ATAQUES A LA CADENA DE SUMINISTROS

Co-funded by the European Union

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

Socios

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

Co-funded by the European Union

Este proyecto ha sido cofinanciado con el apoyo de la Comisión Europea. Esta publicación [comunicación] refleja únicamente las opiniones del autor, y la Comisión no puede ser considerada responsable del uso que pueda hacerse de la información contenida en la misma.

Tabla de Contenidos

Co-funded by the European Union

FACTSHEET – ATAQUES A LA CADENA DE SUMINISTROS

1. Definición

Consiste en el ataque hacia los elementos menos seguros en la cadena de suministros de una organización, tales como proveedores externos o proveedores de servicios, con e objetivo de ganar acceso al objetivo principal del ataque1.

Estas características que definen este tipo de amenazas dificultan su detección y afectan a un gran número de personas, ya que una sola brecha puede impactar en múltiples organizaciones.

2. Relevancia general

Debido a la dependencia de los organismos en redes de terceros, los ataques a la cadena de suministros están volviéndose una amenaza cada vez más relevante. Debido a esta conexión, los atacantes pueden dirigirse a un proveedor más pequeño y menos seguro en lugar de intentar infiltrarse en un sistema que sí cuenta con una protección adecuada2.

Todo lo descrito anteriormente dificulta detectar esta clase de brechas ya que, comúnmente, aparenta ser una actualización u operación del sistema legítima. La vulnerabilidad de un único proveedor puede resultar en la exposición de miles de clientes.

Los ataques a la cadena de suministros resultan ser estratégicamente atractivos tanto para grupos patrocinados por estados como para cibercriminales, debido a su capacidad para generar un impacto significativo y amplio. A medida que un número creciente de individuos recurre a servicios en la nube y a plataformas de terceros, se anticipa que la probabilidad y las repercusiones de este tipo de ataques se agraven significativamente3.

3. Importancia en el ámbito de la salud e impacto en la calidad de los cuidados

Un ataque a la cadena de suministro en el sector de la salud no solo conlleva pérdidas financieras o reputacionales, sino que también afecta la seguridad del paciente y la calidad de la atención4. La dependencia de los hospitales en terceros, tales como historiales clínicos electrónicos, sistemas de diagnóstico e imagen y servicios en la nube, plantea un riesgo significativo. En este contexto, una brecha de seguridad podría dar como resultado el acceso no autorizado a información sensible del paciente. Esto podría causar angustia psicológica o fraude financiero contra los pacientes.

Esta situación tiene un impacto significativo en la calidad de la atención. Las fuentes indican que el ransomware, cuando es transmitido a través de una vulnerabilidad en la cadena de suministro, podría ocasionar retrasos en intervenciones quirúrgicas, demoras en la obtención de resultados de laboratorio, entre otros efectos. Estas interrupciones en la atención médica pueden contribuir a un aumento en las tasas de morbilidad y mortalidad en situaciones de emergencia5.

4. ¿Qué puedo hacer como profesional sanitario?

- Informar de cualquier comportamiento inusual del sistema.
- Ser cauteloso con los emails, portales o aplicaciones de proveedores de servicios.
- Seguir los protocolos organizacionales y seguir las restricciones de seguridad.
- Realizar formaciones sobre ciberseguridad y mantenerse al día sobre cómo se manifiestan este tipo de ataques en el trabajo diario.

5. Más información

5.1 Materiales de aprendizaje

- 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 Vídeos Relacionados

Este vídeo aborda los principales retos que enfrenta el sector sanitario en materia de ciberseguridad, destacando la importancia de proteger los datos sensibles de los pacientes y garantizar la continuidad de los servicios médicos.

Ataque Cadena de Suministro / Ciberseguridad
https://youtu.be/oARd-HTfqCA?si=kutJn88xtz1GZ8Kt

5. 3 Enlaces Relevantes

Un ataque paralizó la logística de distribución de suministros médicos en centros de salud de Cataluña, afectando al 80% de los centros de atención primaria del Instituto Catalán de Salud (ICS) y a más de un tercio de los hospitales.
https://bitlifemedia.com/2025/07/ciberataque-paraliza-logistica-sanitario-cataluna/

Este artículo consiste en el informe de INCIBE que destaca ataques a la cadena de suministro como una amenaza relevante, originados por vulnerabilidades no parcheadas o la instalación de malware en la infraestructura tecnológica.
https://www.incibe.es/incibe-cert/blog/ciberseguridad-en-el-sector-salud-caracteristicas-amenazas-y-recomendaciones

6. Bibliografía

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

Este proyecto ha sido cofinanciado con el apoyo de la Comisión Europea. Esta publicación [comunicación] refleja únicamente las opiniones del autor, y la Comisión no puede ser considerada responsable del uso que pueda hacerse de la información contenida en la misma.