños proveedores de atención médica, reveló que existe una creciente brecha entre losdos.

Los proveedores más grandes tienen más probabilidades de tener defensas de seguridad cibernética sofisticadas y maduras, mientrasque los proveedores más pequeños están luchando para seguir las mejores prácticas en este ámbito.

Para el estudio, KLAS y CHIME analizaron las respuestas a la encuesta de los más buscados de atención médica de 2018, realizada por unos 600 proveedores de atención médica y evaluaron cada uno para determinar si cumplían con las mejores prácticas de ciberseguridad enla atención médica.

Uno de los requisitos de la Ley de Ciberseguridad de 2015 en Estados Unidos, fue que el Departamento de Salud y Servicios Humanos (HHS) forme un grupo para desarrollar orientación para que losproveedores de atención médica los ayuden a administrar y mitigar las amenazas a los datos de los pacientes, según la Ley de Transferencia y Responsabilidad de Seguro Médico (Health Insurance Portability and AccountabilityAct - HIPAA Journal, 2019).

La figura

dos muestras, que los datos junto con planes estratégicos e iniciativas, ocupanel tercer lugar en importancia de los activos que las empresas deben proteger contra los ciberataques, y en el caso de la salud, se refierea la información de sus pacientes.

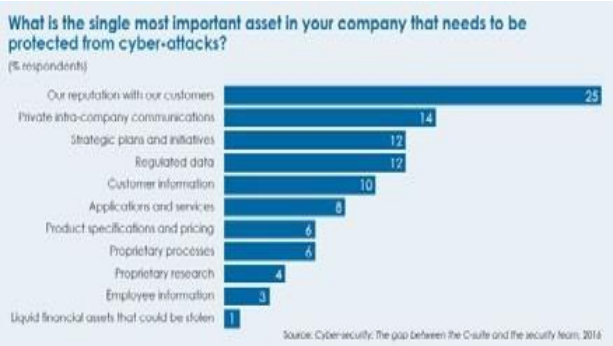

Figura 2. Activos de una compañía que deben ser protegidos de los ciber ataques.

Fuente: Cyber-security: the gap between the C-suite and the security team. 2016.

En concordancia la presente investigación persigue como objetivo: Determinar la importancia que tiene la ciberseguridad dentro de la salud. Luego, mediante el análisis de casos, puntualizar los resultados de la importancia que se da en la actualidad a la ciberseguridad dentro delárea de la salud.

Finalmente, determinar las recomendaciones para realizar una protección primaria, que permita mitigar los riesgos deexposición a los que puede estar expuesta la información de los pacientes,

los activos de información de las empresas relacionadas con la salud, y los casos de afectaciones al área de la salud por ciberataques

En virtud de ello el presente documento presenta una investigación exploratoria, en la que se exponeuna serie de casos que muestran la relación que existe entre la ciberseguridad y la salud.

Ciberataque: La última amenaza de salud para las farmacéuticas.

La figura tres muestra los ataques recientes a la industria de la salud durante 2017 y 2018.

Figura 3. Ataques recientes a la industriade la salud.

Fuente: Data Breach today, The Straits Times, Healthcare News, 2018.

Según la Agencia Bloomberg, 2018, las empresas que gastan miles de millones para probar drogas de vanguardia, se arriesgan a que sus resultados preliminares sean robados o secuestrados por delincuentes profesionales o ciber-terroristas, algunos de ellos patrocinados por estados.

Terrell, la nueva directora digital y detecnología de Glaxo Smith Kline Plc, supervisa la ciberseguridad del gigante farmacéutico británico. A medida que los piratas informáticos intensifican sus ataques contra las empresas de salud, la ejecutiva trata de evitar que roben todo, desde datos de pacientes hasta secretos de medicamentos.

> "Proteges información sobre tus empleados, pacientes, proveedores de atención médica y la propiedad intelectual de un negocio multimillonario" dijo en una entrevista. "Soy la línea de defensa" (Data Breach today, The Straits Times, Healthcare News, 2018).

Si bien es suficientemente malo que los hackersroben números de cuentas bancarias o correos electrónicos, es aún peor cuando exponen datos de salud comprometedores, lo que puede minar seriamente las relaciones personales y profesionales.

En muchos sentidos, los datos de atención médica se consideran mucho másprivados que los datos financieros.

Es mucho más difícil volver a ponerlos bajo llave", dijo John Halamka, director de información del BethIsrael Deaconess Medical Center en Boston, uncentro afiliado a Harvard.

Desde junio del 2017, cuando un ataque generalizado azotó a varias compañías, incluida la gigante farmacéutica estadounidense Merck & Co., los fabricantes de medicamentos informaron intentos más frecuentes y sofisticados de penetrar en sus servidores. Biogen Inc., Amgen Inc. y Celgene Corp. han dicho en informes regulatorios recientes, que los ataques cibernéticos están creciendo en intensidad y son cada vez más difíciles de detectar.

