DATENSCHUTZ VERLETZUNG

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.

CC BY NC

Inhaltsverzeichnis

Co-funded by the European Union

FACTSHEET – DATENSCHUTZVERLETZUNG

1. Definition

Es bezieht sich auf ein absichtliches oder unabsichtliches Ereignis, das zum unbefugten Zugriff, zur unbefugten Offenlegung oder Manipulation sensibler, vertraulicher oder geschützter Daten, einschließlich Patientendaten und elektronischer Gesundheitsakten, führt.1. Verstöße können durch Hacking, Phishing, Fehlkonfiguration, Insiderfehler oder physischen Diebstahl entstehen.

2. Allgemeine Bedeutung

In den letzten Jahren hat die Zahl der Datenschutzverletzungen zugenommen, sowohl in ihrer Häufigkeit als auch in ihrem Schweregrad. Etwa 46 % dieser Vorfälle zielen direkt auf sensible Patientendaten und geistiges Eigentum ab, oft im Zusammenhang mit Ransomware-Angriffen.2.

Datenschutzverletzungen verursachen erhebliche Kosten und können den Ruf schädigen, da persönliche, finanzielle oder vertrauliche Daten offengelegt werden. Bei einem Angriff müssen Unternehmen ihre Systeme anhalten, um den Vorfall zu untersuchen. Dies führt zu Verzögerungen, Stornierungen und Umsatzeinbußen.

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

Cyberkriminelle sind besonders an Datenschutzverletzungen im Gesundheitswesen interessiert. Dies liegt an der enormen Menge an privaten und finanziellen Daten, die von Menschen gesammelt werden und sowohl Krankenhäusern als auch Patienten erheblichen Schaden zufügen. Die gestohlenen Informationen können für Identitätsdiebstahl nützlich sein und schwerwiegende Auswirkungen auf die Gesundheit und Behandlung von Patienten haben.3:

- Risiken für die Patientensicherheit entstehen, wenn Angreifer Patienteninformationen wie Rezepte und Krankengeschichten verändern, was zu einer falschen Medikamentenverabreichung oder Verzögerungen bei der Behandlung schwerer Krankheiten führen kann.
- Laut IBM belaufen sich die Kosten von Datendiebstählen im Gesundheitswesen auf 10,98 Millionen US-Dollar. Darin enthalten sind die Kosten für Medikamente, die Benachrichtigung betroffener Patienten und die Bildung eines Teams zur Aufklärung des Datendiebstahls.
- Rechtliche Strafen gemäß HIPAA in den USA und DSGVO in Europa.
- Datenpannen können den Betrieb im Gesundheitswesen stören. Sie können Systeme offline nehmen, was zu Verzögerungen, Terminabsagen und administrativen Komplikationen führt. Die Wiederherstellung des normalen Betriebs kann Wochen oder Monate dauern, und während dieser Zeit kann der Krankenhausbetrieb mit reduzierter Kapazität erfolgen.

- Eine weitere Folge von Datenschutzverletzungen im Gesundheitswesen ist der Rufschaden, der dazu führen kann, dass Patienten zögern, sensible medizinische Informationen weiterzugeben. Quellen schätzen, dass die Zahl der Patientenbesuche nach der Verletzung um 4,65 % zurückgegangen ist.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.

- Verschlüsseln Sie vertrauliche Daten und verwenden Sie einen sicheren Speicher, der Vorschriften wie HIPAA und DSGVO entspricht.

- Menschliches Versagen ist eines der größten Cybersicherheitsrisiken. Verbessern Sie die Schulung Ihrer Mitarbeiter und informieren Sie sich über die richtigen Maßnahmen bei Vorfällen und die Auswirkungen auf den Patientendatenschutz.

- Befolgen Sie einen Reaktionsplan für Datenschutzverletzungen, sobald Sie einen potenziellen Angriff erkennen.

