RESILIENZA CIBERNETICA

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 - RESILIENZA CIBERNETICA

1. Definizione

È la capacità di un'organizzazione di prepararsi, rispondere e riprendersi dalle minacce informatiche, garantendo al contempo l'assistenza ai pazienti e la continuità operativa. Si concentra sulla riduzione al minimo delle interruzioni causate dagli attacchi informatici e sulla garanzia della sicurezza dei dati sensibili.

Questo concetto combina continuità aziendale, sicurezza dei sistemi informativi e resilienza organizzativa. Descrive la capacità di continuare a raggiungere i risultati attesi nonostante eventi cibernetici complessi.

2. Rilevanza generale

La resilienza cibernetica è rilevante in tutti i settori a causa della dipendenza digitale. Oggigiorno, governi, aziende e privati si affidano a sistemi digitali per le operazioni, le comunicazioni e l'archiviazione dei dati. Questa dipendenza dalla tecnologia ha portato numerosi vantaggi, come l'accesso rapido alle informazioni, un migliore coordinamento dell'assistenza e l'ottimizzazione delle risorse, tra gli altri. Tuttavia, ha anche aumentato la portata e la sofisticatezza delle minacce e degli attacchi informatici, rendendo la prevenzione della sicurezza informatica una questione di alta priorità.

Un altro fattore che rende la resilienza cibernetica una questione importante da affrontare a livello globale è la consapevolezza che le violazioni sono inevitabili e l'attenzione rivolta a come adattarsi, recuperare e prosperare dopo gli incidenti, non solo a prevenirli.

Ecco alcuni dei vantaggi della resilienza informatica:

- **Continuità aziendale:** garantisce che le operazioni aziendali critiche possano continuare durante gli incidenti informatici attivi, riducendo significativamente le interruzioni operative anche quando le difese convenzionali sono compromesse.
- **Tempi di inattività ridotti:** riduce la quantità di tempo e risorse che andrebbero perse durante interruzioni prolungate, consentendo alle organizzazioni di riprendersi rapidamente da attacchi e incidenti.
- **Protezione finanziaria:** riduce i costi associati a guasti del sistema, violazioni dei dati e potenziali conseguenze legali, che in genere seguono incidenti di sicurezza significativi.
- **Gestione della reputazione:** crea e mantiene la fiducia delle parti interessate dimostrando l'affidabilità dell'organizzazione e la sua capacità di gestire sfide impreviste in materia di sicurezza.
- **Conformità normativa:** garantisce che le pratiche organizzative aderiscano alle leggi più severe. Cyber Resilience, appena lanciato, sottolinea la crescente attenzione normativa rivolta a questo tema.
- **Vantaggio sul mercato:** dimostrando solide procedure di sicurezza che distinguono l'azienda dai concorrenti meno preparati, attrae clienti e partner attenti alla sicurezza, concorrenti impreparati.

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

L'assistenza sanitaria moderna si basa su sistemi strettamente interconnessi. A causa dell'enorme quantità di dati sensibili dei pazienti in essa contenuti e della criticità delle sue operazioni, il settore sanitario è diventato il bersaglio principale dei criminali informatici.

La resilienza è fondamentale per prevenire interruzioni estese del servizio, poiché il guasto di un componente potrebbe estendersi all'intera infrastruttura sanitaria. La vita di persone può essere messa direttamente in pericolo se sistemi sanitari vitali, come le cartelle cliniche elettroniche o i dispositivi medici, vengono interrotti. Per proteggere la sicurezza e la privacy dei pazienti, la resilienza cibernetica garantisce la continuità dell'assistenza anche in caso di attacchi.

Inoltre, preservare la fiducia di partner, pazienti e pubblico in generale dipende dalla resilienza informatica. Poiché i dati dei pazienti contengono informazioni estremamente sensibili, interruzioni o compromissioni possono danneggiare la reputazione delle organizzazioni sanitarie.

4. Cosa posso fare come professionista sanitario?

- Mantenere una buona igiene informatica, con misure come l'utilizzo di password complesse, l'abilitazione dell'autenticazione a due fattori e il costante aggiornamento del software.
- Proteggere i dati dei pazienti. Segnalando tempestivamente qualsiasi attività sospetta e gestendo attentamente le informazioni nelle attività quotidiane.
- Partecipa alla formazione informatica. Iscrivendoti a corsi che trattano tecniche di prevenzione, rilevamento e risposta alle violazioni dei dati.

