FEHLER, FEHLKONFIGURATIONEN UND SCHLECHTE SICHERHEITSPRAKTIKEN

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 – FEHLER, FEHLKONFIGURATIONEN UND SCHLECHTE SICHERHEITSPRAKTIKEN

1. Definition

Es handelt sich um interne Schwachstellen und unbeabsichtigte menschliche Fehler, wie Fehlkonfigurationen oder unzureichende Sicherheitspraktiken, die zu Sicherheitsvorfällen, einschließlich Datenlecks, führen können.1Einige Beispiele sind schwache Passwörter, übermäßige Benutzerrechte, das Versäumnis, Patches anzuwenden oder die Verschlüsselung zu vernachlässigen.

2. Allgemeine Bedeutung

Diese Probleme sind relevant, weil sie es Kriminellen ermöglichen, Systeme mühelos zu kompromittieren. Die meisten Datenlecks werden durch menschliches Versagen oder schlechte Konfiguration verursacht, was deutlich machtdie Bedeutung robuster interner Cybersicherheitspraktiken und menschlicher Faktoren für die allgemeine Sicherheitslage.

Laut IBM2Menschliche Fehler sind für mehr als 20 % aller Sicherheitsverletzungen verantwortlich und kosten Unternehmen Millionen. Auch Fehlkonfigurationen können zu langfristigen Sicherheitsrisiken führen. Beispielsweise kann ein nicht korrekt eingerichteter Server sensible Daten monatelang offenlegen, ohne dass es jemand bemerkt. Daher sind die Behebung von Fehlern und die Einhaltung sicherer Verfahren entscheidende Aspekte der Cybersicherheit für Unternehmen.

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

Fehler und Fehlkonfigurationen im Gesundheitswesen wirken sich direkt auf die Sicherheit, Privatsphäre und Qualität der Patientenversorgung aus. Bei medizinischen Geräten kann es zu falschen Medikamentendosierungen, verzögerten Alarmen oder Fehlfunktionen der Überwachungsdienste kommen.

Darüber hinaus könnten vertrauliche Informationen aus Patientenakten öffentlich gemacht werden, was einen Verstoß gegen die DSGVO- und HIPAA-Vorschriften darstellen und das Vertrauen der Öffentlichkeit in medizinisches Fachpersonal untergraben würde.

Letztendlich kann mangelnde Cyberhygiene, wie veraltete Software oder falsche Benutzerberechtigungen, Angreifern ermöglichen, in Netzwerke einzudringen, den Krankenhausbetrieb zu stören, Abläufe zu verzögern und die Qualität der Versorgung zu beeinträchtigen. Der SingHealth-Datenleck in Singapur (2018) betraf Fehlkonfigurationen der Netzwerkzugriffskontrollen, wodurch die persönlichen Gesundheitsdaten von 1,5 Millionen Patienten kompromittiert wurden.3.

4. Was kann ich als medizinisches Fachpersonal tun?

- Befolgen Sie die Sicherheitsrichtlinien und -protokolle der Organisation.
- Nutzen Sie den sicheren Zugriff, indem Sie sich über autorisierte Krankenhaus-Cloud-Plattformen mit starken Passwörtern und Zwei-Faktor-Authentifizierung anmelden.
- Melden Sie ungewöhnliches Systemverhalten oder mögliche Fehlkonfigurationen sofort dem IT-Team.
- 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, um menschliche Fehler zu reduzieren.

