HORNETSECURITY

INFOSHEET
AI POWERED

SECURITY AWARENESS SERVICE

PARA ORGANIZACIONES SANITARIAS

Las ciberamenazas en el sector sanitario no dejan de crecer. Entre errores humanos, vulnerabilidades digitales y cadenas de suministro cada vez más complejas, los datos sensibles están más expuestos que nunca. La clave está en combinar una estrategia de ciberseguridad integral con una formación adaptada en concienciación, para que cada persona del equipo se convierta en una parte activa de la defensa.

¿QUÉ AMENAZAS ESTÁN AFECTANDO AL SECTOR SANITARIO?

Los hospitales y centros de salud son, cada vez más, objetivo de ataques sofisticados, y la tendencia no hace más que aumentar. Estas son algunas señales de alerta:

- Aumento de ciberincidentes: En 2023, los ataques en el ámbito sanitario casi se cuadruplicaron, con más de 133 millones de registros expuestos en 725 brechas de seguridad.
- Ransomware que paraliza hospitales: Casos como el de Change Healthcare muestran hasta qué punto un ataque puede bloquear urgencias, retrasar operaciones y poner en riesgo la seguridad de los pacientes.
- Más tecnología, más puntos débiles: La implantación de historias clínicas electrónicas, consultas online o diagnósticos con IA es positiva... pero también abre muchas puertas a los ciberdelincuentes si no se protege bien.
- Riesgos en la cadena de suministro y presión regulatoria: El sector depende de sistemas interconectados y, además, tiene que cumplir con normativas cada vez más exigentes en materia de ciberseguridad.

Todo esto no solo afecta a la atención al paciente, sino que también pone en juego la reputación y la estabilidad financiera de cualquier organización sanitaria.

PASA A LA ACCIÓN

No dejes que un descuido ponga en riesgo la salud de tus pacientes o los servicios que prestas.Forma a tu equipo y refuerza tus defensas desde dentro.

¡SOLICITA TU DEMO!

SECURITY
AWARENESS SERVICE

RESPUESTA DE LA UE: MEDIDAS PROACTIVAS PARA REFORZAR LA CIBERSEGURIDAD

Ante el aumento de amenazas digitales, la Comisión Europea ha lanzado un plan de acción para mejorar la ciberseguridad en sanidad. Las claves de su propuesta son:

- Prevención con apoyo económico: Se ofrecerán bonos de ciberseguridad y asesoramiento personalizado para ayudar a los hospitales a reforzar sus defensas.
- Detección y respuesta rápida: Se propone un sistema de alerta temprana a nivel europeo y la creación de un Centro de Apoyo especializado en ciberseguridad sanitaria.
- Colaboración internacional: Se utilizarán herramientas como la "caja de herramientas" de Ciberdiplomacia para frenar ataques maliciosos desde fuera de la UE.

POR QUÉ LA CONCIENCIACIÓN EN SEGURIDAD ES CLAVE

El 95% de los incidentes de ciberseguridad tienen su origen en errores humanos. Tus empleados son la primera línea de defensa. Por eso, una buena formación en concienciación en seguridad puede aportar:

- Formación práctica y útil: Que cada persona del equipo sepa cómo detectar correos maliciosos, evitar trampas de phishing o actuar ante un ataque de ransomware.
- Cumplir con la normativa europea: La formación ayuda a que tu organización esté alineada con los requisitos de ciberseguridad de la UE.
- Evitar interrupciones críticas: Reducir riesgos evita retrasos en servicios esenciales como quirófanos, urgencias o diagnósticos.
- Proteger los datos de los pacientes: Cuidar la información médica no es solo cuestión legal, es una cuestión de confianza.

SECURITY AWARENESS SERVICE: TU ALIADO EN CIBERDEFENSA PARA EL SECTOR SALUD

Hornetsecurity contamos con Security Awareness Service, una herramienta de última generación pensada para proteger a empresas de todo tipo, especialmente en sectores tan sensibles como el sanitario. Así es te ayudamos a marcar la diferencia:

- Formación a medida: Ofrecemos módulos personalizados que abordan los retos específicos de la ciberseguridad en sanidad, para que tu equipo esté realmente preparado frente a amenazas reales.
- Contenido completo y actualizado: Desde cómo navegar por internet con seguridad hasta el correcto manejo de datos personales de salud, cubrimos todos los temas clave que necesitas.
- Fácil de poner en marcha: Nuestra solución se integra sin problemas con tus sistemas actuales, sin complicaciones ni interrupciones innecesarias, y mejora la capacidad de respuesta de tu empresa.
- Soporte continuo: Con actualizaciones constantes y seguimiento personalizado, estarás siempre un paso por delante de las ciberamenazas que no paran de evolucionar.