La figura (4) muestra la noticia en la que se determina que, debido a los ataques demalware desde dentro de los hospitales, existela necesidad de que las imágenes sean cifradaspara protegerlas de los ciberataques.

Figura 4. Ataques de malware desde dentro de hospitales expone la necesidad de encriptar imágenes médicas.

Fuente: Health IT & CIO Report, 2019.

Las compañías de salud están ampliando la búsqueda de ciber-defensores fuera de su sector. Glaxo trajo a Terrell de Walmart StoresInc. en julio 2017, para supervisar la estrategiadigital y de datos de la farmacéutica.

Después de sufrir un ataque que calificó de "paralizante", Reckitt Benckiser Group Plc contrató a Seth. Cohen de PepsiCo Inc. para convertirse en su director de información. Otras compañías están actualizando el software, trabajando con rivales para evitar daños y buscando miembros de la junta con experiencia en ciberseguridad.

No hacerlo puede ser costoso: cada violación en el sector de la salud cuesta más de US$5 millones en promedio, según Bank of America Corp. Reckitt Benckiser dijo que el ataque de junio 2017 tuvo un efecto de 90 millonesde libras (US$ 128 millones) en las ventas, mientras que Merck dijo que interrumpió las operaciones globales desde la fabricación hasta la investigación y, que su previsión de beneficios para 2017 hubiera sido más altasi no fuera por el ataque.

En octubre 2017, la farmacéutica dijo que esperaba algún impacto residual, principalmente en el primer semestre de 2018, en tanto toma medidas de protecciónadicionales.

Las pérdidas de datos podrían volverse más costosas cuando entren en vigencia nuevas normas europeas en mayo del 2018. El Reglamento General de Protección de Datos exige multas de hasta el 4% de los ingresos anuales en todo el mundo, para las compañíasque no cumplen con los requisitos y les dan a los consumidores más control sobre cómo se usa su información.

El impacto financiero ya ha sido alto, y si los reguladores van a multar a las empresas además de eso, pueden tomarlo como un indicador potencial de que hay un riesgo bastante mayor para este sector, segun Beijia Ma, estratega de Bank of America en Londres.

Más de la mitad de quienes respondieron una encuesta a ejecutivos farmacéuticos, biotecnológicos y de dispositivos médicos, dijeron el año pasado que están priorizando las inversiones en software y encriptación, según la consultora KPMG LLP.

Los piratas informáticos respaldados por gobiernos son considerados la mayor amenaza, según la encuesta. “Hay muchos, muchos más ataques exitosos y más datos robados que nunca; un crecimiento exponencial en la pérdida de datosy la corrupción de datos”, dijo Michael Ebert, especialista en cibernética de KPMG. Entrelas empresas europeas, dijo, ha habido una “pérdida de propiedad intelectual que no se hadivulgado por completo”.

Si bien los hospitales tienen una gran cantidad de información sobre pacientes, no pueden pagar el mismo nivel de protección que sectorescomo los servicios financieros, dijo Halamka,el ejecutivo de Beth Israel.

Los hackers que buscan datos personales van a “ir a donde hayamucha información y no tan buena seguridad”,dijo. (Agencia Bloomberg, 2018).

Los hospitales: blanco prioritario de los ciberataques

Para la Asociación de hospitales de Puerto Rico, 2018, el campo de la salud es una de las industrias más vulnerables para los ataques cibernéticos.

Durante la última década, los titulares muestran cómo va en aumento la exposición de la información confidencial y privilegiada de los clientes a través de todos los sectores de la sociedad.

Sin embargo, el campo de la salud es un campo fértil de información, la cual se debe custodiar y velar por el manejo de la información delicada de los pacientes.

El 25 % de las organizaciones relacionadasa la salud, que participaron en la encuesta global de percepción del riesgo cibernético en coordinación entre Marsh-Microsoft del 2017, indicaron ser víctimas de un ataque cibernético.

Marsh Saldaña participa activamente en la práctica de salud de Estados Unidos. Aprovechamos el capital intelectual, el análisis y la tecnología de todas las compañías de MMC en un enfoque sin fisuras y colaborativo.

Un ejemplo de esto es el informe de Holding Healthcare to Ransom, del Global Risk Center, en asociación con Oliver Wyman y Marsh, con base en los hallazgos de la encuesta global de percepción del riesgo cibernético de Marsh-Microsoft 2017, éste subraya la extrema vulnerabilidad de la industria de la salud frente a los ciberataques, en comparación con otros sectores.

