SOFTWARE-/HARDWARE-SCHWACHSTELLEN

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 – SOFTWARE-/HARDWARE-SCHWACHSTELLEN

1. Definition

Es handelt sich um Schwächen oder Fehler in Software- oder Hardwaresystemen, die von Bedrohungsakteuren ausgenutzt werden können, um unbefugten Zugriff zu erlangen, Dienste zu stören oder Daten zu kompromittieren.1Beispiele hierfür sind ungepatchte Softwarefehler, Fehlkonfigurationen, veraltete Betriebssysteme oder unsichere medizinische Geräte.

2. Allgemeine Bedeutung

Heutzutage stellen Software-/Hardware-Schwachstellen ein zentrales Problem dar. Mit der Entstehung digitaler Systeme ist fast jeder Sektor auf die Vernetzung von Software und Hardware angewiesen.

Der Missbrauch dieser Schwachstellen könnte zu schwerwiegenden Cyber-Ereignissen wie Ransomware-Angriffen, Identitätsdiebstahl oder der Schließung kritischer Dienste führen.2Daher ist die Beseitigung dieser Schwachstellen von entscheidender Bedeutung für die globale Cybersicherheit, die wirtschaftliche Stabilität und den Schutz der persönlichen Daten der Bürger.

Schwachstellen beziehen sich nicht auf isolierte technische Schwierigkeiten, sondern auf globale Risiken, die mehrere Sektoren weltweit betreffen. Daher ist die Behebung von Schwachstellen durch systematisches Patchen, Monitoring und koordinierte Offenlegung unerlässlich, um die Gesellschaft auf allen Ebenen widerstandsfähiger gegen Cyberangriffe zu machen.2.

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

Das Gesundheitswesen ist für diese Art von Cyberbedrohungen besonders anfällig, da es von medizinischen Geräten, elektronischen Patientenakten und kritischer Infrastruktur abhängig ist, die häufig auf veralteten Systemen laufen, die nur schwer zu aktualisieren sind.

Software-/Hardware-Schwachstellen sind eine wesentliche Ursache für Sicherheitsvorfälle. 80 % der Gesundheitsorganisationen geben sie als Ursache für mehr als 61 % ihrer Sicherheitsvorfälle an. Diese Schwachstellen geben ständig Anlass zur Sorge, insbesondere bei veralteten Systemen und komplexen IT-Infrastrukturen.1.

Die Auswirkungen von Software-/Hardware-Schwachstellen auf die Qualität der medizinischen Versorgung sind weitreichend. Sie gefährden die Patientensicherheit durch Störungen im Versorgungsablauf, die zur Absage von Terminen oder zur Verschiebung von Operationen führen. Darüber hinaus können Angreifer, die medizinische Geräte wie Infusionspumpen, Beatmungsgeräte oder bildgebende Geräte ins Visier nehmen, Patienten direkt schädigen.

4. Was kann ich als medizinisches Fachpersonal tun?

- Achten Sie auf eine gute Cyberhygiene und installieren Sie Updates auf den Geräten und der Software, die Sie bei Ihrer täglichen Arbeit verwenden.
- Achten Sie auf Cyberbedrohungen (Phishing-E-Mails, verdächtige Links) und melden Sie Unregelmäßigkeiten sofort.
- Befolgen Sie das Krankenhausprotokoll und achten Sie darauf, die Sicherheitsrichtlinien einzuhalten.
- Nehmen Sie an Schulungen zur Cybersicherheit teil und bleiben Sie auf dem Laufenden, wie Sie auf Vorfälle reagieren und welche Auswirkungen der Schutz von Patientendaten hat.

5. Weitere Informationen

5.1 Lernmaterialien

- Aufeinanderfolgende Videos zu allgemeinen Themen der Cybersicherheit (JGT-2)
- Webseminare zu wichtigen Aspekten der Cybersicherheit (JGT-3)
- Leitfaden zur Cybersicherheit im Gesundheitswesen (EU-Geltungsbereich) (JGT-7)
- Schulung zur Cybersicherheit durch das Nationale Kryptographiezentrum Spaniens. Nationaler Login erforderlich (JGT-8).
- 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)
- Forschungsarbeit zum Thema Cybersicherheit und Intensivpflegepersonal: Eine Mixed-Methods-Studie (PRAMMER-29)
- Eine integrierte Strategie zur Sensibilisierung für Cybersicherheit zur Beurteilung von Einstellungen und Verhaltensweisen im Bereich Cybersicherheit im schulischen Kontext (PRAMMER-31)
- Gamifizierung und Serious Games zur Sensibilisierung für Cybersicherheit und zur Ausbildung von Ersthelfern: Ein Überblick (PRAMMER-33)
- Ein Serious Game für die Gesundheitsbranche: Informationssicherheits-Sensibilisierungstraining für das Krankenhaus Universiti Kebangsaan Malaysia (PRAMMER-34)
- Videotraining für Fachleute und Studierende (FIRDA-13)
- Videotraining für Fachleute und Studierende (FIRDA-14)
- Digitales Training in Cybersicherheit, unterhaltsame und schnelle Fragen (FIRDA-15)
- Kostenlose Kurse zur Verbesserung der digitalen Kompetenzen von Mitarbeitern im Gesundheitswesen (FIRDA-18)

5.2 Relevante Videos

In diesem Video werden häufige Software- und Hardwareprobleme erörtert, die bei medizinischen Geräten auftreten können, und es werden praktische Ratschläge gegeben, wie diese sicherer gemacht und die Patientensicherheit gewährleistet werden kann.

Cybersicherheit im Gesundheitswesen | Bedeutung der Cybersicherheit im Gesundheitswesen
https://youtu.be/aZLGYxupCrQ?si=MZNID_ADom2kh8aO

Das folgende Video bietet einen Überblick über häufige Software- und Hardware-Schwachstellen in medizinischen Geräten sowie praktische Strategien zur Verbesserung der Cybersicherheit und Gewährleistung der Patientensicherheit.

Cybersicherheit für medizinische Geräte | Tarlogic Security
https://youtu.be/JdOvvCP7uyE?si=KRQXpNjpoSzm0oye

5. 3 Relevante Links

Dieser Artikel deckte 993 Schwachstellen in medizinischen Geräten und Produkten auf, von denen 160 als Waffen eingesetzt werden könnten und 101 in der Praxis immer häufiger auftreten. Er unterstreicht die Notwendigkeit proaktiver Cybersicherheitsmaßnahmen im Gesundheitswesen.
https://industrialcyber.co/medical/healthcare-research-report-reveals-exploitable-vulnerabilities-that-allow-hackers-to-breach-devices-systems/

In diesem Artikel werden häufige Sicherheitsmängel bei medizinischen Geräten erörtert, beispielsweise nicht verschlüsselte Daten und unsichere APIs, und Hersteller erhalten Ratschläge, wie sie ihre Produkte sicherer machen können.
https://www.vumetric.com/blog/medical-device-vulnerabilities-top-8-cybersecurity-vulnerabilities/

6. Literaturverzeichnis

Souppaya, M., & Scarfone, K. (2022).Leitfaden zur Planung des Patch-Managements in Unternehmen:
https://doi.org/10.6028/nist.sp.800-40r4

ENISA-Bedrohungslandschaft: Gesundheitssektor - CYBIL-Portal. (2023, 5. Juli). 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

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.