BACSIRT
Vamos Buenos Aires | Centro de Ciberseguridad
Agencia de Sistemas
www.ba-csirt.gob.ar
BOLETÍN N°47
FECHA DE PUBLICACIÓN
30 | 11 | 18

SALUD Y TIC:
UN SINFIN DE POSIBILIDADES Y DESAFÍOS

Como ya hemos dicho muchas veces, en la actualidad la tecnología ha impregnado cada rincón. Si nos proponemos hacer el ejercicio de identificar algún aspecto de la vida que aún se encuentre "libre de tecnología", lo más probable es que no logremos encontrar ni siquiera un ejemplo. Ello tiene mucho sentido dado las enormes ventajas que las innovaciones tecnológicas nos ofrecen y las infinitas nuevas posibilidades de acción que se abren gracias a su incorporación.

Siguiendo esa línea, en esta oportunidad decidimos ocuparnos de pensar y reflexionar acerca del **vínculo entre Salud y Tecnologías** en sentido amplio, tanto es sus los aspectos positivos como así también, en lo que refiere a la seguridad de la información derivada del mismo y su potencialidad de riesgo.

"La información que las instituciones de salud administran de sus pacientes puede resultar particularmente interesante para los atacantes, quienes esperan convertir en ganancias los datos que logran robar, o bien, poner en riesgo las operaciones de los prestadores médicos."

- Sebastián Stranieri

Tal como indica Sebastián Stranieri, CEO de la firma VU Security, "*hasta hace muy poco tiempo, la tecnología sólo era incorporada a la salud en la innovación de dispositivos o máquinas. Hoy, sin embargo, atraviesa también los negocios y los procesos; desde el alta y baja de pacientes, el seguimiento de tratamientos e incluso el almacenamiento de la historia clínica. La información que las instituciones de salud administran de sus pacientes puede resultar particularmente interesante para los atacantes, quienes esperan convertir en ganancias los datos que logran robar, o bien, poner en riesgo las operaciones de los prestadores médicos.*"

En el mismo sentido, La empresa de seguridad Positive Technology[1] observó un incremento de los ataques informáticos (a nivel general) de un 40% entre el primer y el segundo trimestre de 2018. El mismo informe revela que de la información más buscada por los ciberdelincuentes, el 30%

corresponde a registros médicos. Y la clasificación de la información robada del sector sanitario, indica la siguiente proporción:

- 53% se trata de datos personales
- 37% registros médicos (historias clínicas)
- 4% credenciales
- 2% secretos corporativos
- 2% información sobre tarjetas
- 2% base de datos de clientes

Asimismo, las formas que los ciberdelincuentes utilizan para atacar a dicho sector responden al siguiente recuento:

- 38% malware
- 38% credenciales de usuarios
- 23% ingeniería social
- 15% ataques vía web
- 8% hacking

Un informe del segundo trimestre de 2018 elaborado por la empresa de seguridad Positive Technology, revela que de la información más buscada por los ciberdelincuentes, el 30% corresponde a registros médicos.

Como vemos, la digitalización de la información en lo que refiere a la salud, si bien otorga grandes facilidades en términos de comodidad, precisión en los diagnósticos y mejoras en los resultados de las prácticas, no escapa de los problemas típicos relativos a la seguridad informática; muy por el contrario.

En relación a ello, continúa diciendo Stranieri: "***la Ley Nacional 14.494 ayuda a facilitar la asistencia sanitaria al establecer que debe haber un 'sistema de historia clínica electrónica única de cada persona desde el nacimiento hasta el fallecimiento'***. *Esta unificación requiere que las entidades sanitarias optimicen sus medidas de seguridad para garantizar la privacidad de los datos durante todo el ciclo de vida, en las actividades que utilicen estos datos.*

El acceso a la historia clínica de cada persona debe ser seguro y quedar en la privacidad de la relación médico-pasiente.

Adicionalmente, las regulaciones existentes sobre Protección de Datos Personales se van volviendo cada vez más rigurosas, en consonancia con los efectos de los ataques cibernéticos y la creciente importancia de los datos almacenados en el sistema de salud, que generan a las instituciones la necesidad de estar a la altura del desafío de poder brindar un servicio de excelencia con una administración de datos adecuada. Si bien se ha avanzado en materia de seguridad en el rubro Salud, las medidas de seguridad informática son muy recientes y en muchos casos, su implementación todavía está siendo analizada. Como resultado, los atacantes están tecnológicamente más avanzados que las instituciones médicas.

