CLOUD-SICHERHEIT

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 – CLOUD-SICHERHEIT

1. Definition

Es bezieht sich auf eine Reihe von Richtlinien, Kontrollen, Verfahren und Technologien, deren Zweck es ist, Cloud-basierte Systeme, Daten und Infrastruktur zu schützen1. Es behandelt Themen wie Datenschutz, Identitäts- und Zugriffsverwaltung, Compliance und Widerstandsfähigkeit gegen Cyberangriffe durch die „Cloudifizierung“ von Patientendaten im Gesundheitswesen.

2. Allgemeine Bedeutung

Die Cloud-Sicherheit wird zu einem immer größeren Problembereich, da das Gesundheitswesen zunehmend Cloud-Dienste zur Datenspeicherung und -verarbeitung nutzt, die spezifische Richtlinien und Sicherheitspraktiken erfordern.1Ohne starken Cloud-Schutz können Cyberbedrohungen, Sicherheitsverletzungen oder Fehlkonfigurationen sensible Informationen offenlegen. Da Sicherheitslücken häufig vorkommen, können sie Millionen von Benutzern gleichzeitig betreffen. Dies kann nicht nur finanzielle Schäden und Reputationsschäden verursachen, sondern auch die Einhaltung gesetzlicher Rahmenbedingungen (DSGVO in Europa oder HIPAA in den USA) beeinträchtigen.

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

Der Bedarf an Technologie im klinischen Umfeld ist in letzter Zeit gestiegen; Cloud Computing, Telemedizin, künstliche Intelligenz und elektronische Gesundheit können oft bessere Dienste bieten2.Darüber hinaus ermöglicht die Nutzung von Cloud-Technologie in elektronischen Patientenakten den Patienten einen mühelosen und umfassenden Zugriff auf ihre Gesundheitsinformationen. Der Einsatz von Cloud-Technologie verändert die Art und Weise, wie Ärzte, Pflegepersonal, Kliniken und Krankenhäuser Patienten qualitativ hochwertige und wirtschaftlich erfolgreiche Dienstleistungen bieten.3.

Cloud Computing bietet mehrere Vorteile, darunter eine einfache und bequeme Zusammenarbeit zwischen Benutzern, geringere Kosten, höhere Geschwindigkeit, Skalierbarkeit und Flexibilität.3Doch trotz der zahlreichen Vorteile gibt es auch einige negative Aspekte und Herausforderungen. Cloud Computing birgt auch erhöhte Risiken. Ein Sicherheitsverstoß oder Ausfallzeiten in einem Cloud-basierten System können dazu führen, dass hochsensible Informationen offengelegt, Behandlungen verzögert oder sogar Notdienste unterbrochen werden.4.

4. Was kann ich als medizinisches Fachpersonal tun?

- Nutzen Sie den sicheren Zugriff, indem Sie sich über autorisierte Krankenhaus-Cloud-Plattformen mit starken Passwörtern und Zwei-Faktor-Authentifizierung anmelden.
- Vermeiden Sie die Weitergabe von Dateien mit persönlichen Informationen außerhalb des offiziellen Cloud-Systems.
- Achten Sie auf Cyber-Bedrohungen (Phishing-E-Mails, verdächtige Links) und melden Sie Unregelmäßigkeiten sofort
- 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

- Cybersicherheit für KMU und Selbstständige (JGT-6)
- Allgemeine Schulung (71 Infopakete) zu Cybersicherheitsbeschreibungen. Angeboten vom Nationalen Kryptographiezentrum. (JGT-10)
- Eine Infografik über Sicherheits- und Cybersicherheitsgeräte, die in verschiedenen Gesundheitseinrichtungen eingesetzt werden. (IST-38)
- Ein Überblick über Cybersicherheit im Gesundheitswesen mit Schwerpunkt auf der Rolle von KI und ihrem regulatorischen Rahmen. (IST-39)
- 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)
- Videotraining für Fachleute und Studierende (FIRDA-13)

5.2 Relevante Videos

In diesem Video geht es um das Modell der geteilten Verantwortung für Cloud-Umgebungen. Es erklärt, dass Unternehmen für die Sicherheit ihrer Anwendungen, Workloads und Daten verantwortlich sind, während der Cloud-Anbieter für die Sicherheit der unterstützenden Infrastruktur verantwortlich ist.

Was ist Cloud-Sicherheit?
https://youtu.be/jI8IKpjiCSM?si=vXJzAbIsRoj2ltDh

Das nächste Video zeigt, wie Cloud Computing im Gesundheitswesen eingesetzt wird, indem die Vorteile, wie besserer Zugriff und Skalierbarkeit, gegen die Nachteile, wie Datenschutzrisiken und mögliche Systemabhängigkeiten, abgewogen werden.

Cloud Computing im Gesundheitswesen: Die Vor- und Nachteile
https://youtu.be/xEl_6NZuyS4?si=cFApA9QgHFCEBzPi

5. 3 Relevante Links

Dieser Artikel beschreibt, wie durch eine Fehlkonfiguration im Salesforce-basierten Impfportal des Health Service Executive die persönlichen Daten und Impfdaten von über einer Million irischer Bürger sowie interne HSE-Dokumente offengelegt wurden.
https://appomni.com/blog/saas-risks-in-healthcare-data-exposure-in-hse/

Diesem Artikel zufolge wurden in einer öffentlich zugänglichen Cloud-Datenbank aufgrund fehlenden Passwortschutzes fast 957.000 gesundheitsbezogene Datensätze offengelegt, darunter auch vertrauliche Personal- und Einstellungsinformationen.
https://www.cybersecurity-insiders.com/cloud-security-breach-leads-to-a-leak-of-957000-patient-records/

Ein finnisches Psychotherapieunternehmen erlitt einen massiven Datendiebstahl, durch den private Therapieunterlagen öffentlich wurden. Der Datendiebstahl, der zur Erpressung der Klinik und ihrer Patienten führte, kostete die Klinik nach DSGVO 608.000 Euro aufgrund mangelnder Sicherheit und nicht rechtzeitiger Meldung des Datendiebstahls. Die Folgen hatten erhebliche Auswirkungen auf das Vertrauen und die psychische Gesundheit der Patienten.
https://www.wired.com/story/finland-mental-health-data-breach-vastaamo/

6. Literaturverzeichnis

Liveri, D., Athanasios, D., & Zisi, A. (2021). ENISA Cloud-Sicherheit für das Gesundheitswesen.Enisa.
https://doi.org/10.2824/454966

Tahir, A., Chen, F., Khan, H. U., Ming, Z., Ahmad, A., Nazir, S., & Shafiq, M. (2020). Eine systematische Überprüfung der Cloud-Speichermechanismen in Bezug auf E-Healthcare-Systeme.Sensoren,20(18), 5392.
https://doi.org/10.3390/s20185392

Mehrtak, M., SeyedAlinaghi, S., MohsseniPour, M., Noori, T., Karimi, A., Shamsabadi, A., Heydari, M., Barzegary, A., Mirzapour, P., Soleymanzadeh, M., Vahedi, F., Mehraeen, E., & Dadras, O. (2021). Sicherheitsherausforderungen und -lösungen beim Einsatz von Cloud Computing im Gesundheitswesen.Zeitschrift für Medizin und Leben,14(4), 448-461.
https://doi.org/10.25122/jml-2021-0100

Leitfaden zu HIPAA und Cloud Computing. (2022, Dezember). US-Gesundheitsministerium. Abgerufen am 28. August 2025 von https://www.hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/cloud-computing/index.html

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.