VIOLAZIONE DEI DATI

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

PRAXXER

eolas

BBS Weser

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

Co-funded by
the European Union

Questo progetto è stato co-finanziato con il supporto della Commissione Europea. Questa pubblicazione [comunicazione] riflette solo le opinioni dell'autore, e la Commissione non può essere ritenuta responsabile per l'uso che possa essere fatto delle informazioni ivi contenute.

Indice

Co-funded by the European Union

FACTSHEET - VIOLAZIONE DEI DATI

1. Definizione

Si riferisce a un evento intenzionale o non intenzionale che porta all'accesso non autorizzato, alla divulgazione o alla manipolazione di dati sensibili, riservati o protetti, inclusi i dati dei pazienti e le cartelle cliniche elettroniche. Le violazioni possono derivare da hacking, phishing, configurazione errata, errore interno o furto fisico.

2. Rilevanza generale

Negli ultimi anni si è registrato un aumento delle violazioni dei dati, sia in termini di frequenza che di gravità. Circa il 46% di questi incidenti colpisce direttamente i dati sensibili dei pazienti e la proprietà intellettuale, spesso tramite attacchi ransomware.

Le violazioni dei dati comportano costi significativi e possono danneggiare la reputazione aziendale perché espongono dati personali, finanziari o proprietari. Quando si verifica un attacco, le aziende devono interrompere i propri sistemi per analizzarlo, il che causa ritardi, cancellazioni e perdite di vendite.

3. Importanza nella salute e nell'assistenza e impatto sulla qualità dell'assistenza

I criminali informatici sono particolarmente interessati alle violazioni della privacy in ambito sanitario. Ciò è dovuto all'enorme quantità di dati privati e finanziari raccolti dalle persone, che causa danni significativi sia agli ospedali che ai pazienti. Le informazioni rubate possono essere utili per il furto di identità e hanno un grave impatto sulla salute e sulle cure dei pazienti:

1. I rischi per la sicurezza dei pazienti si verificano quando gli aggressori modificano le informazioni dei pazienti, come le prescrizioni e la storia clinica, il che può portare a una somministrazione errata dei farmaci o a ritardi nel trattamento di malattie gravi.
2. Secondo IBM, il costo delle violazioni dei dati nel settore sanitario ammonta a 10,98 milioni di dollari. Questo importo include le spese per i farmaci, la notifica ai pazienti interessati e la formazione di un team per indagare sul furto di dati.
3. Sanzioni legali, secondo l'HIPAA negli Stati Uniti e il GDPR in Europa.
4. Le violazioni dei dati possono compromettere le attività sanitarie. Possono mettere offline i sistemi, causando ritardi, appuntamenti annullati e complicazioni amministrative. Il ripristino del normale funzionamento può richiedere settimane o mesi e, durante questo periodo, l'ospedale potrebbe operare a capacità ridotta.
5. Un'altra conseguenza delle violazioni dei dati in ambito sanitario è il danno reputazionale, che può indurre i pazienti a esitare a condividere informazioni mediche sensibili. Le fonti stimano un calo del 4,65% delle visite dei pazienti dopo la violazione.

4. Cosa posso fare come professionista sanitario?

- Utilizza un accesso sicuro effettuando l'accesso tramite piattaforme cloud ospedaliere autorizzate con password complesse e autenticazione a due fattori.
- Crittografa i dati sensibili e utilizza un archivio sicuro conforme alle normative HIPAA e GDPR.
- L'errore umano è uno dei rischi più significativi per la sicurezza informatica. Migliorate la formazione dei dipendenti e rimanete aggiornati su come rispondere agli incidenti e sull'impatto sulla protezione dei dati dei pazienti.
- Non appena si rileva un potenziale attacco, è necessario adottare un piano di risposta alle violazioni dei dati.

