ANGRIFFE AUF DIE LIEFERKETTE

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

PRAMMER

eolas

BBS Weser

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

Co-funded by
the European Union

Dieses Projekt wurde mit Unterstützung der Europäischen Kommission kofinanziert. Die Verantwortung für den Inhalt dieser Veröffentlichung [Mitteilung] trägt allein der Verfasser; die Kommission haftet nicht für die weitere Verwendung der darin enthaltenen Informationen.

Inhaltsverzeichnis

Co-funded by the European Union

FACTSHEET – ANGRIFFE AUF DIE LIEFERKETTE

1. Definition

Es tritt auf, wenn ein böswilliger Akteur eine Organisation ins Visier nimmt, indem er weniger sichere Elemente in ihrer Lieferkette kompromittiert, anstatt die Hauptorganisation direkt zu erreichen, wie etwa Drittanbieter oder Dienstleister, um Zugang zum Hauptziel zu erhalten.1.

Dies erschwert die Erkennung und betrifft eine große Anzahl von Personen, da ein einzelner Verstoß mehrere nachgelagerte Organisationen betreffen kann.

2. Allgemeine Bedeutung

Da Unternehmen stark von Netzwerken Dritter abhängig sind, werden Angriffe auf die Lieferkette weltweit zu einer ernstzunehmenden Bedrohung. Durch diese Vernetzung können Angreifer kleinere, weniger sichere Lieferanten angreifen, anstatt in ein gut geschütztes System einzudringen.2.

All dies erschwert die Erkennung solcher Sicherheitsverletzungen. Oftmals handelt es sich dabei um legitime Updates oder Systemoperationen. Ein einziger kompromittierter Anbieter genügt, um Tausende von Kunden zu gefährden.

Darüber hinaus sind Angriffe auf die Lieferkette sowohl für staatlich geförderte Gruppen als auch für Cyberkriminelle strategisch attraktiv, da sie die größte Wirkung und Reichweite haben. Da immer mehr Menschen Cloud-Dienste und Dienste anderer Unternehmen nutzen, werden die Wahrscheinlichkeit und die Auswirkungen solcher Angriffe voraussichtlich deutlich zunehmen.3.

3. Bedeutung für Gesundheit und Pflege und Auswirkungen auf die Pflegequalität

Ein Angriff auf die Lieferkette im Gesundheitswesen führt nicht nur zu finanziellen oder Reputationsverlusten, sondern beeinträchtigt auch die Patientensicherheit und die Qualität der Versorgung.4Da Krankenhäuser auf Drittanbieter angewiesen sind (z. B. elektronische Patientenakten, Diagnose- und Bildgebungssysteme, Cloud-Dienste usw.), könnte ein Verstoß den vollständigen Zugriff auf sensible Patientendaten bedeuten und so psychische Belastungen oder finanziellen Betrug gegenüber Patienten verursachen.5.

Diese Situation hat erhebliche Auswirkungen auf die Qualität der Versorgung. Quellen beschreiben, wie Ransomware, die durch eine Kompromittierung der Lieferkette eingeschleust wird, Operationen verzögern, Laborergebnisse verschieben usw. kann, was in Notfällen zu einer Erhöhung der Morbiditäts- und Mortalitätsraten führen kann.

4. Was kann ich als medizinisches Fachpersonal tun?

- Melden Sie jedes ungewöhnliche Systemverhalten.
- Seien Sie vorsichtig bei E-Mails, Portalen oder Apps von Drittanbietern.
- Befolgen Sie die Organisationsprotokolle und halten Sie sich stets an die Sicherheitsbeschränkungen.
- Nehmen Sie an Cyber-Schulungen teil und bleiben Sie auf dem Laufenden, wie sich Lieferkettenrisiken in Ihrer täglichen Arbeit manifestieren.

