ERRORI, CONFIGURAZIONI ERRATE E PRATICHE DI SICUREZZA SCARSE

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 - ERRORI, CONFIGURAZIONI ERRATE E PRATICHE DI SICUREZZA SCARSE

1. Definizione

Si tratta di vulnerabilità interne ed errori umani involontari, come configurazioni errate o pratiche di sicurezza inadeguate, che possono portare a incidenti di sicurezza, tra cui fughe di dati. Alcuni esempi sono password deboli, privilegi utente eccessivi, mancata applicazione di patch o crittografia non adeguata.

2. Rilevanza generale

Questi problemi sono rilevanti perché consentono ai criminali di compromettere i sistemi senza sforzo. La maggior parte delle fughe di dati è causata da errori umani o da una configurazione errata, il che evidenzia l'importanza di solide pratiche di sicurezza informatica interna e del fattore umano nella strategia di sicurezza complessiva.

Secondo IBM, gli errori umani rappresentano oltre il 20% di tutte le violazioni, con un costo per le organizzazioni che ammonta a milioni. Anche una configurazione errata può causare un'esposizione a lungo termine. Ad esempio, un server non configurato correttamente può divulgare dati sensibili per mesi prima che qualcuno se ne accorga. Pertanto, correggere gli errori e garantire il rispetto delle procedure di sicurezza sono entrambi aspetti cruciali della sicurezza informatica per le aziende.

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

Errori e configurazioni errate in ambito sanitario hanno un impatto diretto sulla sicurezza, la privacy e la qualità delle cure dei pazienti. Quando interessano i dispositivi medici, possono causare un dosaggio errato dei farmaci, allarmi ritardati o malfunzionamenti dei servizi di monitoraggio.

Anche le informazioni sensibili contenute nelle cartelle cliniche dei pazienti potrebbero essere rese pubbliche, il che violerebbe le normative GDPR e HIPAA e comprometterebbe la fiducia del pubblico nei confronti degli operatori sanitari.

In definitiva, una scarsa igiene informatica, come software obsoleti o autorizzazioni utente improprie, può consentire agli aggressori di infiltrarsi nelle reti, interrompere le operazioni ospedaliere, ritardare le procedure e ridurre la qualità dell'assistenza. La violazione di SingHealth a Singapore (2018) ha comportato configurazioni errate nei controlli di accesso alla rete, compromettendo i dati sanitari personali di 1,5 milioni di pazienti.

4. Cosa posso fare come professionista sanitario?

- Seguire le linee guida e i protocolli di sicurezza dell'organizzazione.
- Utilizza un accesso sicuro effettuando l'accesso tramite piattaforme cloud ospedaliere autorizzate con password complesse e autenticazione a due fattori.
- Segnalare immediatamente al team IT qualsiasi comportamento anomalo del sistema o potenziale configurazione errata.
- Partecipa alla formazione sulla sicurezza informatica e resta aggiornato su come rispondere agli incidenti e sull'impatto della protezione dei dati dei pazienti per ridurre l'errore umano.

5. Ulteriori informazioni

5.1 Materiali didattici

- Cybersecurity for your sector (JGT-1)
- Sequential videos for general topics about cybersecurity (JGT-2)
- Web seminars about key aspects of cibersecurity (JGT-3)
- Awareness kit about cibersecurity in enterprises (JGT-4)
- Cybersecurity for SMEs & self-employed (JGT-6)
- Cibersecurity guide for healthcare sector (EU scope) (JGT-7)
- Cibersecurity training from National Cryptographic Centre of Spain. Requires National login (JGT-8)
- An article exploring the current state of cybersecurity in healthcare. (IST-36)
- Educational project on safe and responsible digital use. (IST-41)
- IT Security Requirements and Protective Measures – Tips and Practical Examples (BBS-42)
- Research paper on Cybersecurity and critical care staff: A mixed methods study (PRAMMER-29)
- A Critical Review on Cybersecurity Awareness Frameworks and Training Models (PRAMMER-30)
- An integrated cybernetic awareness strategy to assess cybersecurity attitudes and behaviours in school context (PRAMMER-31)
- 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

Il webinar analizza come gli errori medici in terapia intensiva siano spesso prevedibili e prevenibili, sottolineando l'importanza della consapevolezza, dei miglioramenti del sistema e delle pratiche di sicurezza dei pazienti per ridurre i danni.

[Webinar] Errori medici, danni e sicurezza del paziente
https://youtu.be/VB7MsPH_sG8?si=rNpZrED9yTYm7oyu

5.3 Link rilevanti

Questo articolo spiega come un errore di configurazione nel portale irlandese per la vaccinazione contro il COVID-19 (basato su Salesforce) abbia consentito agli utenti registrati di accedere a documenti HSE interni e a dati personali sensibili appartenenti a oltre un milione di persone.
https://www.darkreading.com/cyberattacks-data-breaches/nhs-breach-hse-bug-expose-healthcare-data-british-isles

Errori di configurazione hanno reso accessibili al pubblico migliaia di server di imaging DICOM, esponendo nomi di pazienti, date di nascita, informazioni sulle malattie e immagini mediche, con conseguenze sui sistemi di diversi Paesi.
https://www.sharitsec.eu.org/2023/09/critical-dicom-server-misconfigurations.html

Molti dispositivi medici hanno credenziali codificate o non dispongono della corretta autenticazione, il che li rende facili bersagli per attacchi come il denial-of-service o la manomissione.
https://www.csoonline.com/article/568861/insecure-configurations-expose-ge-healthcare-devices-to-attacks.html

6. Bibliografia

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

Cost of a data breach 2025 | IBM. (s. f.).
https://www.ibm.com/reports/data-breach

Wikipedia contributors. (2025, 7 agosto). 2018 SingHealth data breach. Wikipedia.
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

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.