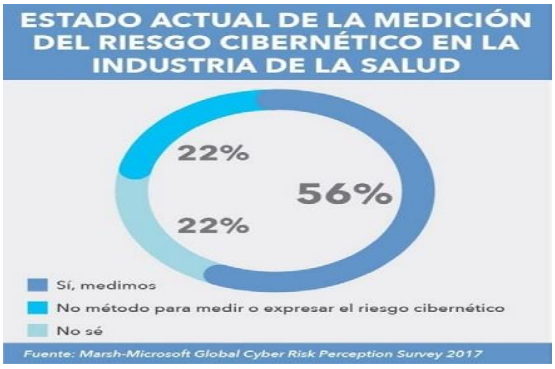

Figura 5. Estado actual de la medición del riesgo cibernético en la industria de la salud.

Fuente: MarshMicrosoft Global Cyber RiskPerception Survey, 2017.

Con las inversiones recientes en tecnología y capital humano, Marsh ahora tiene la capacidadde aprovechar el conocimiento de 10.000 transacciones de seguros por año, más de 15 millones de reclamaciones históricas y muchos otros puntos de datos.

Éstos nos ayudana evaluar alternativas y tomar decisiones informadas con respecto a la retención de riesgos, la transferencia de éstos y evaluar diversas opciones presentadas para encontrar la mejor opción para los clientes (Asociación dehospitales de Puerto Rico, 2018).

La figura (5) muestra el estado actual de la medición del riesgo cibernético en la industria de la salud, en el que se aprecia que el 56% delas empresas encuestadas sí miden el riesgo cibernético.

Un ciberataque paraliza 16 hospitales de Reino Unido y les exige dinero

El Portal El País, 2017, el 12 de mayo publica que se ha llevado a cabo un ataque internacionalen el que varios países y organizaciones se han visto afectadas. Varios hospitales inglesesfueron objeto de un ciberataque a gran escala,que impidió a los profesionales acceder a sus ordenadores y provocó el desvío de numerosos pacientes de urgencias, información que fueconfirmada por el servicio nacional de salud (NHS, por sus siglas en inglés).

El ataque afectó simultáneamente a ordenadores y teléfonos de al menos 16 hospitales y centros de salud de Londres, Nottingham, Herefordshire, Blackburn y Cumbria, según el NHS. Se trató de un ataquede ransomware, similar al que afectó al centro corporativo de Telefónica y otras empresas españolas.

En las pantallas de los ordenadoresinfectados por el virus informático, de origen desconocido, aparecía un mensaje que exigía un rescate pecuniario (300 dólares a una cuenta en bitcoin, según capturas de pantallas publicadas en la prensa y redes sociales) a cambio de acceder al sistema, como se puedeapreciar en la figura (6).

El ataque obligó a apagar los ordenadores en diversos hospitales y los médicos tuvieron que utilizar lápiz y papel, según testimonios recogidos por la BBC. Varios hospitales tuvieron que cancelar citas y solicitaron a los pacientes que eviten acudir salvo en casos de verdadera urgencia.

Figura 6. Mensaje exigiendo rescate pecuniario a los hospitales afectados.

Fuente: El País, 2017.

Razones por las que la asistencia médica se ha vuelto más susceptible a los ataques cibernéticos

En el Portal de noticias Healt IT & CIO Report, Garrity, 2019 publica que la atención médica seestá convirtiendo en un objetivo más importantepara los ataques cibernéticos debido a muchas razones, como los tipos de datos almacenadosy la falta de gasto en ciberseguridad.

The Next Web describió cinco razones porlas que los hospitales, los sistemas de salud y otros agentes de atención médica se han convertido en fuentes más comunes de ataques cibernéticos.

El valor de los datos de atención médica: en el mercado negro, un registro de salud de un solo paciente podría venderse por alrededor de $ 1,000. Estos registros incluyen números de seguro social, medicamentos e información de tarjetas de crédito, lo que hace que los ataquesa gran escala valgan millones. 2.

La creciente complejidad de los sistemas de salud: los sistemas de tecnología de los hospitales son cada vez más complicados, confiando en una red interconectada de dispositivos. Para lospiratas informáticos, solo se necesita atacar una vulnerabilidad en un solo dispositivo para destruir toda la red.

Atención errónea de las actualizaciones tecnológicas: los hospitales están más dispuestos a gastar dinero en nuevos equipos médicos que en ciberseguridad y soluciones operativas.

La falta de comprensión: algunos hospitales no tienen equipos de ciberseguridado incluso departamentos de TI, ya que su personal mínimo se centra en mejorar los resultados de salud en lugar de pensar en la seguridad.

La falta de fondos: mejorar losestándares de la tecnología de seguridad requeriría que los

hospitales y los sistemas de salud paguen una gran cantidad de dinero, más allá de la infraestructura

Estas organizaciones de atención médica tendrían que pagar precios más altos por episodio de paciente e implementar más restricciones internas en las nuevas adquisiciones de tecnología.

