CUANDO EL HISTORIAL DEL PACIENTE VALE MÁS QUE EL DINERO

Consolidado como uno de los objetivos prioritarios de los ciber-delincuentes a escala global, no siendo España una excepción, el sector sanitario está viendo cómo la combinación de infraestructuras tecnológicas heterogéneas, equipos de TI con recursos limitados y la gestión de información altamente sensible convierte a hospitales y centros de salud en un blanco especialmente atractivo.

Álvaro Fernández
Director de Ventas en Sophos Iberia

Los datos clínicos -historiales médicos, diagnósticos, tratamientos, información genética...- tienen un valor extraordinario en el mercado negro y, a diferencia de las credenciales o tarjetas financieras, no pueden cancelarse ni reemplazarse. Su exposición o pérdida compromete la privacidad de los pacientes, y puede tener consecuencias directas sobre la continuidad asistencial y la seguridad sanitaria y la calidad del cuidado.

Ransomware en sanidad, más allá del cifrado

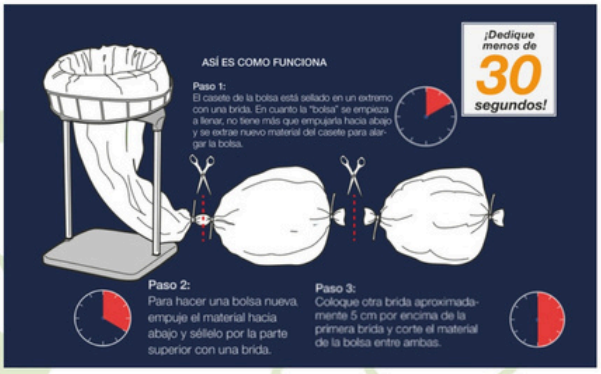
Durante años, la amenaza era el cifrado masivo de datos: los atacantes bloqueaban los sistemas hospitalarios y exigían un pago para restaurarlos. Pero el panorama está cambiando, y no precisamente a mejor. Según el informe "*State of Ransomware in Healthcare 2025*" elaborado por Sophos a partir de las experiencias reales de 292 proveedores sanitarios de todo el mundo, el cifrado de datos ha caído a su nivel más bajo en cinco años: sólo un tercio de los ataques (34%) derivaron en cifrado en 2025, frente al 74% registrado en 2024.

Sin embargo, los atacantes se han adaptado rápidamente: los casos de extorsión sin cifrado (en los que ciberdelincuentes roban los datos y exigen un rescate bajo amenaza de publicarlos) se han triplicado en tres años y ya suponen el 12% de los incidentes en 2025.

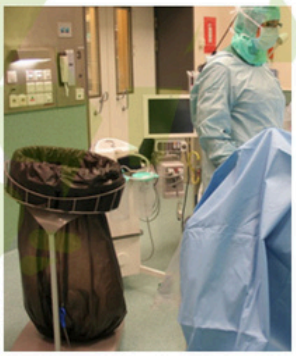
LEANpio

llevamos la **mejora continua** por dentro

En LEANpio, entendemos que la gestión de residuos en el sector sanitario es clave para garantizar la seguridad, la higiene y la protección medioambiental. Por eso, ofrecemos soluciones avanzadas que reducen riesgos, optimizan procesos y mejoran el entorno de trabajo.



Nuestra tecnología de bolsa continua Longopac permite una gestión con contacto 0, eliminando la manipulación directa y reduciendo significativamente la contaminación cruzada. Además, asegura una bolsa siempre disponible, lo que agiliza los cambios y mejora la eficiencia en el día a día en entornos como hospitales, farmacias o laboratorios.



Esta eficiencia también se traduce en sostenibilidad: su diseño optimizado reduce el consumo de material y permite disminuir hasta un 80% las emisiones de CO_2 frente a sistemas tradicionales, gracias al uso de materiales reciclados y al máximo aprovechamiento de cada bolsa.

Pactosafe®: máxima seguridad en residuos peligrosos

Su sistema de sellado 100% hermético elimina la exposición a residuos tóxicos y olores, garantizando un entorno de trabajo más seguro. Además, su accionamiento mediante pedal evita el contacto manual, reforzando el concepto de contacto 0.

Está diseñado para la manipulación segura de residuos como citostáticos, antibióticos o antivirales, y funciona como un sistema cerrado (CSDD), esencial para cumplir con los protocolos actuales del sector sanitario.

Fabricado en acero inoxidable y pensado para una limpieza rápida y eficaz, también destaca por su menor impacto ambiental, con un 40% menos de consumo de material. Todo ello cumpliendo con las normativas nacionales e internacionales en la gestión de residuos.

www.LEANpio.com +34 976 753 000 leanpio@leanpio.com

La razón es clara: los historiales médicos tienen un valor intrínseco en el mercado negro que va mucho más allá del coste operativo de bloquear un sistema. La amenaza de exponer información clínica sensible -diagnósticos sobre enfermedades crónicas, tratamientos psiquiátricos, datos de menores...- ejerce una presión que muchas organizaciones no están preparadas para resistir.