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)
- Online workshop on how to set-up our device. (JGT-5)
- 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)
- General training (71 infopacks) about cibersecurity descriptions. Provided by cryptographic National centre. (JGT-10)
- An article exploring the current state of cybersecurity in healthcare. (IST-36)
- An article on security strategies applicable to electronic patient records (IST-37)

- 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)
- A compendium on the processing of patient data on online platforms. (IST-40)
- Educational project on safe and responsible digital use. (IST-41)
- Regulation of cybersecurity in healthcare (BBS-23)
- Cybersecurity of hospitals and healthcare providers (BBS-24)
- Digital Identities - With Security in Mind (BBS-25)
- 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

Questo video approfondisce la sfida di raggiungere la resilienza cibernetica nel sistema sanitario, illustrando come il panorama della sanità digitale sia in continua evoluzione. Sottolinea inoltre l'importanza di costruire solide difese di sicurezza informatica in grado di adattarsi e ripristinarsi in tempo reale.

Cosa ci vorrà per costruire una vera resilienza cibernetica nel settore sanitario?
https://youtu.be/BNsD1jKZ8Es?si=wcFCbn65VHv3aLzH

Il prossimo video si concentra su come costruire la resilienza cibernetica in ambito sanitario. Offre consigli pratici per integrare e rafforzare la sicurezza dei dati nei sistemi clinici, in un panorama sanitario digitale in rapida evoluzione. La proposta è di integrare misure di sicurezza nelle operazioni sanitarie per garantire che i sistemi rimangano resilienti alle minacce costanti.

Come costruire la resilienza cibernetica nel settore sanitario | Discorso principale HealthSec 2025
https://youtu.be/U7LIBdQi78k?si=aKhDfOr3aMyzQB32

5.3 Link rilevanti

Questo articolo sottolinea come l'inazione e gli investimenti insufficienti nella resilienza IT abbiano un impatto significativo sull'assistenza ai pazienti, sulla continuità operativa e sulla sicurezza di fronte alla crescente minaccia di attacchi informatici e interruzioni tecniche nel settore sanitario.
https://www.mckinsey.com/industries/healthcare/our-insights/tech-resilience-for-healthcare-providers-inaction-has-a-heavy-toll?utm_source=chatgpt.com

Per garantire la continuità dell'assistenza ai pazienti anche in caso di attacchi informatici, l'articolo sottolinea l'importanza che le organizzazioni sanitarie diano priorità alla resilienza cibernetica. Questo obiettivo può essere raggiunto andando oltre la prevenzione, puntando alla prontezza, attraverso una pianificazione coordinata del ripristino e un'infrastruttura solida.
https://www.rubrik.com/blog/company/25/7/cyber-resilience-in-healthcare-preparing-for-the-inevitable-attack?utm_source=chatgpt.com

Nel maggio 2021, l'Health Service Executive (HSE) irlandese è stato vittima di un devastante attacco ransomware Conti che ha bloccato i sistemi IT a livello nazionale, paralizzando i servizi sanitari, esponendo dati sensibili e richiedendo un lungo processo di ripristino che ha comportato il ricorso a metodi tradizionali (carta e penna) e un'approfondita revisione post-incidente.
https://en.wikipedia.org/wiki/Health_Service_Executive_ransomware_attack?utm_source=chatgpt.com

6. Bibliografia

Susnjara, S., & Smalley, I. (2025, 13 agosto). Cyber Resilience. IBM. Recuperado 18 de agosto de 2025, de https://www.ibm.com/think/topics/cyber-resilience

Tashi, K., & Beato, F. (2024, 1 febrero). Healthcare pays the highest price of any sector for cyberattacks — that's why cyber resilience is key. World Economic Forum. Recuperado 18 de agosto de 2025, de https://www.weforum.org/stories/2024/02/healthcare-pays-the-highest-price-of-any-sector-for-cyberattacks-that-why-cyber-resilience-is-key/?utm_source=chatgpt.com

What is Cyber Resilience and Why Does it Matter? | Fortinet. (s. f.). Fortinet. https://www.fortinet.com/resources/cyberglossary/cyber-resilience?utm_source=chatgpt.com

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.