MEDIZINPRODUKTE

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

PRAMMER

eolas

BBS Weser

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

Co-funded by
the European Union

Dieses Projekt wurde mit Unterstützung der Europäischen Kommission kofinanziert. Die Verantwortung für den Inhalt dieser Veröffentlichung [Mitteilung] trägt allein der Verfasser; die Kommission haftet nicht für die weitere Verwendung der darin enthaltenen Informationen.

Inhaltsverzeichnis

Co-funded by the European Union

FACTSHEET – MEDIZINPRODUKTE

1. Definition

Medizinische Geräte sind internetfähige oder softwaregesteuerte Geräte im Gesundheitswesen, von Diagnoseinstrumenten bis hin zu lebenserhaltenden Geräten (z. B. Beatmungsgeräte, Herzschrittmacher). Aufgrund potenzieller Schwachstellen stellen sie einen erheblichen Angriffsvektor dar.1.

2. Allgemeine Bedeutung

Medizinische Geräte werden alsSchlüsselbereich der Verwundbarkeit und besonderer Schwerpunkt neuer Vorschriften wie des Cyber Resilience Act aufgrund ihrer direkten Auswirkungen auf die Patientenversorgung2Sie ermöglichen präzise Diagnosen, wirksame Behandlungen und eine kontinuierliche Patientenüberwachung. Darüber hinaus tragen sie indirekt zu einer längeren Lebenserwartung und einer verbesserten Gesundheitsversorgung bei.3.

Gleichzeitig sind medizinische Geräte jedoch anfällig für Cyberangriffe, die schwerwiegende Folgen haben und das Leben der Betroffenen bedrohen können. Aus diesem Grund sind globale Regulierung und Wachsamkeit notwendig, um Ineffizienzen zu vermeiden.

3. Bedeutung für Gesundheit und Pflege und Auswirkungen auf die Pflegequalität

Im Gesundheitswesen beeinflussen medizinische Geräte die Sicherheit und Leistungsfähigkeit der Patienten direkt. Lebenserhaltende Technologien sind in der Intensivpflege unverzichtbar, und tragbare Monitore helfen chronischen Patienten, ihre medizinischen Probleme von zu Hause aus zu bewältigen.4.

Ausfälle oder Schwachstellen bei solchen Geräten bergen Risiken, die von einer verzögerten Behandlung bis hin zu lebensbedrohlichen Vorfällen reichen. Die Gewährleistung eines sicheren, effektiven und zuverlässigen Einsatzes dieser Technologien schafft Vertrauen, verringert vermeidbare Schäden und verbessert die Lebensqualität erheblich.

4. Was kann ich als medizinisches Fachpersonal tun?

- Befolgen Sie beim Bedienen der Geräte die Anweisungen und Protokolle des Anbieters.
- Melden Sie alle Probleme oder verdächtigen Aktivitäten im Zusammenhang mit Geräten.
- Achten Sie auf die richtige Cyber-Hygiene, verwenden Sie sichere Passwörter und aktivieren Sie die Zwei-Faktor-Authentifizierung.
- Sensibilisieren Sie die Patienten für die sichere Verwendung ihrer medizinischen Geräte zu Hause.

5. Weitere Informationen

5.1 Lernmaterialien

- Aufeinanderfolgende Videos zu allgemeinen Themen der Cybersicherheit (JGT-2)
- Ein Artikel über Sicherheitsstrategien für elektronische Patientenakten (IST-37)
- Ein Überblick über Cybersicherheit im Gesundheitswesen mit Schwerpunkt auf der Rolle von KI und ihrem regulatorischen Rahmen. (IST-39)
- Ein Kompendium zur Verarbeitung von Patientendaten auf Online-Plattformen. (IST-40)
- Regulierung der Cybersicherheit im Gesundheitswesen (BBS-23)
- Cyberangriffe stellen eine permanente und erhebliche Bedrohung für Gesundheitssysteme dar: Die Ausbildung muss dies widerspiegeln (PRAMMER-32).
- Videotraining für Fachleute und Studierende (FIRDA-14)

5.2 Relevante Videos

Um Patienten vor Online-Bedrohungen zu schützen, wird in dem Video betont, wie wichtig es ist, für vernetzte medizinische Geräte strenge Cybersicherheitsmaßnahmen wie zeitnahe Software-Updates und eindeutige Passwörter einzuhalten.

Cybersicherheitsbewusstsein für vernetzte medizinische Geräte
https://youtu.be/TU1w6fQ-yf8?si=ZhG1zl9sialnzdk6

Dieses Video befasst sich mit den neuesten Richtlinien und regulatorischen Aktualisierungen der FDA und hebt potenzielle Bedrohungen und Schwachstellen hervor, die mehr als nur die Sicherheit und Wirksamkeit medizinischer Geräte gefährden könnten.

Warum Cybersicherheit für medizinische Geräte so wichtig ist
https://youtu.be/YBuJjr7TtnQ?si=ROPBfouPAzLMvM2w

5. 3 Relevante Links

Forscher entdeckten Sicherheitslücken in den MiniMed-Insulinpumpen von Medtronic, die eine Fernsteuerung ermöglichten. So ließen sich die Insulinabgabe unterbrechen oder tödliche Überdosen verabreichen. Die Medienberichterstattung über das Problem führte zu einem freiwilligen Rückruf und Austausch des Geräts durch Medtronic, nachdem es lange Zeit bei der Risikominderung gedauert hatte.
https://www.wired.com/story/medtronic-insulin-pump-hack-app/

Die FDA fand Mängel an den Patientenmonitoren Contec CMS8000 und Epsimed MN-120. Sie gab an, dass diese Mängel ausgenutzt werden könnten, um die Monitore per Fernzugriff außer Funktion zu setzen, sich in Netzwerke einzuhacken oder private Patientendaten preiszugeben. Bisher gab es keine Vorfälle oder Todesfälle, aber Gesundheitseinrichtungen wurden aufgefordert, Maßnahmen zu ergreifen, um diese Risiken zu verringern.
https://www.reuters.com/business/healthcare-pharmaceuticals/us-fda-identifies-cybersecurity-risks-certain-patient-monitors-2025-01-30/

Der führende deutsche Medizintechnikkonzern Fresenius – Europas größter privater Krankenhausbetreiber – wurde von der Ransomware „Snake“ getroffen. Angreifer erbeuteten sensible Patientendaten aus Dialysezentren in Serbien, bevor sie diese verschlüsselten, und erhöhten damit die Cybersicherheitsrisiken für medizinische Geräte.
https://medicaltechnology.h5mag.com/medical_technology_jun23/case_studies_cybersecurity_medical_device_industry

6. Literaturverzeichnis

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

Young, M. (2025, 22. Januar).Europäische Kommission veröffentlicht Aktionsplan zur Cybersicherheit von Krankenhäusern und Gesundheitsdienstleistern | Covington Digital HealthCovington Digital Health.
https://www.covingtondigitalhealth.com/2025/01/european-commission-publishes-action-plan-on-cybersecurity-of-hospitals-and-healthcare-providers/

Überblick. (2025, 26. August). Öffentliche Gesundheit.
https://health.ec.europa.eu/medical-devices-sector/overview_en

Weltgesundheitsorganisation: WHO. (2020, 2. Juli).Medizinische Geräte.
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

Dieses Projekt wurde mit Unterstützung der Europäischen Kommission kofinanziert. Die Verantwortung für den Inhalt dieser Veröffentlichung [Mitteilung] trägt allein der Verfasser; die Kommission haftet nicht für die weitere Verwendung der darin enthaltenen Informationen.