VULNERABILIDADES DE SOFTWARE/HARDWARE

Co-funded by the European Union

ESCAPE. Preparando a los profesionales sanitarios para los ciberataques.
Proyecto n.º 2023-1-ES01-KA220-VET-000151536

Socios

ESCAPE. Preparación de profesionales sanitarios ante ciberataques. Proyecto n.° 2023-1-ES01-KA220-VET-000151536

Co-funded by the European Union

Este proyecto ha sido cofinanciado con el apoyo de la Comisión Europea. Esta publicación [comunicación] refleja únicamente la opinión del autor, y la Comisión no se responsabiliza del uso que pueda hacerse de la información que contiene.

Tabla de contenido

FACTSHEET – VULNERABILIDADES DE SOFTWARE/HARDWARE

1. Definición

Consiste en debilidades o fallas en sistemas de software o hardware que pueden ser explotadas por actores de amenazas para obtener acceso no autorizado, interrumpir servicios o comprometer datos. Algunos ejemplos incluyen errores de software sin parches, configuraciones incorrectas, sistemas operativos obsoletos o dispositivos médicos inseguros.

2. Importancia general

Hoy en día, las vulnerabilidades de software y hardware son una preocupación central. Con la aparición de los sistemas digitales, casi todos los sectores dependen de software y hardware interconectados.

El abuso de estas vulnerabilidades podría provocar ciberataques importantes, como ataques de ransomware, robo de identidad o el cierre de servicios críticos.[2] Por lo tanto, abordar estas vulnerabilidades es crucial para la ciberseguridad global, la estabilidad económica y la protección de la información personal de los ciudadanos.

Las debilidades no se refieren a dificultades técnicas aisladas, sino a riesgos globales que afectan a múltiples sectores a nivel mundial. Por lo tanto, gestionar las debilidades mediante la aplicación sistemática de parches, la supervisión y la divulgación coordinada es esencial para lograr una sociedad más resiliente a la ciberseguridad en todos los niveles.

3. Importancia en el ámbito de la salud e impacto en la calidad de los cuidados

La atención médica es particularmente vulnerable a este tipo de amenaza cibernética debido a su dependencia de dispositivos médicos, registros médicos electrónicos e infraestructura crítica que con frecuencia operan en sistemas obsoletos y difíciles de actualizar.

Las vulnerabilidades de software/hardware son una causa subyacente importante de incidentes de seguridad, y el 80 % de las organizaciones sanitarias las citan como la fuente de más del 61 % de sus incidentes de seguridad. Estas vulnerabilidades son una fuente constante de preocupación, especialmente en sistemas obsoletos e infraestructuras de TI complejas.

El impacto de las vulnerabilidades de software y hardware en la calidad de la atención es amplio. Comprometen la seguridad del paciente al interrumpir los servicios, lo que obliga a cancelar citas o reprogramar cirugías. Además, si los atacantes atacan dispositivos médicos como bombas de infusión, ventiladores o dispositivos de diagnóstico por imagen, pueden perjudicar directamente a los pacientes.

4. ¿Qué puedo hacer como profesional sanitario?

Tenga una buena higiene cibernética e instale actualizaciones en los dispositivos y software que utiliza en su trabajo diario.

Esté alerta a las amenazas cibernéticas (correos electrónicos de phishing, enlaces sospechosos) e informe inmediatamente cualquier irregularidad.

- Siga el protocolo de su hospital y asegúrese de respetar las pautas de seguridad.

- Participe en la capacitación sobre ciberseguridad y manténgase al día sobre cómo responder ante incidentes y el impacto de la protección de datos de los pacientes.

5. Más información

5.1 Materiales de aprendizaje

- Sequential videos for general topics about cybersecurity (JGT-2)
- Web seminars about key aspects of cibersecurity (JGT-3)
- Cibersecurity guide for healthcare sector (EU scope) (JGT-7)
- Cibersecurity training from National Cryptographic Centre of Spain. Requires National login (JGT-8)
- An article on security strategies applicable to electronic patient records (IST-37)
- An overview of cybersecurity in healthcare, focusing on the role of AI and its regulatory framework. (IST-39)
- A compendium on the processing of patient data on online platforms. (IST-40)
- Research paper on Cybersecurity and critical care staff: A mixed methods study (PRAMMER-29)
- An integrated cybernetic awareness strategy to assess cybersecurity attitudes and behaviours in school context (PRAMMER-31)
- Gamification and Serious Games for Cybersecurity Awareness and First Responders Training: An overview (PRAMMER-33)
- A Serious Game for Healthcare Industry: Information Security Awareness Training Program for Hospital Universiti Kebangsaan Malaysia (PRAMMER-34)

5.2 Vídeos relevantes

Este vídeo analiza problemas comunes de software y hardware que pueden surgir con los dispositivos médicos y proporciona consejos prácticos sobre cómo hacerlos más seguros y proteger la seguridad del paciente.

Cybersecurity in Healthcare | Importance of Cybersecurity in Healthcare
https://youtu.be/aZLGYxupCrQ?si=MZNID_ADom2kh8aO

El siguiente video proporciona una descripción general de las vulnerabilidades comunes de software y hardware en los dispositivos médicos, así como estrategias prácticas para mejorar la ciberseguridad y garantizar la seguridad del paciente.

Medical Device Cybersecurity | Tarlogic Security
https://youtu.be/JdOvvCP7uyE?si=KRQXpNjpoSzm0oye

5. 3 Enlaces relevantes

This article revealed 993 flaws in medical devices and products, 160 of which could be used as weapons and 101 of which were becoming more common in the wild. It emphasizes the need for proactive cybersecurity measures in healthcare settings.

https://industrialcyber.co/medical/healthcare-research-report-reveals-exploitable-vulnerabilities-that-allow-hackers-to-breach-devices-systems/

This article discusses common security flaws in medical devices, such as data that isn't encrypted and APIs that aren't secure, and offers manufacturers advice on how to make their products safer.

https://www.vumetric.com/blog/medical-device-vulnerabilities-top-8-cybersecurity-vulnerabilities/

6. Bibliografía

Souppaya, M., & Scarfone, K. (2022). Guide to enterprise patch management planning:

https://doi.org/10.6028/nist.sp.800-40r4

ENISA threat landscape: Health Sector - CYBIL portal. (2023, 5 julio). Cybil Portal.

https://cybilportal.org/publications/enisa-threat-landscape-health-sector/

ESCAPE. Preparación de profesionales sanitarios ante ciberataques. Proyecto n.° 2023-1-ES01-KA220-VET-000151536

Co-funded by the European Union

Este proyecto ha sido cofinanciado con el apoyo de la Comisión Europea. Esta publicación [comunicación] refleja únicamente la opinión del autor, y la Comisión no se responsabiliza del uso que pueda hacerse de la información que contiene.