En la figura (7) se aprecia la noticia publicada pornel portal Health IT & CIO Report.

Figura 7. R azones por las que el áreade salud se ha vuelto más susceptible a los ciberataques.

Fuente: Health IT & CIO Report,2019.

La violación de datos de un centro de rehabilitación expone millones de registros de pacientes

El portal de noticias de Becker denominada Health IT & CIO Report (Park, 2019), da a conocer que los datos de identificación personal de aproximadamente 145.000 pacientes en el centro de tratamiento de adicciones de Steps to Recovery con sede en Levittown, Pa. y el Centro de Recuperación de Adicciones de Ohio en Columbia, fueron expuestos en una base dedatos en línea, informa CNET.

El director de operaciones de Pasos hacia la recuperación, Cory Cooper, dijo a CNET que una firma de seguridad informática investigará la violación. El centro aún tiene que notificar a los pacientes afectados, y el Sr. Cooper señalaque lo harán si la investigación lo considera necesario, por ejemplo, si se demuestra que lainformación ha sido visitada y / o utilizada por piratas informáticos con intenciones maliciosas.

Palmetto Health alertó a 23,000 pacientes de ataque de phishing.

Según el HIPAA Journal, Palmetto Health, consede en Columbia, S.C., correos electrónicos que contenían un enlace malicioso fueron enviados a los empleados del hospital. Si los empleados hacían clic en el enlace malicioso, se les dirigía a un sitio web que les pedíaque ingresaran sus credenciales de correoelectrónico. El hacker luego obtenía acceso a sus cuentas de correo electrónico.

Una investigación encontró que los correos electrónicos del hacker fueron enviados en noviembre de 2018. La revisión del incidente se completó el 19 de febrero de 2019 y reveló quela información de salud protegida de 23.811 pacientes había sido expuesta, informó el HIPAA Journal.

Los nombres de los pacientes y la información de tratamiento o consulta se vieron afectados. Un número limitado de correos electrónicoscontenía información del seguro de salud, números de Seguro Social o información financiera (Mackenzie, HIPAA Journal, 2019).

En la figura (8) se aprecia el portal de noticias de Health IT & CIO Report publicando la noticia del ataque de phishing.

Figura 8. Palmetto Health alerta un ataque de phishing a correos de 23.000pacientes.

Fuente: Health IT & CIO Report, 2019.

Los hospitales de Texas registran la mayoría de los ataques cibernéticos en Estados Unidos

Desde 2014, más de 1,4 millones de texanos han sufrido robo de sus registros de salud, lo que hace que los hospitales en el estado corran el mayor riesgo de ataques cibernéticos, segúndatos del HHS y citados por la Radio Pública de Texas.

El año pasado, más de 9 millones de estadounidenses fueron afectados por ataques cibernéticos.

Las infracciones ocurrieron en hospitales, aseguradoras de salud y otras organizaciones de esta área. Según el informe,cuatro de los últimos cinco años, Texas ha liderado el país en infracciones totales de piratería informadas a HIPAA.

Parte de la razón de los numerosos ataques es debido a la población del estado. Texas tiene más hospitales que muchos otros estados, lo que lo hace más susceptible a los ataques cibernéticos.

Por lo general, los hospitales y los sistemas de salud en Texas sufren de piratería informática. Sin embargo, en 2018, un error de codificación expuso los datos de más de 1,2 millones de personas (Mackenzie, Health IT & CIO Report, 2019).

La figura (8) muestra la publicación de Health IT & CIO Report relacionada con que los hospitales de Texas son los que más ciberataques sufren en Estados Unidos.

Figura 9. Registros de los hospitales deTexas son los más ciberatacados en Estados Unidos.

Fuente: Health IT & CIO Report, 2019.

El Departamento de Seguridad Nacional re-edita la advertencia cibernética en dispositivos médicos

Una nueva investigación llevó al Departamento de Seguridad Nacional, a reenviar una advertencia sobre vulnerabilidades de seguridad cibernética en dispositivos médicos electrónicos, según el Digital Journal.

En la alerta, el departamento advirtió a los hospitales y clínicas de salud que utilizan dispositivos médicos electrónicos, incluidos los dispositivos quirúrgicos y de anestesia, ventiladores, bombas de infusión de medicamentos y desfibriladores externos. Los monitores de pacientes, los equipos de laboratorio y análisis y otros sistemas digitales también son vulnerables a los ataques cibernéticos.

Los investigadores descubrieron que muchos dispositivos médicos electrónicos están diseñados con contraseñas "codificadas", lo que brinda a los piratas informáticos una oportunidad para modificar la configuración o instalar firmware malicioso. La FDA ha expresado preocupaciones similares (Mackenzie, HealthIT & CIO Report, 2019).