Desde hace varias décadas existe una nueva especialidad en la Medicina llamada Informático en Salud o Informático Médico.

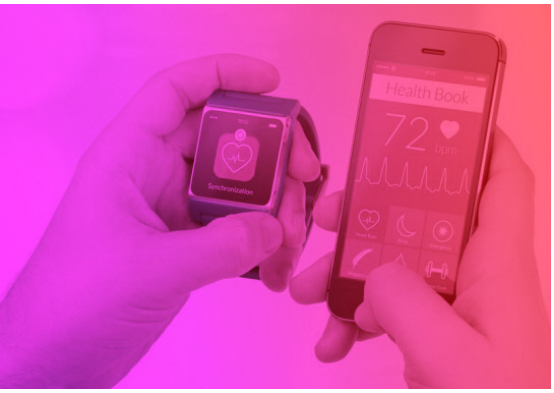
Para reducir esta brecha, ***es fundamental trabajar en la concientización de los profesionales de salud y motivar la implementación de medidas de seguridad en las instituciones para reducir las amplias posibilidades de que la identidad digital de los pacientes, así como su historial clínico, sea vulnerada****. Desde el profesional sanitario que deja la historia clínica abierta sin contraseña, abandonando distraídamente el lugar, pasando por sistemas que utilizan redes públicas y aplicaciones con validación simple y contraseñas poco robustas que pueden ser fácilmente quebrantadas, hasta arquitecturas informáticas que no han incorporado los conceptos actuales de ciberseguridad; todas son debilidades que pueden ser aprovechadas por los atacantes informáticos.*

Los dispositivos más vulnerables son aquellos sin contraseñas o con contraseñas poco robustas. Luego, le siguen aquellos dispositivos que no tienen instaladas las últimas actualizaciones o parches de seguridad y finalmente, aquellos que utilizan redes públicas para navegar*. De todos modos, en el futuro cercano y dado el nivel de los ataques actuales, las instituciones sanitarias deberán fortalecer, además, la seguridad de todo el instrumental médico que utilice facilidades computacionales o de IoT, ya que éstos también pueden ser víctimas de ataque. Una medida básica de protección es la utilización de software con el licenciamiento correcto, el cual debe mantenerse actualizado instalando los parches de seguridad pertinentes para evitar vulnerabilidades."*

En consonancia con el último punto desarrollado por Stranieri, Florencia Vilardel (parte del Equipo de BA-CSIRT) que se dedica a investigar sobre Salud y Tecnologías, publicó este año una nota en el sitio Ciberseguridad Latam[2] acerca de una vulnerabilidad encontrada en un modelo de marcapasos implantable[3] . Allí, ella decía: "*[...] Siguiendo mi investigación, encontré la publicación de una vulnerabilidad dentro del equipo monitor del paciente marca 'Medtronic' (modelo 'MyCareLink 24950') en la web del CERT para el control de Sistemas Industriales de EE.UU*[4] *. La misma fue reportada el 7 de agosto de 2018, con el identificador "ICSMA-18-219-01" -CVSS v3 4.9, por los investigadores Billy Rios, Jesse Young y Jonathan Butts, a la NCCIC (National Cybersecurity and Communications Integration Center) de Estados Unidos. La explotación exitosa de las vulnerabilidades halladas por estos investigadores, permitiría a un ciberdelincuente tener acceso físico a las credenciales del equipo y, con ellas, cargar datos inválidos a la red de Medtronic CareLink. Asimismo, el modelo afectado puede almacenar las contraseñas en un formato recuperable, permitiendo al ciberatacante usar esas credenciales para la autenticación de la red.*"

De lo dicho hasta aquí, por si nos quedaba alguna duda, queda más que claro que la implementación de las tecnologías en las diferentes áreas debe ir acompañada por procesos de alto grado de control y seguimiento de los alcances y potenciales riesgos que estas conllevan. Y, tal como se desprende de lo expresado por Vilardel, **cuando se trata de dispositivos que intervienen directamente en la salud de las personas, la responsabilidad con la que debe tratarse toda la**

Cuando se trata de dispositivos que intervienen directamente en la salud de las personas, la responsabilidad con la que debe tratarse la cuestión de la seguridad informática de los mismos es aún mayor, ya que lo que está en juego es nada menos que la vida.



