ATTACCHI ALLA CATENA DI APPROVVIGIONAMENTO

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 - ATTACCHI ALLA CATENA DI APPROVVIGIONAMENTO

1. Definizione

Si verifica quando un malintenzionato prende di mira un'organizzazione compromettendo elementi meno sicuri nella sua catena di approvvigionamento anziché direttamente l'organizzazione principale, come fornitori terzi o provider di servizi, per ottenere l'accesso al bersaglio principale.

Ciò rende difficile individuarlo e colpisce un gran numero di persone, poiché una singola violazione può colpire più organizzazioni a valle.

2. Rilevanza generale

A causa della forte dipendenza delle organizzazioni dalle reti di terze parti, gli attacchi alla catena di approvvigionamento stanno diventando una minaccia sempre più grave a livello mondiale. Grazie a questa connessione, gli aggressori possono prendere di mira un fornitore più piccolo e meno sicuro invece di cercare di penetrare in un sistema ben protetto.

Tutto quanto sopra esposto rende difficile rilevare questo tipo di violazione. Spesso, si presenta come un aggiornamento legittimo o un'operazione di sistema. Basta un solo provider compromesso per esporre migliaia di clienti.

Inoltre, gli attacchi alla catena di approvvigionamento sono strategicamente allettanti sia per i gruppi sponsorizzati dallo Stato che per i criminali informatici, poiché hanno un impatto e una portata maggiori. Con l'aumento del numero di persone che utilizzano servizi cloud e servizi di altre aziende, si prevede che le possibilità e gli effetti di questo tipo di attacchi peggioreranno notevolmente.

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

Un attacco alla catena di approvvigionamento nel settore sanitario non solo comporta perdite finanziarie o danni alla reputazione, ma influisce anche sulla sicurezza dei pazienti e sulla qualità dell'assistenza. Poiché gli ospedali si affidano a terzi (ad esempio, cartelle cliniche elettroniche, sistemi diagnostici e di imaging, servizi cloud, ecc.), una violazione potrebbe significare l'accesso totale ai dati sensibili dei pazienti, causando disagio psicologico o frodi finanziarie ai loro danni.

Questa situazione ha un impatto significativo sulla qualità dell'assistenza. Le fonti descrivono come il ransomware diffuso attraverso una compromissione della catena di approvvigionamento potrebbe ritardare interventi chirurgici, posticipare i risultati di laboratorio, ecc., il che potrebbe aumentare i tassi di morbilità e mortalità nelle emergenze.

4. Cosa posso fare come professionista sanitario?

- Segnalare qualsiasi comportamento anomalo del sistema.
- Fate attenzione alle e-mail, ai portali o alle app di fornitori terzi.
- Seguire i protocolli organizzativi e rispettare sempre le restrizioni di sicurezza.
- Partecipa alla formazione informatica e resta aggiornato su come i rischi della catena di approvvigionamento si manifestano nel tuo lavoro quotidiano.

5. Ulteriori informazioni

5.1 Materiali didattici

- Web seminars about key aspects of cibersecurity (JGT-3)
- Cibersecurity guide for healthcare sector (EU scope) (JGT-7)
- 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)
- 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)

5.2 Video correlati

Questo video descrive cosa sono gli attacchi dannosi alla catena di approvvigionamento, come vengono identificati e gestiti e come le organizzazioni del settore possono prevenirli.

Che cosa sono gli attacchi alla catena di approvvigionamento | Attacchi alla catena di approvvigionamento nella sicurezza informatica | Intellipaat

https://www.youtube.com/live/LIkxOiNOkec?si=W-h6-lM893uKdTnt

In questo video viene illustrato come le debolezze dei fornitori di software e hardware di terze parti possano rendere i sistemi sanitari più vulnerabili agli attacchi informatici, mettendo a rischio la sicurezza dei pazienti e la resilienza operativa.

Come la catena di approvvigionamento rende l'assistenza sanitaria vulnerabile agli attacchi informatici

https://youtu.be/IFBBxNiKysY?si=0UhDHhqvG2LC8DTh

Questo breve video intitolato "2 Minute Drill" parla delle recenti violazioni della catena di approvvigionamento e di come queste mettano a rischio la sicurezza dei pazienti nei sistemi sanitari.

Esercitazione di 2 minuti: violazioni della catena di approvvigionamento e rischi per la sicurezza dei pazienti con Drex DeFord
https://youtu.be/mi9t_AhLcIQ?si=kheM-OWdkFZG1hyD

5.3 Link rilevanti

Questo articolo descrive un caso in cui Shields Health Care Group, Eye Care Leaders e MCG Health sono stati coinvolti in violazioni della catena di approvvigionamento che hanno avuto un impatto complessivo su oltre 4,3 milioni di persone. Shields da sola ha interessato circa 2 milioni di pazienti. Questi incidenti dimostrano come un singolo fornitore compromesso possa mettere a repentaglio i dati dei pazienti di più operatori sanitari.
https://planet9security.com/supply-chain-attacks-in-healthcare-the-case-of-shields-eye-care-leaders-and-mcg-health/?

Un importante distributore farmaceutico spagnolo, Alliance Healthcare, ha subito un attacco informatico che ha bloccato il suo sito web, i sistemi di fatturazione e l'elaborazione degli ordini. Le rotte di approvvigionamento alternative hanno limitato l'impatto sui pazienti, ma l'interruzione ha evidenziato i rischi associati ai canali di distribuzione dei farmaci.
https://www.scworld.com/news/cyberattack-hits-spanish-pharmaceutical-company-alliance-healthcare?

6. Bibliografia

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

Organization, W. I. P. (2022). Global Innovation Index 2022: What is the Future of Innovation-driven Growth? WIPO. https://www.wipo.int/edocs/pubdocs/en/wipo-pub-2000-2022-en-main-report-global-innovation-index-2022-15th-edition.pdf

Lella, I., Theocharidou, M., Tsekmezoglou, E., Malatras, A., & García, S. (2021). ENISA Threat Landscape for Supply Chain Attacks. https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%20for%20Supply%20Chain%20Attacks.pdf

BobSulli. (2024, 17 octubre). The 2024 Study on Cyber Insecurity in Healthcare: The Cost and Impact on Patient Safety and Care | Ponemon-Sullivan Privacy Report. https://ponemonsullivanreport.com/2024/10/the-2024-study-on-cyber-insecurity-in-healthcare-the-cost-and-impact-on-patient-safety-and-care/

European Data Protection Board (2021). Guidelines 07/2020 on the concepts of controller and processor in the GDPR. https://www.edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf

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.