En este contexto, durante los últimos doce meses el equipo *Sophos X-Ops* ha identificado 88 grupos de ciber-amenazas distintos atacando a organizaciones sanitarias en todo el mundo. Entre los más activos destacan *GOLD FEATHER* (*Qilin*), *GOLD IONIC* (*INC Ransom*) y *GOLD HUBBARD (RansomHub*), grupos sofisticados que han convertido la sanidad en un nicho estratégico de sus operaciones.

Las grietas por las que entra el adversario

¿Por qué sigue siendo tan sencillo comprometer la seguridad de un centro sanitario? Los datos de Sophos son reveladores. La causa técnica más repetida en los ataques sufridos en 2025 fueron las vulnerabilidades sin parchear, las cuales estaban presentes en el 33% de los incidentes.

> Los factores organizativos resultan igualmente determinantes: el 42% de las víctimas apuntaron a la falta de personal especializado en el momento del ataque como elemento contribuyente clave, y el 41% reconocieron la existencia de lagunas de seguridad conocidas que no habían sido corregidas.

A esto se suma una realidad que el "*Active Adversary Report 2026*" de Sophos pone sobre la mesa:

> el 67% de los incidentes analizados tuvieron su origen en ataques relacionados con la identidad (credenciales comprometidas, ausencia de autenticación multifactor, sistemas de identidad débiles...).

En el 59% de los casos, el MFA simplemente no estaba configurado. Y, una vez dentro de la red, los atacantes tardan una media de apenas 3 ó 4 horas en llegar al servidor de *Active Directory* de la organización, reduciendo enormemente el margen de reacción.

Proteger lo que no puede detenerse

Un hospital no es una empresa convencional. Sus sistemas no pueden apagarse para realizar un mantenimiento de seguridad. Sus redes incluyen dispositivos médicos *legacy* -escáneres TAC, máquinas de radiología, equipos de UCI...- que no admiten agentes de protección tradicionales. Y su personal, aunque altamente cualificado en su campo, no puede convertirse de un día para otro en un equipo de ciberseguridad de guardia.

Para resolver esa situación de falta de personal especializada en ciberseguridad y de problemas técnicos, como redes sin segmentar o ausencia de sistemas de detección de intrusiones, el Consorcio Hospitalario Provincial de Castellón optó por un enfoque integral basado en la plataforma de Sophos, incluyendo detección y respuesta gestionadas (*Sophos MDR*), gestión de vulnerabilidades (*Sophos Managed Risk*), *firewall* de próxima generación (*Sophos XGS*) y detección de intrusiones en red (*Sophos NDR*) para monitorizar incluso los equipos médicos que no soportan agentes.

La implementación completa se realizó en tres meses sin interrumpir la actividad asistencial, y con resultados relevantes: en los tres primeros meses de operación, el sistema detectó cerca de un millón potenciales de amenazas. De ellas, 50.000 fueron escaladas y correlacionadas por los algoritmos de inteligencia artificial. En una ocasión, el equipo MDR de Sophos intervino activamente para detener un intento de ejecución de código malicioso, sin que el personal del hospital tuviera que hacer nada, ofreciendo así protección sin detener la operativa.

> Los ciber-ataques a la sanidad no son únicamente un problema tecnológico, sino un problema de salud pública

Cuando un hospital pierde el acceso a sus sistemas, los pacientes son derivados a otros centros, se retrasan diagnósticos y, en los casos más graves, se compromete la continuidad asistencial. Y el coste medio de recuperación de un ataque de *ransomware* en el sector sanitario -aunque ha caído un 60% en el último año hasta los 1,02 millones de dólares- sigue siendo una cifra que ningún centro puede absorber fácilmente. Proteger los datos clínicos es, en última instancia, proteger a los pacientes, al personal sanitario y a toda la sociedad.

Litek

EXPERTOS EN TERAPIAS AVANZADAS Y FARMACIA HOSPITALARIA

Producción de terapias avanzadas y medicamentos estériles

Soluciones personalizadas para la producción de terapias avanzadas. Preparación de medicamentos estériles en farmacia hospitalaria, garantizando máxima seguridad, calidad y control en cada proceso.

Compounding seguro

Soluciones de compounding diseñadas para garantizar la máxima seguridad para el paciente y la protección del operario, manteniendo los más altos estándares de calidad y control.

LITEK PHARMA

• Barrio Usilla 28. 48490 Ugao-Miraballes. Bizkaia. España •
+34 946 959 930 • info@litek-pharma.com