Actualmente el vínculo entre salud y tecnologías abarca múltiples aspectos de la vida de las personas. Un ejemplo de ello son las aplicaciones y dispositivos existentes para llevar diferentes controles de su estado de salud.

cuestión es aún mayor, ya que lo que está en juego es nada menos que la vida. Por otra parte, saliendo de los extremos, como hemos mencionado anteriormente, los riesgos a la privacidad y al filtrado de información sensible también resultan preocupantes y merecen adecuada atención y tratamiento.

Al respecto, Stranieri expresa: "*una herramienta infaltable en la práctica de los profesionales de la salud es* ***el acceso seguro a la historia clínica de sus pacientes, que debe ser privado y de uso exclusivo de la relación paciente–médico. Lo mismo aplica con la validación de tratamientos autorizados, cuyo acceso debe ser exclusivo al paciente y al médico o equipo interviniente****. Es fundamental que todos los procesos médicos brinden la seguridad y confidencialidad necesaria al paciente, dada la importancia que esta información representa para cada individuo.*

Hoy en día, la ciberseguridad es un tema integral y horizontal a todo el sector médico. Es necesario revisar los procesos, aumentar la capacitación sobre temas de seguridad informática, fortalecer las aplicaciones y por supuesto, cuidar la identidad digital de los pacientes y los accesos a la infraestructura de la organización."

En este sentido, desde **BA-CSIRT** encontramos sumamente satisfactorio e interesante, como uno de los tantos caminos que los profesionales de la Seguridad Informática pueden transitar desde lo laboral y que demuestra la gran versatilidad e interdisciplinariedad que caracteriza al campo profesional de las tecnologías, la especialidad de "Informático Médico"; existente hace varias décadas. Así lo explica Daniel Luna, médico especialista en Medicina Interna, magister en Ingeniería de Sistemas de Información, doctor en Ingeniería Informática y jefe de los Departamentos de Informática Médica e Informática en Salud del Hospital Italiano: "*hay una disciplina, dentro de la medicina, que lleva más de 30 años. Inclusive, está reconocida en Estados Unidos y en países de Europa, y lo estará acá en breve, como una subespecialidad dentro de la medicina. Se llama informático en salud o informático médico. [...] En el hospital tenemos hace 16 años, desde 2001, una residencia de informática médica, que tiene una especialidad reconocida por el ministerio de Educación. Y estamos dictando una maestría a distancia, que en su segundo año ya tiene 150 alumnos [...] El objetivo es que alguien que esté trabajando en salud, haciendo sistemas de información, conozca el ecosistema de la salud (no tiene que saber atender pacientes), y que los que vengan de la salud conozcan el ecosistema de la información también. La idea de la transdisciplina es reforzar los conocimientos de la disciplina opuesta. El informático, en términos generales, es un gran traductor para el diseño, desarrollo e implementación de sistemas en el campo de la salud. Entonces, como los médicos tienen mucho poder y se resisten bastante a que les cambien la forma de trabajo, el objetivo es nivelar conocimiento, para actuar como facilitadores.*"[5]

Tal es la repercusión y el avance imparable de la aplicación de las tecnologías en las áreas de saludo que desde el Gobierno de la Ciudad

Sgún un informe presentado por la empresa de seguridad Positive Technology, el 30% de la información más buscada por los ciberdelincuentes corresponde a registros médicos.

han abierto la residencia de Informática Médica para tratar de emular el proceso educativo que ha comenzado el Hospital Italiano. Como decíamos más arriba, **la tecnología es el presente y será, sin dudas, el futuro. Cuanto mejor y más responsablemente aprendamos a usarla, mayores e increíbles cosas podremos hacer**. ▪

[1] https://www.ptsecurity.com/upload/corporate/ww-en/analytics/Cybersecurity-threatscape-2018-Q2-eng.pdf
[2] https://www.ciberseguridadlatam.com/2018/09/19/reglamentaciones-de-los-marcapasos-mantenerse-actualizado-para-no-ser-vulnerable/
[3] Pequeño dispositivo que se coloca en el pecho o el abdomen de los pacientes con deficiencia cardíaca a los fines de ayudarlos a controlar ritmos anormales. Estos dispositivos utilizan impulsos eléctricos, simulando a los del propio corazón, para hacer que el mismo pueda latir a un ritmo normal manteniendo, de ese modo, la vida del paciente.
[4] https://ics-cert.us-cert.gov/
[5] http://www.consensosalud.com.ar/informatico-en-salud-la-especialidad-del-futuro/