Ciberseguridad para dispositivos médicos

¿Qué es la ciberseguridad de los dispositivos médicos?

La ciberseguridad de los dispositivos médicos es vital para proteger los datos y las vidas de los pacientes, así como para proteger a las instituciones médicas de los ataques de ransomware. Con la evolución de los dispositivos médicos y su conectividad, las ciberamenazas han seguido evolucionando a la par, creando nuevos riesgos.

¿Por qué es tan importante la ciberseguridad de los dispositivos médicos?

Los riesgos de la ciberseguridad de los dispositivos médicos son muchos y variados, lo que subraya la necesidad de contar con certificaciones y normas actualizadas, así como de someterse a evaluaciones de ciberseguridad. Una gestión eficaz de los riesgos implica **mejorar los procesos del ciclo de vida** y realizar **rigurosas pruebas de penetración** para identificar vulnerabilidades y reforzar la seguridad.

Riesgos y requisitos de ciberseguridad para los dispositivos médicos

Los riesgos de ciberseguridad para los dispositivos médicos son:

- **Requisitos reglamentarios:**
  Los dispositivos médicos están sujetos a **estrictas normativas** de organismos como la **FDA** en Estados Unidos, la **EMA** en Europa, la **NAPA** en China y otras agencias reguladoras regionales. Estas normativas exigen el cumplimiento de normas y

directrices específicas de ciberseguridad para garantizar que los dispositivos estén a salvo de la piratería informática y otras ciberamenazas. El incumplimiento puede dar lugar a **sanciones graves**, **retiradas del mercado** o **prohibiciones**.

- **Seguridad del paciente:**
  Los fallos de ciberseguridad en los dispositivos médicos pueden **poner en peligro directamente la seguridad del paciente.** Si se vulnera un dispositivo como un marcapasos o una bomba de insulina, estos podrían funcionar mal, suministrando dosis de tratamiento incorrectas o fallando en momentos críticos.

- **Privacidad e interrupciones:**
  Dado que los dispositivos médicos a menudo almacenan y transmiten información sanitaria delicada, una violación de la seguridad puede **exponer los historiales médicos personales**, provocando el robo de la identidad y **la pérdida de la confidencialidad del paciente.** Este es un riesgo típico en los ataques de ransomware, en los que **actores maliciosos cifran datos críticos** y exigen un rescate para desbloquearlos. Estos ataques no sólo comprometen la privacidad de los pacientes, sino que también **interrumpen las operaciones esenciales de los sistemas sanitarios**, lo que subraya la necesidad crítica de medidas sólidas de ciberseguridad.

Normas y directrices de ciberseguridad para dispositivos médicos

Dados los riesgos que entraña, la ciberseguridad de los dispositivos médicos se somete a pruebas según **estrictas normas internacionales y nacionales.** Los organismos reguladores de todo el mundo han publicado directrices relativas a la regulación de la ciberseguridad de los dispositivos médicos y describen los ensayos a los que deben someterse para llegar a los mercados. En Applus+ Laboratories podemos ayudarte con las siguientes normas:

- **MDCG 2019-16 Orientaciones de la UE sobre ciberseguridad de los dispositivos médicos**
  Garantizar la integridad y confidencialidad de los datos de los dispositivos médicos en todo el mercado europeo.

- **EE.UU./Directrices de la FDA sobre ciberseguridad en dispositivos médicos - Consideraciones sobre el sistema de calidad y contenido de las presentaciones previas a la comercialización**
  Directrices para incorporar medidas de ciberseguridad desde el diseño hasta la implantación en el marco normativo estadounidense.

- **Norma IEC TR 60601-4-5 sobre ciberseguridad de los dispositivos médicos**
  Una hoja de ruta técnica para implantar normas mundiales de ciberseguridad en dispositivos médicos.

- **Norma IEC 81001-5-1 para las actividades de seguridad del software sanitario y los sistemas informáticos sanitarios en el ciclo de vida del producto:**
  Estrategias para mantener la ciberseguridad a lo largo de la vida operativa del dispositivo, aplicables en todo el mundo.

¿Por qué elegir Applus+ Laboratories para la ciberseguridad de los dispositivos médicos?

Applus+ Laboratories ofrece **servicios integrales de ensayos de ciberseguridad** para evaluar dispositivos médicos. Además, tenemos muchos años de experiencia haciendo **evaluaciones de ciberseguridad** y realizando **ensayos de penetración** en todo tipo de Objetivos de Evaluación (TOEs).

Ensayos de seguridad

Applus+ Laboratories ofrece amplios servicios de ensayos de penetración para evaluar la resistencia de los sistemas frente a ataques y accesos no autorizados. Mediante la realización de simulaciones de ciberataques, evaluamos las vulnerabilidades de los dispositivos médicos en varios componentes:

En Hardware

Ataques de última generación y herramientas hechas ha medida por los expertos del laboratorio:

- Fault Injection
- Side Channel
- Reverse Engineering
- Design Review
- Logical Attacks
- IC/SoC Attacks

- PCB HW Hacking
- Biometric Attacks

En Software y Firmware

Robusto conocimeinto y experiencia en sistemas embebidos, arranque seguro, TEE y white box crypto:

- Binary Reverse Engineering
- Static Attacks
- Source Code Audits
- Debugging
- Fuzzing
- Dynamic Tamper / Hooking
- SW Timing Analysis and CCA
- Symbolic Execution

En Protocolos de Comunicación

Para IP stack protocols, sistemas industriales y protocolos privados:

- Ataques en todas las capas (OSI Model) incluyendo hardware hecho a medida para estimular las capas inferiores (wired and wireless protocols)
- Fuzzing
- Dynamic Tamper / Hooking

Nuestra experiencia en ciberseguridad mejora aún más las medidas de seguridad que recomendamos. Las actividades de ensayos de penetración realizadas en nuestro

laboratorio de expertos no sólo ayudan a reforzar la ciber resiliencia de los productos. El informe generado por los expertos de Applus+ Laboratories puede utilizarse como **prueba del cumplimiento** de los requisitos de ciberseguridad exigidos por los organismos reguladores de todo el mundo, como la FDA en EE.UU.

Verificación de conformidad

Nuestros equipos también pueden dar soporte a los fabricantes de todo el mundo para verificar si su producto cumple con los estándares o pautas específicas solicitadas por los organismos reguladores. De igual modo, nuestro certificado de conformidad facilita la preparación del producto para el proceso de aprobación en diversos mercados.

Ponte en contacto con Applus+ Laboratories para ensayar y **certificar la ciberseguridad de tus dispositivos médicos** y conseguir que tu producto llegue al mercado lo antes posible.