05/03/2024

¿Están realmente a salvo nuestros datos clínicos en la era digital?

Cada vez son más frecuentes los casos de ciberdelincuencia. Uno de los objetivos de los piratas informáticos son los hospitales y nuestros datos clínicos. El botín puede ser muy jugoso. ¿Estamos de verdad seguros?

En 1983 se estrenó una película mítica: Juegos de guerra. Que yo recuerde, es la primera que trata sobre hackers y ciberataques. Un joven Matthew Broderick accede a un sistema de inteligencia artificial militar y activa un simulacro de guerra nuclear con un rudimentario ordenador de los de la época.

Que la informática ha llegado para facilitarnos la vida, nadie lo discute ya: hoy en día tramitamos nuestras vidas a golpe de clic, sin mover el culo del sofá. Ahora bien, tengamos presente que cuanto más nos digitalizamos, mayor es la probabilidad de ser víctimas cibernéticas. Si bien, en el film, el ataque es una gamberrada juvenil, los ciberdelincuentes en la actualidad se mueven en las redes gracias a potentes computadoras y a sofisticados softwares.

Los hospitales son claves para el funcionamiento de toda sociedad, y cualquier bloqueo de su sistema informático provoca un colapso de consecuencias devastadoras. A finales de septiembre del 2020, una acción pirata bloqueó el sistema informático de un hospital de Düsseldorf, en Alemania. El resultado fue desastroso: se cerró el servicio de urgencias, y un paciente falleció al no poder administrarle su tratamiento, siendo considerado como el primer ataque informático a un hospital de la historia con víctimas.

Los ataques a hospitales españoles se han recrudecido desde la pandemia, tal y como confirma el Instituto Nacional de Ciberseguridad (INCIBE), que es el estamento que se ocupa de estos asuntos. No nos debe resultar extraño: el confinamiento ha impulsado el aumento del uso de las redes para mantener los tratamientos de aquellos que no podían salir de casa, para compartir información médica sobre la covid-19 con otros centros y, sobre todo, para informar a los familiares de los pacientes ingresados.

Exigencias de los piratas

Aunque nuestro país está considerado como la cuarta potencia internacional en ciberseguridad, nuestros centros sanitarios tienen muchos dispositivos conectados a internet que son puertas abiertas para los ciberdelincuentes. Los ataques se llaman ransomware, y consisten en la introducción de un programa malicioso (denominado en el argot malware) que bloquea los datos y las aplicaciones del hospital. Luego los piratas piden un rescate para su desbloqueo, normalmente en bitcoins para que no sea trazable.

El año pasado resultó muy marcado por los ciberataques. Solo en el primer trimestre se cuantificaron hasta cuarenta incidentes de seguridad. En el mes de marzo, los piratas accedieron a archivos médicos del Hospital Clínic de Barcelona y los hicieron públicos a través de Telegram. La filtración solo constituía el 1% y no eran de datos estructurados (es decir, nombre, fecha de nacimiento, etc), pero su publicación constituía una “fe de vida” al estilo de las peores mafias (como cuando secuestran a alguien y los captores envían una oreja por correo). Pedían más de cuatro millones de dólares y causaron un notable perjuicio al funcionamiento del hospital, puesto que los sanitarios tuvieron que adoptar las antiguas técnicas de trabajo analógico. La Generalitat aseguró que no pagaría el rescate y se reforzaron las medidas de protección.

Hace unas pocas semanas, el sistema de salud de Rumanía se ha colapsado por un ransomware que ha afectado a cientos de establecimientos sanitarios. Los atacantes pidieron un rescate a cambio de la clave de desbloqueo. Aunque las autoridades creen

haber identificado el tipo de malware utilizado, no han conseguido todavía dar con los autores del ataque. Lo cierto es que da miedo que tu historial médico ande a la vista de todos, ¿verdad?

Acceso a datos clínicos

Los piratas roban nuestros datos médicos y los ponen a la venta en la dark internet, porque saben que hay muchos interesados. Son bases de datos muy apetecibles para cualquier empresa o compañía de seguros. Una aseguradora podría negar la cobertura de salud a alguien que sabe que tiene una determinada enfermedad de antemano, gracias a los datos que ha comprado en el mercado negro. Una empresa podría no contratar a un candidato determinado si tiene esta o aquella dolencia. Incluso cualquier país podría diseñar un ataque adecuado a las particularidades de su rival, si conoce los datos de salud de sus ciudadanos.

