ATAQUES DE DENEGACIÓN DE SERVICIO

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 DE DENEGACIÓN DE SERVICIO

1. Definición

Se trata de un acto intencionado que busca provocar la indisponibilidad de un sistema informático, una red o un servicio mediante la generación de un volumen excesivo de tráfico o la solicitud de una cantidad desproporcionada de recursos1. La eficacia se establece mediante el uso de dispositivos vulnerables.

2. Relevancia general

Los ataques DoS pueden bloquear sitios web, plataformas financieras, servicios gubernamentales y más, causando daños reputacionales y económicos. Tanto los mecanismos de defensa como los agentes maliciosos están experimentando un avance en sus capacidades técnicas, lo que da lugar a una dinámica de confrontación que conlleva altos costos asociados a los daños ocasionados por la recuperación tras períodos de inactividad2.

El hecho de que estos ataques se realicen con escasos recursos financieros y un nivel técnico limitado es motivo de preocupación, ya que conllevan repercusiones significativas. La accesibilidad de los medios para llevar a cabo estos ataques hace que se encuentre entre las formas más comunes de agresión cibernética.

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

Los ataques de denegación de servicio (DoS) son especialmente graves en el sector sanitario debido a que afectan a la disponibilidad de los sistemas digitales2. La mayor parte de la información privada de los pacientes, que incluye datos sobre tratamientos y historiales médicos, se encuentra almacenada en plataformas electrónicas. Esta situación conlleva que los ciberataques representen un riesgo significativo para la seguridad y la integridad de la vida de los pacientes. Si los atacantes tienen éxito, pueden interrumpir la programación de citas, retrasar o impedir el acceso a datos críticos de pacientes, o incluso comprometer los sistemas de respuesta de emergencia, lo que podría causar retrasos en el tratamiento y un mayor riesgo clínico3.

Esta clase de ataque tiene un impacto significativo en la calidad de la atención médica. En otros sectores, las consecuencias pueden limitarse a daños financieros; sin embargo, en el ámbito de la salud, esto puede socavar la confianza de los pacientes en los servicios de salud digital e incluso poner en riesgo la vida humana. Por todo ello, la resiliencia digital es un componente fundamental para la ciberseguridad y para el mantenimiento de una atención médica de alta calidad5.

4. ¿Qué puedo hacer como profesional sanitario?

- é puedo hacer como profesional sanitario?
- Estar familiarizado con los procedimientos de tu centro sanitario a la hora de realizar copias de seguridad manuales durante las interrupciones del servicio6.
- Comunicar al equipo de seguridad cualquier tipo de amenaza posible y priorizar el almacenamiento efectivo, esencial de información5.
- Mantener una comunicación fluida y clara con los pacientes para preservar sy confianza en el sistema sanitario.
- Realiza formaciones sobre ciberseguridad y mantente al día sobre cómo responder ante los incidentes.

5. Más información

5.1 Materiales de aprendizaje

- Cibersecurity guide for healthcare sector (EU scope) (JGT-7)
- General training (71 infopacks) about cibersecurity descriptions. Provided by cryptographic National centre. (JGT-10)
- 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)
- Research paper on Cybersecurity and critical care staff: A mixed methods study (PRAMMER-29)
- 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 explica qué es un ataque de denegación de servicio, cómo funciona este tipo de ataque y las medidas que se pueden tomar para protegerse frente a él.

¿Qué son los ataques de denegación de servicio? Así funciona un DoS y cómo protegerse
https://youtu.be/_sVObRVfoms?si=A8sOvKmDKYE51tjx

5. 3 Enlaces Relevantes

Este artículo habla sobre cómo Microsoft ha observado un aumento de ataques DDoS dirigidos a organizaciones sanitarias, con interrupciones que pueden afectar servicios críticos.
https://www.techtarget.com/healthtechsecurity/news/366594390/Healthcare-DDoS-Attacks-Are-Increasing-Microsoft-Says

En julio de 2024, la Guardia Civil detuvo tres personas en Manacor (Mallorca), Huelva y Sevilla por participar en ataques DDoS dirigidos a instituciones públicas, empresas y organismos de España, vinculados al grupo hacktivista NoName057(16).
https://www.rtve.es/noticias/20240720/guardia-civil-detiene-tres-hackers-atacar-instituciones-empresas-espana-otros-paises-ucrania/16192797.shtml

6. Bibliografía

Cloudflare. (s. f.). ¿Qué es un ataque DDoS?
https://www.cloudflare.com/es-es/learning/ddos/what-is-a-ddos-attack/.com

Lella, I., Theocharidou, M., Tsekmezoglou, E., Naydenov, R. S., Ciobanu, C., & Malatras, A. (2022). ENISA Threat Landscape 2022: July 2021 to July 2022. Enisa, 43-49.
https://doi.org/10.2824/764318

Denial of Service (DoS) guidance. (s. f.).
https://www.ncsc.gov.uk/collection/denial-service-dos-guidance-collection

Health. (s. f.). OECD. Recuperado 26 de agosto de 2025, de
https://www.oecd.org/en/topics/chronic-diseases.html

Data privacy and security. (2025). NHS England.
https://digital.nhs.uk/services/networks-and-connectivity-transformation-frontline-capabilities/connectivity-hub/advice-and-guidance/mobile-backup-solutions-for-fixed-healthcare-sites/business-continuity

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.