5. Weitere Informationen

5.1 Lernmaterialien

- Webseminare zu wichtigen Aspekten der Cybersicherheit (JGT-3)
- Leitfaden zur Cybersicherheit im Gesundheitswesen (EU-Geltungsbereich) (JGT-7)
- Ein Artikel über Sicherheitsstrategien für elektronische Patientenakten (IST-37)
- Eine Infografik über Sicherheits- und Cybersicherheitsgeräte, die in verschiedenen Gesundheitseinrichtungen eingesetzt werden. (IST-38)
- Gamifizierung und Serious Games zur Sensibilisierung für Cybersicherheit und zur Ausbildung von Ersthelfern: Ein Überblick (PRAMMER-33)
- Ein Serious Game für die Gesundheitsbranche: Informationssicherheits-Sensibilisierungstraining für das Krankenhaus Universiti Kebangsaan Malaysia (PRAMMER-34)
- Videotraining für Fachleute und Studierende (FIRDA-13)

5.2 Relevante Videos

In diesem Video wird beschrieben, was böswillige Angriffe auf die Lieferkette sind, wie sie erkannt und bekämpft werden und wie Branchenorganisationen sie verhindern können.

Was ist ein Supply-Chain-Angriff? | Supply-Chain-Angriffe in der Cybersicherheit | Intellipaat
https://www.youtube.com/live/LIkxOiNOkec?si=W-h6-lM893uKdTnt

In diesem Video wird erläutert, wie Schwachstellen bei Software- und Hardware-Anbietern von Drittanbietern Gesundheitssysteme anfälliger für Cyberangriffe machen können, was die Patientensicherheit und die Betriebsstabilität gefährden kann.

Wie die Lieferkette das Gesundheitswesen anfällig für Cyberangriffe macht
https://youtu.be/IFBBxNiKysY?si=0UhDHhqvG2LC8DTh

In diesem kurzen Video mit dem Titel „2-Minuten-Übung“ geht es um die jüngsten Verstöße in der Lieferkette und darum, wie diese die Sicherheit der Patienten in Gesundheitssystemen gefährden.

2-Minuten-Übung: Lieferkettenverletzungen und Patientensicherheitsrisiken mit Drex DeFord
https://youtu.be/mi9t_AhLcIQ?si=kheM-OWdkFZG1hyD

5. 3 Relevante Links

Dieser Artikel beschreibt einen Fall, in dem Shields Health Care Group, Eye Care Leaders und MCG Health in Lieferkettenverletzungen verwickelt waren, von denen insgesamt über 4,3 Millionen Menschen betroffen waren. Allein Shields betraf rund 2 Millionen Patienten. Diese Vorfälle zeigen, wie ein einzelner kompromittierter Lieferant die Patientendaten mehrerer Gesundheitsdienstleister gefährden kann.
https://planet9security.com/supply-chain-attacks-in-healthcare-the-case-of-shields-eye-care-leaders-and-mcg-health/?

Der spanische Pharmagroßhändler Alliance Healthcare wurde Opfer eines Cyberangriffs, der seine Website, Abrechnungssysteme und Auftragsabwicklung lahmlegte. Alternative Lieferwege begrenzten die Auswirkungen auf die Patienten, doch die Störung verdeutlichte die Risiken, die mit den Vertriebskanälen für Medikamente verbunden sind.
https://www.scworld.com/news/cyberattack-hits-spanish-pharmaceutical-company-alliance-healthcare?

6. Literaturverzeichnis

ENISA-Bedrohungslandschaft: Gesundheitssektor - CYBIL-Portal. (2023, 5. Juli). Cybil Portal.
https://cybilportal.org/publications/enisa-threat-landscape-health-sector/

Organisation, W. I. P. (2022).Global Innovation Index 2022: Wie sieht die Zukunft des innovationsgetriebenen Wachstums aus?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-Bedrohungslandschaft für Lieferkettenangriffe.
https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%20for%20Supply%20Chain%20Attacks.pdf

Bob Sulli. (2024, 17. Oktober).Die Studie zur Cyber-Unsicherheit im Gesundheitswesen 2024: Kosten und Auswirkungen auf die Patientensicherheit und -versorgung | Ponemon-Sullivan-Datenschutzbericht.
https://ponemonsullivanreport.com/2024/10/the-2024-study-on-cyber-insecurity-in-healthcare-the-cost-and-impact-on-patient-safety-and-care/

Europäischer Datenschutzausschuss (2021).Leitfaden 07/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO.
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

Dieses Projekt wurde mit Unterstützung der Europäischen Kommission kofinanziert. Die Verantwortung für den Inhalt dieser Veröffentlichung [Mitteilung] trägt allein der Verfasser; die Kommission haftet nicht für die weitere Verwendung der darin enthaltenen Informationen.