VULNERABILITÀ SOFTWARE/ HARDWARE

Co-funded by the European Union

ESCAPE. *Preparing healthcare professionals for cyberattacks*
Project No.2023-1-ES01-KA220-VET-000151536

Partner

INSTITUTO DE EDUCACION SECUNDARIA
JAVIERGARCIATELLEZ

ISTITUTO DEI SORDI
DI TORINO

Firda

PRAXXER

eolas

BBS Weser

ESCAPE. Preparing healthcare professionals for cyberattacks
Project No.2023-1-ES01-KA220-VET-000151536

Co-funded by
the European Union

Questo progetto è stato co-finanziato con il supporto della Commissione Europea. Questa pubblicazione [comunicazione] riflette solo le opinioni dell'autore, e la Commissione non può essere ritenuta responsabile per l'uso che possa essere fatto delle informazioni ivi contenute.

Indice

Co-funded by the European Union

FACTSHEET - VULNERABILITÀ SOFTWARE/HARDWARE

1. Definizione

Si tratta di debolezze o difetti nei sistemi software o hardware che possono essere sfruttati dagli autori delle minacce per ottenere accessi non autorizzati, interrompere i servizi o compromettere i dati. Tra gli esempi figurano bug software non corretti, configurazioni errate, sistemi operativi obsoleti o dispositivi medici non sicuri.

2. Rilevanza generale

Al giorno d'oggi, le vulnerabilità software/hardware sono una preoccupazione centrale. Con l'avvento dei sistemi digitali, quasi ogni settore dipende da software e hardware interconnessi.

L'abuso di queste vulnerabilità potrebbe portare a eventi informatici significativi come attacchi ransomware, furto di identità o chiusura di servizi critici. Pertanto, affrontare queste vulnerabilità è fondamentale per la sicurezza informatica globale, la stabilità economica e la protezione delle informazioni personali dei cittadini.

I punti deboli non si riferiscono a difficoltà tecniche isolate, ma piuttosto a rischi globali che interessano molteplici settori in tutto il mondo. Pertanto, la gestione delle debolezze attraverso interventi sistematici di correzione, monitoraggio e divulgazione coordinata è essenziale per rendere la società più resiliente a livello informatico a tutti i livelli.

3. Importanza nella salute e nell'assistenza e impatto sulla qualità dell'assistenza

Il settore sanitario è particolarmente vulnerabile a questo tipo di minaccia informatica a causa della sua dipendenza da dispositivi medici, cartelle cliniche elettroniche e infrastrutture critiche che spesso operano su sistemi obsoleti e difficili da aggiornare.

Le vulnerabilità software/hardware sono una causa significativa di incidenti di sicurezza: l'80% delle organizzazioni sanitarie le cita come causa di oltre il 61% dei propri incidenti di sicurezza. Queste vulnerabilità sono fonte di costante preoccupazione, in particolare per i sistemi obsoleti e le infrastrutture IT complesse.

L'impatto delle vulnerabilità software/hardware sulla qualità dell'assistenza è ampio. Compromettono la sicurezza dei pazienti interrompendo i servizi, costringendo ad annullare gli appuntamenti o a riprogrammare gli interventi chirurgici. Inoltre, se gli aggressori prendono di mira dispositivi medici come pompe per infusione, ventilatori o dispositivi di imaging, possono danneggiare direttamente i pazienti.

4. Cosa posso fare come professionista sanitario?

- a posso fare come professionista sanitario?
- Mantieni una buona igiene informatica e installa gli aggiornamenti sui dispositivi e sui software che utilizzi quotidianamente nel tuo lavoro.
- Prestare attenzione alle minacce informatiche (e-mail di phishing, link sospetti) e segnalare immediatamente eventuali irregolarità.
- Segui il protocollo ospedaliero e assicurati di rispettare le linee guida sulla sicurezza.
- Partecipa alla formazione sulla sicurezza informatica e resta aggiornato su come rispondere agli incidenti e sull'impatto della protezione dei dati dei pazienti.

5. Ulteriori informazioni

5.1 Materiali didattici

- 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 Video correlati

In questo video vengono illustrati i problemi software e hardware più comuni che possono verificarsi con i dispositivi medici e vengono forniti consigli pratici su come renderli più sicuri e tutelare la sicurezza dei pazienti.

Sicurezza informatica in ambito sanitario | Importanza della sicurezza informatica in ambito sanitario
https://youtu.be/aZLGYxupCrQ?si=MZNID_ADom2kh8aO

Il seguente video fornisce una panoramica delle vulnerabilità software e hardware più comuni nei dispositivi medici, nonché strategie pratiche per migliorare la sicurezza informatica e garantire la sicurezza dei pazienti.

Sicurezza informatica dei dispositivi medici | Tarlogic Security
https://youtu.be/JdOvvCP7uyE?si=KRQXpNjpoSzm0oye

5.3 Link rilevanti

Questo articolo ha rivelato 993 falle nei dispositivi e nei prodotti medici, 160 delle quali potrebbero essere utilizzate come armi e 101 delle quali stanno diventando sempre più comuni. Sottolinea la necessità di misure proattive di sicurezza informatica in ambito sanitario.
https://industrialcyber.co/medical/healthcare-research-report-reveals-exploitable-vulnerabilities-that-allow-hackers-to-breach-devices-systems/

Questo articolo ha rivelato 993 falle nei dispositivi e nei prodotti medici, 160 delle quali potrebbero essere utilizzate come armi e 101 delle quali stanno diventando sempre più comuni. Sottolinea la necessità di misure proattive di sicurezza informatica in ambito sanitario.
https://www.vumetric.com/blog/medical-device-vulnerabilities-top-8-cybersecurity-vulnerabilities

6. Bibliografia

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. Preparing healthcare professionals for cyberattacks
Project No.2023-1-ES01-KA220-VET-000151536

Co-funded by
the European Union

Questo progetto è stato co-finanziato con il supporto della Commissione Europea. Questa pubblicazione [comunicazione] riflette solo le opinioni dell'autore, e la Commissione non può essere ritenuta responsabile per l'uso che possa essere fatto delle informazioni ivi contenute.