5. Ulteriori informazioni

5.1 Materiali didattici

- Cibersecurity guide for healthcare sector (EU scope) (JGT-7)
- An article exploring the current state of cybersecurity in healthcare. (IST-36)
- An infographic on security and cybersecurity devices used in different healthcare settings. (IST-38)
- Educational project on safe and responsible digital use. (IST-41)
- Regulation of cybersecurity in healthcare (BBS-23)
- Research paper on Cybersecurity and critical care staff: A mixed methods study (PRAMMER-29)
- Cyber-attacks are a permanent and substantial threat to health systems: Education must reflect that (PRAMMER-32)
- Gamification and Serious Games for Cybersecurity Awareness and First Responders Training: An overview (PRAMMER-33)
- A Serious Game for Healthcare Industry: Information Security Awareness Training Program for Hospital Universiti Kebangsaan Malaysia (PRAMMER-34)
- Systematically Applying Gamification to Cyber Security Awareness Trainings: A framework and case study approach (PRAMMER-35)

5.2 Video correlati

Questo video spiega come avviene una violazione dei dati quando vengono rubate informazioni sensibili e sottolinea i gravi rischi che ciò comporta per gli individui, tra cui il furto di identità e la perdita di denaro.

I pericoli di una violazione dei dati
https://youtu.be/0kK902-ZvNM?si=88dPA3YzMOBh2Dip

Questo video mostra che quasi tutte le organizzazioni sanitarie hanno subito violazioni dei dati negli ultimi due anni, ciascuna delle quali ha comportato un costo medio di 2,4 milioni di dollari per la risoluzione.

Casi di studio: rischi di violazione dei dati sanitari
https://youtu.be/VDrWbjgM3Ik?si=ZsGCq4znqXMylOvH

In questo video, il presentatore discute le principali tendenze in materia di sicurezza informatica per il 2025 e oltre, come le minacce emergenti come il phishing basato sull'intelligenza artificiale, le frodi deepfake e l'intelligenza artificiale ombra, nonché le innovazioni in materia di difesa come la risposta agli incidenti assistita dall'intelligenza artificiale e la transizione alla crittografia resistente ai quanti.

Tendenze della sicurezza informatica per il 2025 e oltre
https://youtu.be/kqaMIFEz15s?si=vfWlFH2uQVbr4OlO

5.3 Link rilevanti

Centinaia di cartelle cliniche di pazienti pediatrici sono state scoperte in una stanza non chiusa a chiave del Tallaght Hospital. Il Commissario irlandese per la protezione dei dati ha avviato un'indagine su potenziali violazioni del GDPR relative alle pratiche di archiviazione fisica.
https://www.thesun.ie/news/15690762/children-records-data-breach-tallaght-hospital-hse/?

AMEOS, che gestisce oltre 100 strutture sanitarie in Germania, Svizzera e Austria, ha subito una violazione dei dati grazie alla quale gli aggressori hanno ottenuto brevemente l'accesso ai dati di pazienti e dipendenti. L'organizzazione ha risposto disattivando le reti e richiedendo l'intervento di esperti forensi.
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?

La CNIL in Francia sta indagando su una grave violazione che ha colpito oltre 33 milioni di persone. La violazione si è verificata quando elaboratori di pagamenti terzi hanno gestito dati per l'assicurazione sanitaria complementare, esponendo informazioni bancarie e personali molto riservate.
https://www.hoganlovells.com/en/publications/significant-data-breach-investigation-launched-by-cnil-affecting-over-33-million-in-france?

6. Bibliografia

European action plan on the cybersecurity of hospitals and healthcare providers. (2025, 8 agosto). Public Health. https://health.ec.europa.eu/ehealth-digital-health-and-care/digital-health-and-care/european-action-plan-cybersecurity-hospitals-and-healthcare-providers_en

ENISA threat landscape: Health Sector - CYBIL portal. (2023, 5 julio). Cybil Portal. https://cybilportal.org/publications/enisa-threat-landscape-health-sector/

Technologies, I. (2025, 7 abril). The 5 Most Alarming Healthcare Data Breaches You Need to Know. 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). The impact of healthcare data breaches on patient hospital visit behavior. International Journal Of Research In Marketing. 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

Questo progetto è stato co-finanziato con il supporto della Commissione Europea. Questa pubblicazione [comunicazione] riflette solo le opinioni dell'autore, e la Commissione non può essere ritenuta responsabile per l'uso che possa essere fatto delle informazioni ivi contenute.