Ataques de malware desde dentro de los hospitales, exponen la necesidad de cifrar imágenes médicas

Los expertos israelíes en ciberseguridad crearon un malware que puede alterar las tomografías computarizadas para indicar que un paciente sano tiene cáncer y que un enfermoestá sano, según The Washington Post.

Un investigador del Centro de Investigación de Seguridad Cibernética de la Universidaddijo que creó el malware para resaltar las vulnerabilidades en los equipos de imágenes médicas críticas y las redes que transmitenesas imágenes a los ataques cibernéticos. Uno de los investigadores, Yisroel Mirsky, dijo al Post que los hospitales son vulnerables a los ataques porque tienden a preocuparse más por proteger los datos compartidos entre los hospitales y con otros médicos, ignorando "lo que sucede dentro del propio sistema hospitalario".

Después de que se les dijo a los radiólogos que las imágenes fueron afectadas por malware y se les dio un segundo conjunto de imágenes, todavía se afectó el 60 por ciento de las mismas.En las imágenes que eliminaron nódulos cancerosos, los radiólogos no diagnosticarona los pacientes realmente enfermos el 87 por ciento de las veces.

Aunque estos estudios se centraron en las imágenes de cáncer de pulmón, el malware puede atacar las tomografías computarizadas para detectar tumores cerebrales,enfermedades cardíacas, coágulos de sangre, lesiones de la columna vertebral, fracturas de huesos, lesiones de ligamentos y artritis. (Mackenzie, Health IT & CIO Report, 2019).

UCLA Health pagará $ 7.5M para resolver un caso de acción colectiva por violación de datos De acuerdo con la revista HIPAA, UCLA Healthacordó pagar $ 7.5 millones para resolver una demanda colectiva presentada por pacientes después de una violación de datos que puso en riesgo su información personal y de salud.

El sistema de salud de la universidad descubrióactividades sospechosas en su red en octubre de 2014 y se contactó con el FBI para pedir ayuda. En ese momento, se asumió que no sehabían comprometido los registros médicos, pero en mayo de 2015, se descubrió que los piratas informáticos habían obtenido acceso a la información médica protegida de los pacientes.

Cerca de 4,5 millones de pacientes se vieron

afectados por la violación de datos.

La Oficina de Derechos Civiles de HHS determinó que UCLA Health seguía el protocolo apropiado y estaba satisfecho con los esfuerzos posteriores al incumplimiento del sistema de salud universitario para mejorar la seguridad, según el Diario.

Pero los pacientes no estaban tan satisfechos y presentaron una demanda colectiva, argumentando que UCLA Health no les notificó la violación de los datos de manera oportuna, hubo una violación del contrato y que no proteger la privacidad de los pacientes fue negligencia, según al informe.

UCLA Health alertó a los pacientes el 15 de julio de 2015 sobre la violación de datos. HIPAA requiere que las organizaciones notifiquen al personal afectado en menos de 60 días desde el descubrimiento de que la información de salud personal se ha visto afectada. Los pacientes declararon que UCLA debió haberlos notificado más rápidamente, ya que el incidente ocurrió nueve meses antes de su notificación. Los pacientes tuvieron hasta el 20 de mayo para objetar el acuerdo. Pudieron reclamar hasta $ 5,000 para cubrir los costos de protección de identificación y hasta $ 20,000 por cualquier pérdida o daño causado por la violación de datos.

De los $ 7.5 millones del acuerdo, $ 2 millones se reservaron para reclamaciones de pacientes.Los otros $ 5.5 millones se destinaron a UCLA Health desarrollando un fondo de ciberseguridad para mejorar las defensas de seguridad (Mackenzie, Health IT & CIO Report, 2019).

En la figura se puede observar la publicación de Health IT & CIO Report informando que UCLA Health tuvo que pagar

$7,5 millones de dólares para resolver un caso de acción colectiva por violación de datos.

Figura 10. UCLA Health paga $7,5 millones para resolver un caso de acción colectiva por violación de datos.

Fuente: Health IT & CIO Report, 2019.

Los datos médicos se están volviendo más vulnerables a los ataques cibernéticos. Aquí está cómo están luchando de inicio lasempresas.

La figura 10 muestra el número de violaciones a datos, destacando la escaladacreciente que en 2018 llegó a 365 mil.

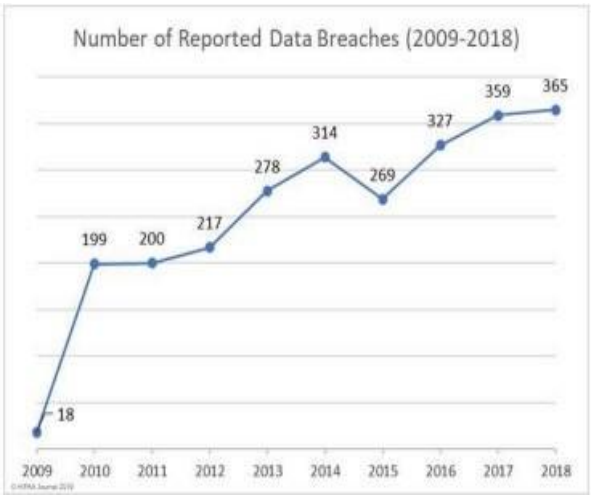

Figura 10. Número de violaciones de datosreportados (2009-2018).

