SICUREZZA DEL CLOUD

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

1. Definizione 1
2. Rilevanza generale 1
3. Importanza nella salute e nell'assistenza e impatto sulla qualità dell'assistenza 1
4. Cosa posso fare come professionista sanitario? 2
5. Ulteriori informazioni 2
    1. Materiali didattici 2
    2. Video correlati 2
    3. Link rilevanti 3
6. Bibliografia 4

Co-funded by the European Union

FACTSHEET - SICUREZZA DEL CLOUD

1. Definizione

Si riferisce a una serie di policy, controlli, procedure e tecnologie il cui scopo è proteggere sistemi, dati e infrastrutture basati sul cloud. Affronta questioni come la privacy dei dati, la gestione dell'identità e degli accessi, la conformità e la resilienza contro gli attacchi informatici derivanti dalla "cloudificazione" dei dati dei pazienti in ambito sanitario.

2. Rilevanza generale

La sicurezza del cloud è un'area di crescente preoccupazione, poiché il settore sanitario adotta sempre più servizi cloud per l'archiviazione e l'elaborazione dei dati, che richiedono linee guida e pratiche di sicurezza specifiche. Minacce informatiche, violazioni o configurazioni errate possono esporre informazioni sensibili senza una solida protezione cloud. Data la sua natura condivisa, una falla nella sicurezza può colpire milioni di utenti contemporaneamente, causando non solo danni finanziari e reputazionali, ma anche compromettendo la conformità ai quadri normativi (GDPR in Europa o HIPAA negli Stati Uniti).

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

La necessità di tecnologia in ambito clinico è cresciuta di recente; cloud computing, telemedicina, intelligenza artificiale e sanità elettronica possono spesso offrire servizi di qualità superiore. Inoltre, l'utilizzo della tecnologia cloud nelle cartelle cliniche elettroniche facilita l'accesso dei pazienti alle proprie informazioni sanitarie, semplice e completo. L'uso della tecnologia cloud trasforma il modo in cui medici, infermieri, cliniche e ospedali forniscono ai pazienti servizi di alta qualità e finanziariamente vantaggiosi.

Il cloud computing offre numerosi vantaggi, tra cui una collaborazione semplice e pratica tra gli utenti, costi ridotti, maggiore velocità, scalabilità e flessibilità. Tuttavia, nonostante i numerosi vantaggi, presenta anche alcuni aspetti negativi e sfide. Il cloud computing comporta anche rischi elevati, che possono far sì che una violazione o un periodo di inattività di un sistema ospitato nel cloud esponga informazioni altamente sensibili, ritardi nelle cure o persino interrompa i servizi di emergenza.

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.
- Evitare di condividere file con informazioni personali al di fuori del sistema cloud ufficiale.
- Prestare attenzione alle minacce informatiche (e-mail di phishing, link sospetti) e segnalare immediatamente eventuali irregolarità
- Partecipa alla formazione sulla sicurezza informatica e resta aggiornato su come rispondere agli incidenti e sull'impatto della protezione dei dati dei pazienti.

5. Ulteriori informazioni

5.1 Materiali didattici

- Cybersecurity for SMEs & self-employed (JGT-6)
- General training (71 infopacks) about cibersecurity descriptions. Provided by cryptographic National centre. (JGT-10)
- An infographic on security and cybersecurity devices used in different healthcare settings. (IST-38)
- An overview of cybersecurity in healthcare, focusing on the role of AI and its regulatory framework. (IST-39)
- 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)
- Cybersecurity for entities (HIPAA), full pack including checklists (FIRDA-12)
- Video training for professionals and students (FIRDA-13)

5.2 Video correlati

Questo video illustra il modello di responsabilità condivisa per gli ambienti cloud. Spiega che le aziende sono responsabili della sicurezza delle proprie applicazioni, dei carichi di lavoro e dei dati, mentre il fornitore del cloud è responsabile della sicurezza dell'infrastruttura che li supporta.

Che cos'è la sicurezza nel cloud?
https://youtu.be/jI8IKpjiCSM?si=vXJzAbIsRoj2ltDh

Il prossimo video mostra come il cloud computing viene utilizzato in ambito sanitario, soppesando i suoi pro, come un migliore accesso e scalabilità, e i contro, come i rischi per la privacy dei dati e le possibili dipendenze del sistema.

Cloud Computing in sanità: pro e contro
https://youtu.be/xEl_6NZuyS4?si=cFApA9QgHFCEBzPi

5.3 Link rilevanti

Questo articolo descrive come un errore di configurazione nel portale di vaccinazione basato su Salesforce dell'Health Service Executive abbia reso pubblici i dati personali e di vaccinazione di oltre un milione di cittadini irlandesi, nonché documenti interni dell'HSE.
https://appomni.com/blog/saas-risks-in-healthcare-data-exposure-in-hse/

Secondo questo articolo, un database cloud reso accessibile al pubblico ha rivelato circa 957.000 dati relativi all'assistenza sanitaria, tra cui informazioni sensibili sul personale e sulle assunzioni, a causa della mancanza di protezione tramite password.
https://www.cybersecurity-insiders.com/cloud-security-breach-leads-to-a-leak-of-957000-patient-records/

Un'azienda finlandese di psicoterapia ha subito una grave violazione dei dati che ha reso pubblici i dati privati dei pazienti. La violazione, che ha portato all'estorsione nei confronti della clinica e dei suoi pazienti, è costata alla clinica 608.000 euro ai sensi del GDPR per scarsa sicurezza e mancata segnalazione tempestiva della violazione. Le conseguenze hanno avuto un impatto significativo sulla fiducia e sulla salute mentale dei pazienti.
https://www.wired.com/story/finland-mental-health-data-breach-vastaamo/

6. Bibliografia

Liveri, D., Athanasios, D., & Zisi, A. (2021). ENISA Cloud Security for the Healthcare Services. Enisa.
https://doi.org/10.2824/454966

Tahir, A., Chen, F., Khan, H. U., Ming, Z., Ahmad, A., Nazir, S., & Shafiq, M. (2020). A Systematic Review on Cloud Storage Mechanisms Concerning e-Healthcare Systems. Sensors, 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). Security challenges and solutions using healthcare cloud computing. Journal Of Medicine And Life, 14(4), 448-461.
https://doi.org/10.25122/jml-2021-0100

Guidance on HIPAA & Cloud Computing. (2022, diciembre). U.S. Department Of Health And Human Services. Recuperado 28 de agosto de 2025, de 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

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.