HORNETSECURITY BY proofpoint.

FACTSHEET

CIBERSEGURIDAD EN EL SECTOR SANITARIO

La disrupción digital en la sanidad puede afectar a la investigación, la atención médica, la confianza y la seguridad

Hoy en día, en el entorno sanitario digital, todo —desde el diagnóstico y el tratamiento hasta los historiales de pacientes y la facturación— depende de sistemas de ITseguros y fiables. Una sola brecha puede tener consecuencias de gran alcance: no solo comprometer datos sensibles de pacientes, sino también interrumpir operaciones clínicas, retrasar tratamientos y, en los casos más graves, poner vidas en peligro.
A diferencia de otros sectores, en sanidad el tiempo de inactividad no solo implica pérdidas económicas o de productividad: puede afectar directamente a la salud de los pacientes. Por eso, la ciberseguridad es un componente crítico de la calidad asistencial.

¿Por qué la sanidad es un objetivo prioritario?

» **Datos de alto valor:** Las organizaciones sanitarias gestionan información personal muy valiosa, ideal para el robo de identidad, el fraude y la extorsión.

» **Urgencia en la atención:** La presión del tiempo aumenta la probabilidad de pagar rescates para restaurar la operativa rápidamente.

» **El factor humano:** Personal muy ocupado y una colaboración compleja incrementan la exposición al phishing, la ingeniería social y las filtraciones accidentales.

» **Infraestructuras obsoletas:** Sistemas heredados y entornos difíciles de parchear crean brechas de seguridad explotables

DATOS DE PACIENTES Y OPERATIVOS

- Historias clínicas y datos médicos
- Diagnósticos, resultados de laboratorio e imágenes
- nformación de seguros, facturación y pagos
- Credenciales del personal, correos electrónicos y documentos internos

Confianza, credibilidad, reputación y confianza de los stakeholders

DATOS DE INVESTIGACIÓN

- Datos y protocolos de ensayos clínicos
- Conjuntos de datos de participantes
- Información genómica y biomarcadores
- Resultados de estudios y documentos de colaboración

Integridad de la investigación y marca empleadora

03/26

HORNETSECURITY
BY proofpoint.

7,42 M$

Coste medio de una brecha de datos en sanidad (el sector más costoso por 14º año consecutivo).

279 DÍAS

Tiempo medio para identificar y contener una brecha (el más largo de todos los sectores, más de 5 semanas por encima de la media).

18 %

De los ataques de ransomware en sanidad se debieron a credenciales comprometidas.

22 %

De los ataques en sanidad se originaron a través de correos electrónicos maliciosos.

¿QUÉ OCURRE CUANDO LOS DATOS SON ROBADOS?

1. ENGAÑO
correo de phishing | login falso | "solicitud urgente"

2. ACCESO
por ejemplo, mediante

3. PROPAGACIÓN
enlaces compartidos
movimiento lateral

4. LOCALIZACIÓN DE DATOS
historias clínicas
archivos de investigación

5. EXFILTRACIÓN
copia silenciosa de los datos

6. PRESIÓN
filtraciones en la dark web, chantaje, rescates y extorsión repetida

RESERVA TU DEMO

HORNETSECURITY
BY proofpoint.

10 BUENAS PRÁCTICAS PARA PREVENIR BRECHAS DE DATOS

Evaluar y mejorar

1. Realiza evaluaciones de riesgo periódicas de sistemas, dispositivos y flujos de trabajo.
2. Prueba los controles (simula ataques y valida planes de detección y respuesta).

Reducir el riesgo humano

3. Forma al personal de manera continua (phishing, ingeniería social, etc.).
4. Fomenta una cultura de seguridad (canales claros de reporte).

Proteger accesos y sistemas

5. **Implementa controles de acceso sólidos basados en el principio de mínimo privilegio.**
6. **Utiliza autenticación multifactor (MFA) siempre que sea posible.**
7. **Mantén actualizados y parcheados los sistemas de ITI y los dispositivos médicos.**

Proteger y recuperar

8. Cifra los datos sensibles.
9. Realiza copias de seguridad de sistemas y datos críticos siguiendo una regla resiliente como 3-2-1-1.
10. Desarrolla un plan de respuesta a incidentes con roles, contactos y prioridades de recuperación bien definidos.

CÓMO HORNETSECURITY AYUDA AL SECTOR SANITARIO

Una suite de seguridad cloud integral para Microsoft 365 que cubre seguridad, cumplimiento, concienciación y backup. Ayuda a las organizaciones sanitarias a prevenir incidentes y a recuperarse más rápido. Incluye, entre otros, los siguientes servicios:

SECURITY AWARENESS	Refuerza el "firewall humano" con formación específica y simulaciones realistas de phishing, reduciendo de forma medible la susceptibilidad a ataques.
ADVANCED THREAT PROTECTION	Protección frente a ataques avanzados como spear phishing, ransomware y exploits zero-day mediante tecnologías de detección avanzadas.
SPAM & MALWARE PROTECTION	Bloquea correos maliciosos antes de que lleguen a la bandeja de entrada del personal, protegiendo la comunicación clínica.
365 TOTAL BACKUP	Recuperación rápida de datos de Microsoft 365 para garantizar la continuidad asistencial y el cumplimiento normativo, al tiempo que se reduce el impacto del ransomware y el borrado accidental.
PERMISSION MANAGEMENT	Aplica el principio de mínimo privilegio en Microsoft 365 y detecta comparticiones de riesgo y configuraciones incorrectas.

hornetsecurity.com | info@hornetsecurity.com | +49 511 515 464-0