Fuente: HIPAA Journal, 2019.

Las nuevas empresas de ciberseguridad están trabajando para defender los datos de pacientesde piratas informáticos y asegurar el futuro de la asistencia de salud.

¿De dónde vienen estos datos?

La inseguridad cibernética en el cuidado de la salud está empeorando, especialmente cuandose trata de proteger los datos del cuidado de lasalud.

Entre 2009 y 2018, hubo más de 2,500 violaciones de datos de salud de más de 500 registros cada una.

Desde la mejora de la seguridad en los dispositivos médicos hasta la privacidad del paciente, estamos viendo una nueva clase de nuevas empresas de ciberseguridad que buscan específicamente ayudar a asegurar el futuro de la atención médica.

Las empresas emergentes como Cynerio analizan el comportamiento de los dispositivos médicos para identificar posibles actividades maliciosas.

Otros, incluido CyberMDX, usan inteligencia artificial - IA para agregar capas adicionales de protección para dispositivos médicos conectados.

El riesgo de que los piratas informáticos exploten las cadenas de suministro de software

de dispositivos médicos para interrumpir las operaciones de atención médica es una de las principales preocupaciones. La figura 11 muestra por qué las cadenas de suministro de software para dispositivos médicos son complejas.

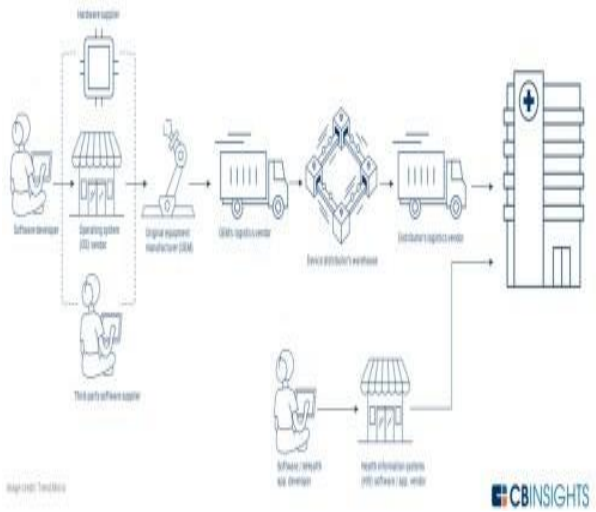

Figura 11. Las cadenas de suministro de software para dispositivos médicos son complejas.
Fuente: Trend Micro, 2019.

Se sabe que los piratas informáticos se infiltranen las cadenas de suministro y dañan los sistemas operativos de software al instalar una "puerta trasera", una vulnerabilidad que permitea los piratas informáticos evitar los esquemas de autenticación.

¿Qué hay en internet?

Los dispositivos médicos que son accesibles remotamente a través de Internet son particularmente vulnerables.

Imagine cada dispositivo de acceso remoto en un hospital, como un posible punto de entrada para crackers (ciber-delincuentes).

Un caso de IA equivocada.

A principios de abril 2019, los investigadores de la Universidad BenGurion del Negev demostraron que los piratas informáticos pueden acceder a las exploraciones médicas en 3D delos pacientes y agregar o eliminar imágenesde tumores malignos, engañando a algoritmos artificialmente inteligentes y colocando a los pacientes en riesgo de diagnóstico erróneo.

En la figura 12 se muestra una tomografía computarizada que fue manipulada por ciberdelincuentes y descubierta por los investigadores de la Universidad Ben-Gurion del Negev.

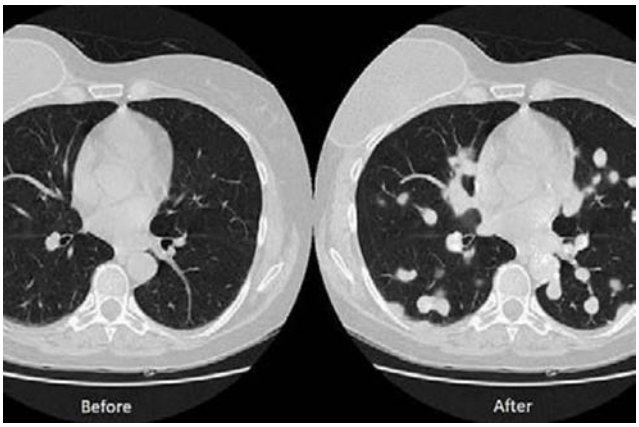

Figura 12. Tomografía computarizada manipulada por ciberdelincuentes.
Fuente: CB Insights, 2019.