5. Weitere Informationen

5.1 Lernmaterialien

- Leitfaden zur Cybersicherheit im Gesundheitswesen (EU-Geltungsbereich) (JGT-7)
- Ein Artikel, der den aktuellen Stand der Cybersicherheit im Gesundheitswesen untersucht. (IST-36)
- Eine Infografik über Sicherheits- und Cybersicherheitsgeräte, die in verschiedenen Gesundheitseinrichtungen eingesetzt werden. (IST-38)
- Bildungsprojekt zur sicheren und verantwortungsvollen digitalen Nutzung. (IST-41)
- Regulierung der Cybersicherheit im Gesundheitswesen (BBS-23)
- Forschungsarbeit zum Thema Cybersicherheit und Intensivpflegepersonal: Eine Mixed-Methods-Studie (PRAMMER-29)
- 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)
- Online-Lektion zum Thema Cybersicherheit (FIRDA-20)

5.2 Relevante Videos

In diesem Video wird erklärt, wie es zu einem Datenleck kommt, wenn vertrauliche Informationen gestohlen werden, und es wird auf die ernsten Risiken hingewiesen, die dies für Einzelpersonen mit sich bringt, darunter Identitätsdiebstahl und finanzielle Verluste.

Die Gefahren einer Datenpanne
https://youtu.be/0kK902-ZvNM?si=88dPA3YzMOBh2Dip

Dieses Video zeigt, dass es in den letzten zwei Jahren in fast allen Gesundheitsorganisationen zu Datenlecks kam, deren Behebung durchschnittlich 2,4 Millionen US-Dollar kostete.

Fallstudien: Risiken von Datenschutzverletzungen im Gesundheitswesen
https://youtu.be/VDrWbjgM3Ik?si=ZsGCq4znqXMylOvH

In diesem Video bespricht der Moderator wichtige Cybersicherheitstrends für 2025 und darüber hinaus, darunter neue Bedrohungen wie KI-gesteuertes Phishing, Deepfake-Betrug und Schatten-KI sowie Verteidigungsinnovationen wie KI-gestützte Vorfallreaktion und den Übergang zu quantenresistenter Kryptografie.

Cybersicherheitstrends für 2025 und darüber hinaus
https://youtu.be/kqaMIFEz15s?si=vfWlFH2uQVbr4OlO

5. 3 Relevante Links

In einem unverschlossenen Zimmer des Tallaght Hospital wurden Hunderte Patientenakten von Kindern entdeckt. Der irische Datenschutzbeauftragte leitete eine Untersuchung wegen möglicher DSGVO-Verstöße im Zusammenhang mit der physischen Speicherung ein. https://www.thesun.ie/news/15690762/children-records-data-breach-tallaght-hospital-hse/?

Bei AMEOS, dem Betreiber von über 100 Gesundheitseinrichtungen in Deutschland, der Schweiz und Österreich, kam es zu einem Datenleck, bei dem Angreifer kurzzeitig Zugriff auf Patienten- und Mitarbeiterdaten erlangten. Das Unternehmen reagierte mit der Deaktivierung von Netzwerken und der Einschaltung forensischer Hilfe. https://www.techradar.com/pro/security/european-healthcare-giant-ameos-reveals-data-breach-millions-of-users-warned-to-be-on-their-guard-heres-what-we-know?

Die französische Datenschutzbehörde CNIL untersucht einen schwerwiegenden Datendiebstahl, von dem über 33 Millionen Menschen betroffen sind. Der Datendiebstahl ereignete sich, als externe Zahlungsabwickler Daten für Zusatzkrankenversicherungen verarbeiteten. Dabei wurden sehr private Bank- und persönliche Informationen offengelegt. https://www.hoganlovells.com/en/publications/significant-data-breach-investigation-launched-by-cnil-affecting-over-33-million-in-france?

6. Literaturverzeichnis

In einem unverschlossenen Zimmer des Tallaght Hospital wurden Hunderte Patientenakten von Kindern entdeckt. Der irische Datenschutzbeauftragte leitete eine Untersuchung wegen möglicher DSGVO-Verstöße im Zusammenhang mit der physischen Speicherung ein. https://www.thesun.ie/news/15690762/children-records-data-breach-tallaght-hospital-hse/?

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

Technologies, I. (7. April 2025). Die 5 alarmierendsten Datenschutzverletzungen im Gesundheitswesen, die Sie kennen sollten.Infosprint Technologies. https://www.infosprint.com/blogs/cybersecurity/the-5-most-alarming-healthcare-data-breaches-you-need-to-know?

Park, E., & Lim, J. H. (2025). Die Auswirkungen von Datenschutzverletzungen im Gesundheitswesen auf das Krankenhausbesuchsverhalten von Patienten.Internationale Zeitschrift für Marketingforschung. https://doi.org/10.1016/j.ijresmar.2025.01.004

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.

CC BY NC