DISPOSITIVI MEDICI

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 - DISPOSITIVI MEDICI

1. Definizione

I dispositivi medici sono dispositivi connessi a Internet o gestiti da software utilizzati in ambito sanitario, che spaziano dagli strumenti diagnostici alle apparecchiature di supporto vitale (ad esempio, ventilatori polmonari e pacemaker). Rappresentano un vettore di attacco significativo a causa delle potenziali vulnerabilità.

2. Rilevanza generale

I dispositivi medici sono identificati come un'area di vulnerabilità chiave e oggetto di attenzione specifica da parte di nuove normative come il Cyber Resilience Act, a causa del loro impatto diretto sull'assistenza ai pazienti. Forniscono diagnosi accurate, trattamenti efficaci e un monitoraggio continuo dei pazienti. Inoltre, indirettamente, contribuiscono a prolungare l'aspettativa di vita e a migliorare l'assistenza sanitaria.

Allo stesso tempo, però, i dispositivi medici sono vulnerabili agli attacchi informatici, che possono avere gravi conseguenze, mettendo a repentaglio la vita delle persone. Per questo motivo, sono necessarie una regolamentazione e una vigilanza globali per prevenire inefficienze.

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

In ambito sanitario, i dispositivi medici influenzano direttamente la sicurezza e le prestazioni dei pazienti. Le tecnologie di supporto vitale sono essenziali in terapia intensiva e i monitor indossabili aiutano i pazienti cronici a gestire i propri problemi di salute da casa.

Guasti o vulnerabilità di questo tipo di dispositivi presentano rischi che vanno dal ritardo nel trattamento a incidenti potenzialmente letali. Garantire che queste tecnologie vengano utilizzate in modo sicuro, efficace e protetto crea fiducia, riduce i danni prevenibili e migliora notevolmente la qualità della vita.

4. Cosa posso fare come professionista sanitario?

- Seguire le istruzioni e i protocolli dei fornitori quando si utilizzano i dispositivi.
- Segnala qualsiasi problema o attività sospetta relativa ai dispositivi.
- Seguire le corrette norme di igiene informatica, utilizzare password complesse e abilitare l'autenticazione a due fattori.
- Promuovere la consapevolezza tra i pazienti sull'uso sicuro dei loro dispositivi medici a casa.

5. Ulteriori informazioni

5.1 Materiali didattici

- Sequential videos for general topics about cybersecurity (JGT-2)
- 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)
- Regulation of cybersecurity in healthcare (BBS-23)
- Cyber-attacks are a permanent and substantial threat to health systems: Education must reflect that (PRAMMER-32)

5.2 Video correlati

Per proteggere i pazienti dalle minacce online, il video sottolinea quanto sia fondamentale adottare solide pratiche di sicurezza informatica, come aggiornamenti software tempestivi e password univoche per i dispositivi medici connessi.

Cybersecurity Awareness for Connected Medical Devices
https://youtu.be/TU1w6fQ-yf8?si=ZhG1zl9sialnzdk6

Questo video analizza le ultime linee guida e gli aggiornamenti normativi della FDA, evidenziando potenziali minacce e vulnerabilità che potrebbero compromettere non solo la sicurezza e l'efficacia dei dispositivi medici.

Why Cybersecurity is Critical for Medical Devices
https://youtu.be/YBuJjr7TtnQ?si=ROPBfouPAzLMvM2w

5.3 Link rilevanti

I ricercatori hanno scoperto falle di sicurezza nelle pompe per insulina MiniMed di Medtronic che consentivano di controllarle a distanza, interrompendo l'erogazione di insulina o somministrando dosi eccessive letali. La copertura mediatica del problema ha portato al ritiro volontario e alla sostituzione del dispositivo da parte di Medtronic, a seguito di ritardi prolungati nel mitigare il rischio.
https://www.wired.com/story/medtronic-insulin-pump-hack-app/

La FDA ha rilevato difetti nei monitor per pazienti Contec CMS8000 ed Epsimed MN-120. Ha affermato che questi difetti potrebbero essere utilizzati per bloccare da remoto i monitor, hackerare reti o divulgare informazioni private sui pazienti. Finora non si sono verificati incidenti o decessi, ma alle strutture sanitarie viene chiesto di adottare misure per ridurre questi rischi.
https://www.reuters.com/business/healthcare-pharmaceuticals/us-fda-identifies-cybersecurity-risks-certain-patient-monitors-2025-01-30/

L'importante azienda tedesca di apparecchiature mediche Fresenius, il più grande operatore ospedaliero privato d'Europa, è stata colpita dal ransomware "Snake". Gli aggressori hanno sottratto dati sensibili dei pazienti dai centri di dialisi in Serbia prima di crittografarli, aumentando i rischi per la sicurezza informatica legati ai dispositivi medici.
https://medical-technology.h5mag.com/medical_technology_jun23/case_studies_cybersecurity_medical_device_industry

6. Bibliografia

Liveri, D., Drougkas, A., & Zisi, A. (2021). Cloud Security for Healthcare Services. ENISA.
https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20Cloud%20Security%20for%20Healthcare%20Services.pdf

Young, M. (2025, 22 enero). European Commission Publishes Action Plan on Cybersecurity of Hospitals and Healthcare Providers | Covington Digital Health. Covington Digital Health.
https://www.covingtondigitalhealth.com/2025/01/european-commission-publishes-action-plan-on-cybersecurity-of-hospitals-and-healthcare-providers/

Overview. (2025, 26 agosto). Public Health.
https://health.ec.europa.eu/medical-devices-sector/overview_en

World Health Organization: WHO. (2020, 2 julio). Medical devices.
https://www.who.int/health-topics/medical-devices

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.