¿Están a salvo nuestros datos? Tanto la Ley de Autonomía del Paciente como la Ley General de Salud Pública recogen el derecho a la intimidad personal y al deber de los sanitarios de mantener secreto sobre los datos de los pacientes. ¿Y quién puede tener acceso a nuestra historia clínica? Según el artículo 9 del Reglamento General de Protección de Datos (RGPD), el tratamiento de nuestros datos personales está prohibido, a no ser en unos supuestos en concreto: que demos consentimiento explícito para ello, que sea necesario para proteger nuestros intereses vitales, que se solicite judicialmente o que sea del interés público general (fines científicos, preventivos, históricos o estadísticos).

El profesional sanitario puede acceder a las historias para tratar al paciente, pero también con fines docentes, siempre que se garantice el anonimato y exista consentimiento expreso. En el caso de que la persona tenga trascendencia pública y sea identificable, deberán extremarse los cuidados. Todos somos humanos y estamos sujetos a la tentación de la curiosidad, pero, en este caso en concreto, violar la privacidad de los pacientes está tipificado en el código penal como delito de descubrimiento y revelación de secretos (artículo 197).

Puede suceder que el personal sanitario entre en las historias con intenciones más aviesas que el simple cotilleo. En 2017, un médico accedió a la historia clínica del amante de la mujer. Alegó que su propósito había sido el de verificar (o descartar) la existencia de enfermedades de transmisión sexual con el fin de protegerse él mismo ante posibles contagios. Fue condenado a cárcel e inhabilitación y una fuerte multa por el daño moral causado.

Hace tres años, el Tribunal Supremo condenó a una enfermera por acceder al historial de una antigua amiga desde el centro de salud donde trabajaba. La perjudicada denunció que había sido amenazada por la acusada con desvelar sus datos médicos y esta fue condenada a dos años de prisión y a seis de inhabilitación absoluta para desempeñar su profesión.

Tomar precauciones

Como pacientes tenemos derecho a una copia de nuestros informes médicos (artículo 18 de la Ley 41/2002). El hospital tiene la obligación de proporcionárnoslos en el caso de que queramos para solicitar una segunda opinión en otro centro. En el caso de fallecimiento, solo tendrán acceso las personas que estén directamente vinculadas, salvo que lo hayamos prohibido expresamente en vida.

¿Qué pasa si vemos difundidos nuestros datos? Debemos acudir a la Agencia Española de Protección de Datos o a la Justicia (AEPD). Existe el canal prioritario en la AEPD para solicitar la retirada urgente de material “sensible”. El organismo iniciará la apertura de un procedimiento sancionador y estudiar si se ha violado el RGPD.

Vivimos en la era digital con todos los peligros que conlleva. No queda otra que adaptarse y tener precaución, pero no miedo.

Vivimos en la era digital con todos los peligros que conlleva. No queda otra que adaptarse y tener precaución, pero no miedo. Cuando se empezó a utilizar el tranvía en Santander, a principios del siglo XIX, una persona fue contratada para ir delante de la máquina tocando el cornetín y enarbolando una bandera. Su función consistía en alertar a los viandantes, que no estaban acostumbrados aún a aquel novedoso ingenio. Como siempre iba delante del tranvía, el imaginario popular empezó a llamarle “el cagueta”, ya que parecía que corría para salvarse del atropello.

Con la era digital pasa lo mismo: internet es un novedoso ingenio que puede arrollarnos al menor despiste. Adaptémonos a las nuevas circunstancias, y sigamos las instrucciones para que no suceda. La tecnología debe ser una herramienta y no un tormento. Hace veinte años, los historiales médicos eran carpetas repletas de folios que acababan perdiéndose con el tiempo y el uso. Cuanto más grande era el dosier, más hojas se traspapelaban con la manipulación. Gracias a la historia digital ya no se pierden los datos como antes, y ya no es necesario ir al archivo a buscar carpetas. Ahora está íntegra y disponible al instante.

Constituye una de las mayores mejoras de nuestra sanidad en los últimos años, pero necesita protección.

Fuente

Link de la informacion