La amenaza cibernética genómica.

Las pruebas de ADN son una industria de $ 5.2B,según el Consenso de analistas de la industriade CB Insights. junto con el crecimiento de la industria de pruebas de ADN, se almacenan más datos genéticos y pueden ser altamente sensibles.

Varios ataques genómicos ya han sido demostrados y se pueden anticipar más.El año pasado, MyHeritage, un servicio israelí de pruebas de genealogía y ADN, expuso accidentalmente las cuentas de 92M relacionadas con los servicios de ascendencia en línea de la compañía (no se filtraron datos de ADN).

La combinación masiva de datos genómicos también plantea problemas de privacidad. Los investigadores han mostrado esquemas de re-identificación en los que los atacantes pueden inferir la identidad de una persona mediantela correlación de múltiples puntos de datos incompletos, como datos genómicos parciales, etc. (CB Insights, 2019).

Los datos de atención médica se consideran mucho más privados que los datos financieros.Es mucho más difícil volver a ponerlos bajo llave. los ataques cibernéticos están creciendo en intensidad y son cada vez más difíciles de detectar. (Agencia Bloomberg, 2018).

Las organizaciones de salud también enfrentan riesgos operativos internos, como récords impresos perdidos o robados, acceso depersonas que no son empleados a áreas restringidas, entre otros. De hecho, el errorhumano y el uso indebido de información son notorios en la industria de la salud.

Es la únicaindustria que tiene más amenazas internas detrás de violaciones de datos, que

externos. Las altas implicaciones (seguridad humana y datos confidenciales) hacen que la habilidad de recuperarse luego de que la informaciónes comprometida ya sea por error humano oun ataque cibernético sea imperativa para la industria (Asociación de hospitales de Puerto Rico, 2018).

Las grandes compañías de tecnología, incluidas GE Healthcare, Philips y Silex Technologies recibieron advertencias. Silex Technologies fabrica productos de electrocardiogramas inalámbricos, y ciertos sistemas de tomografía computarizada de Philips pueden ser susceptibles a ataques cibernéticos.

Las soluciones para estas vulnerabilidades potenciales no deben depender únicamente de los fabricantes de dispositivos, sino tambiénde los usuarios, según May Wang, PhD, cofundador y director de tecnología de Zingbox, una compañía de seguridad de Internet para dispositivos médicos (Mackenzie, Health IT & CIO Report, 2019).

Estudios demostraron que tomografías computarizadas atacadas por malware son una amenaza inmediata. En un estudio ciego que involucró tomografías computarizadas reales, 70 de ellas fueron alteradas por malware. Tres radiólogos expertos fueron engañados para realizar diagnósticos erróneos lo que ocurrió las tres veces, informó el Post (Mackenzie, HealthIT & CIO Report, 2019).

CONCLUSIONES

A lo largo de los casos expuestos en el presente documento, se ha demostrado la importancia que tuvo, tiene y tendrá la ciberseguridad para todas las áreas, pero principalmente para la médica, debido a la poca importancia que prestan a la misma las instituciones relacionadas con el área de salud.

A lo mencionado hay que agregar que, por la falta de concientización de la importancia de la seguridad de información en el campo de la salud, no se destina la suficiente cantidad de recursos para su desarrollo, sino los necesarios para dar cumplimiento a ciertas normas y estándares exigidos por algunos organismos de control como el HIPAA, la Oficina de Derechos Civiles de HHS, la FDA, Departamento de Salud y Servicios Humanos (HHS), entre otros, por lo que, los ciberdelincuentes pueden dar rienda suelta a sus oscuros actos en favor de sus ilegales intereses.

Se debe partir de la premisa de que no se debe menospreciar a estos individuos, en vista de que invierten la mayoría de su tiempo,junto a una taza de café y su clandestinidad,a la investigación de la forma más adecuada de afectar a los sistemas informáticos interconectados en general, que usan a la Internet como su autopista de comunicación con el mundo.

Por tanto, ningún esfuerzo será suficiente pues, mientras se está tratando de minimizar una afectación por parte de las empresas relacionadas con la salud, los cibercriminales ya están desarrollando nuevas formas de ataque.

RECOMENDACIONES

Las compañías de salud deben ampliar la búsqueda de ciber-defensores fuera de su sector (Agencia Bloomberg, 2018).

Si bien los riesgos son reales y han sido reconocidos por la industria, muchas organizaciones de la salud aún tienen que establecer e implementar un marco holístico, de cumplimiento y supervisión adecuada por parte de las juntas de directores, cuando se tratade la seguridad de los datos confidenciales.