5. Weitere Informationen

5.1 Lernmaterialien

- Cybersicherheit für Ihre Branche (JGT-1)
- Aufeinanderfolgende Videos zu allgemeinen Themen der Cybersicherheit (JGT-2)
- Webseminare zu wichtigen Aspekten der Cybersicherheit (JGT-3)
- Sensibilisierungspaket zur Cybersicherheit in Unternehmen (JGT-4)
- Cybersicherheit für KMU und Selbstständige (JGT-6)
- Leitfaden zur Cybersicherheit im Gesundheitswesen (EU-Geltungsbereich) (JGT-7)
- Schulung zur Cybersicherheit durch das Nationale Kryptographiezentrum Spaniens. Nationaler Login erforderlich (JGT-8).
- Ein Artikel, der den aktuellen Stand der Cybersicherheit im Gesundheitswesen untersucht. (IST-36)
- Bildungsprojekt zur sicheren und verantwortungsvollen digitalen Nutzung. (IST-41)
- IT-Sicherheitsanforderungen und Schutzmaßnahmen – Tipps und praktische Beispiele (BBS-42)
- Forschungsarbeit zum Thema Cybersicherheit und Intensivpflegepersonal: Eine Mixed-Methods-Studie (PRAMMER-29)
- Eine kritische Überprüfung von Rahmenwerken und Schulungsmodellen zur Sensibilisierung für Cybersicherheit (PRAMMER-30)
- Eine integrierte Strategie zur Sensibilisierung für Cybersicherheit zur Beurteilung von Einstellungen und Verhaltensweisen im Bereich Cybersicherheit im schulischen Kontext (PRAMMER-31)
- Cyberangriffe stellen eine permanente und erhebliche Bedrohung für Gesundheitssysteme dar: Die Ausbildung muss dies widerspiegeln (PRAMMER-32).
- 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)
- Systematische Anwendung von Gamification in Schulungen zur Sensibilisierung für Cybersicherheit: Ein Rahmenkonzept und eine Fallstudienanalyse (PRAMMER-35)
- 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)
- Online-Lektion zum Thema Cybersicherheit (FIRDA-20)

5.2 Relevante Videos

Das Webinar erörtert, wie medizinische Fehler in der Intensivpflege oft vorhersehbar und vermeidbar sind, und betont die Bedeutung von Bewusstsein, Systemverbesserungen und Patientensicherheitspraktiken zur Schadensminderung.

[Webinar] Medizinische Fehler, Schäden und Patientensicherheit
https://youtu.be/VB7MsPH_sG8?si=rNpZrED9yTYm7oyu

5. 3 Relevante Links

In diesem Artikel wird erläutert, wie ein Konfigurationsfehler im irischen COVID-19-Impfportal (das auf Salesforce basiert) registrierten Benutzern Zugriff auf interne HSE-Dokumente und sensible personenbezogene Daten von über einer Million Menschen verschaffte.
https://www.darkreading.com/cyberattacks-data-breaches/nhs-breach-hse-bug-expose-healthcare-data-british-isles

Durch Fehlkonfigurationen wurden Tausende von DICOM-Bildgebungsservern öffentlich zugänglich, wodurch Patientennamen, Geburtsdaten, Krankheitsinformationen und medizinische Bilder offengelegt wurden und Systeme in mehreren Ländern betroffen waren.
https://www.sharitsec.eu.org/2023/09/critical-dicom-server-misconfigurations.html

Viele medizinische Geräte verfügen über fest codierte Anmeldeinformationen oder nicht über die richtige Authentifizierung, was sie zu einem leichten Ziel für Angriffe wie Denial-of-Service oder Manipulation macht.
https://www.csoonline.com/article/568861/insecure-configurations-expose-ge-healthcare-devices-to-attacks.html

6. Literaturverzeichnis

ENISA-Bedrohungslandschaft: Gesundheitssektor - CYBIL-Portal. (2023, 5. Juli). Cybil Portal.
https://cybilportal.org/publications/enisa-threat-landscape-health-sector/

Kosten einer Datenpanne 2025 | IBM. (s. f.).
https://www.ibm.com/reports/data-breach

Wikipedia-Mitwirkende. (7. August 2025).2018 SingHealth-DatenverletzungWikipedia.
https://en.wikipedia.org/wiki/2018_SingHealth_data_breach

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.