Estas organizaciones deben tomar medidas proactivas para aumentar la visibilidad de los problemas de riesgos cibernéticos y distribuir la responsabilidad de la gestión del riesgo cibernético a través de toda la empresa, ya que todos somos responsables del manejo de la información del paciente en todas sus fases (Asociación de hospitales de Puerto Rico, 2018).

Para combatir los ataques cibernéticos,los hospitales deben desviar dinero y recursos ala ciberseguridad. Pero en clínicas rurales, esto puede ser un reto.

La atención médica necesita ponerse al día con los delincuentes cibernéticos,según el Sr. Lunsford. Para hacerlo, los hospitales y los sistemas de salud deben invertirmás dinero en ciberseguridad (Mackenzie, Health IT & CIO Report, 2019).

“Los líderes de seguridad deben hacer más para colaborar conDHS y otras agencias, como HHS y NIST, quehan centrado sus esfuerzos para proteger los dispositivos médicos críticos”,

dijo el Dr. Wang a The Digital Journal (Mackenzie, Health IT & CIOReport, 2019).

Para evitar que el malware altere las exploraciones de CT y MRI, los hospitales deben instalar encriptación de extremo a extremo en su red de sistemas de comunicación y archivo de imágenes.

Los hospitales también deben firmar digitalmente todas las imágenes, de acuerdo con el Post (Mackenzie, Health IT & CIO Report, 2019).

REFERENCIAS BIBLIOGRÁFICAS

Agencia Bloomberg. (5 de Febrero de 2018). *Gestión.* Obtenido de Gestión :https://gestion.pe/economia/ciberataqueultima-amenaza-salud-farmaceuti- cas-226483

Asociación de hospitales de Puerto Rico. (20 de Octubre de 2018). *Asociación de hospita-les de Puerto Rico.* Obtenido de Noticias: http://hospitalespr.org/los-hospitales-blancoprioritario-de-los-ciberataques/

CB Insights. (22 de Abril de 2019). *Research Briefs.* Obtenido de Research Briefs: https://www.cbinsights.com/research/healthc are-data-cyber-attacks/

Health Insurance Portability and Accountability Act - HIPAA Journal. (3 de Julio de 2019). *Ley de Transferencia y Responsabilidad de Seguro Médico - HIPAA Journal.* Obtenido de HIPAA Journal: https://www.hipaajournal.com/smaller-healthcare-providers-struggling-toimplement-healthcare-cybersecurity-bestpractices/

Mackenzie, G. (9 de Abril de 2019). *HealthIT & CIO Report.* Obtenido de Becker: https://www.beckershospitalreview.com/cybersecurity/texas-hospitals-record-mostcyberattacks-in-us.html

Mackenzie, G. (24 de Abril de 2019). *Heal-th IT & CIO Report.* Obtenido de Bec- ker: https://www.beckershospitalreview.com/cyb ersecurity/5-reasons-healthca- rehas-becomemore-susceptible-to-cyberattacks.html

Mackenzie, G. (4 de Abril de 2019). *Health IT & CIO Report.* Obtenido de Becker: https://www.beckershospitalreview.com/cyb ersecurity/department-of-homeland-securityreissues-cyber-warning-on-medical-devices.html

Mackenzie, G. (3 de Abril de 2019). *HealthIT & CIO Report.* Obtenido de Becker: https://www.beckershospitalreview.com/cybersecurity/hospital-malware-attacks-fromwithin-exposes-need-to-encrypt-medicalimaging.html Mackenzie, G. (27 de Marzo de 2019). *HealthIT & CIO Report.* Obtenido de

Becker: https://www.beckershospitalreview.com/cyb ersecurity/ucla-health-topay-7-5m-to-settledata-breach-class-action-case.html

Mackenzie, G. (12 de Abril de 2019). *HI- PAA Journal.* Obtenido de Palmetto Health: https://www.beckershospitalreview.com/cyb ersecurity/palmetto-heal- thalerts-23-000patients-of-phishing-attack.html

Park, A. (22 de Abril de 2019). *Health IT & CIO Report.* Obtenido de Becker: https://www.beckershospitalreview.com/cyb ersecurity/rehab-center-data-breach-exposesmillions-of-patient-records.html

Portal El País. (12 de Mayo de 2017). *El País.* Obtenido de Tecnología: https:/elpais.com/tecnologia/2017/05/12/act ualidad/1494602389_458942.html

Rouse, M. (Mayo de 2018). *TechTarget.* Obtenido de Search Security: https://searchsecurity.techtarget.com/definiti on/cybersecurity

Wikipedia, l. E. (8 de Abril de 2019). *Wikipe-dia.* Obtenido de La Enciclopedia Libre: https://es.wikipedia.org/wiki/Ciencias_de_la _salud