DENIAL-OF-SERVICE-ANGRIFFE

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 – DENIAL-OF-SERVICE-ANGRIFFE

1. Definition

Es handelt sich um einen böswilligen Versuch, ein Computersystem, Netzwerk oder einen Dienst durch das Senden von zu viel Datenverkehr oder die Anforderung zu vieler Ressourcen unzugänglich zu machen.1. Die Wirksamkeit wird durch die Verwendung anfälliger Geräte bestimmt.

2. Allgemeine Bedeutung

DoS-Angriffe können Websites, Finanzplattformen, Behördendienste und mehr blockieren und so zu Reputations- und finanziellen Schäden führen. Sowohl Abwehrmechanismen als auch böswillige Akteure verbessern ihre technischen Fähigkeiten, was zu einem Tauziehen führt, das aufgrund der Ausfallzeit hohe Schadenskosten verursacht.2.

Die Tatsache, dass diese Angriffe mit geringen finanziellen Mitteln und technischem Know-how durchgeführt werden können, ist besorgniserregend, da sie schwerwiegende Folgen haben. Da die Mittel zur Durchführung solcher Angriffe leicht zugänglich sind, gehören sie zu den am weitesten verbreiteten Formen der Cyber-Aggression.

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

Insbesondere im Gesundheits- und Pflegebereich sind Denial of Service (DoS)-Angriffe kritisch, da sie auf die Verfügbarkeit digitaler Systeme abzielen2Die meisten privaten Patientendaten (Behandlungsdaten, Gesundheitsakten usw.) werden auf elektronischen Plattformen gespeichert, was diese Art von Cyberangriff potenziell lebensbedrohlich machen kann. Sind die Angreifer erfolgreich, können sie die Terminplanung stören, den Zugriff auf kritische Patientendaten verzögern oder verhindern oder sogar Notfallsysteme kompromittieren, was zu Behandlungsverzögerungen und zusätzlichen klinischen Risiken führen kann.3.

Diese Situation hat erhebliche Auswirkungen auf die Qualität der Gesundheitsversorgung. Während sie in anderen Sektoren lediglich finanzielle Schäden verursacht, kann sie im Gesundheitswesen das Vertrauen der Patienten in digitale Gesundheitsdienste untergraben und sogar Menschenleben gefährden. Aus diesen Gründen ist digitale Resilienz ein wesentliches Element sowohl der Cybersicherheit als auch der Aufrechterhaltung einer qualitativ hochwertigen Gesundheitsversorgung.5.

4. Was kann ich als medizinisches Fachpersonal tun?

- Informieren Sie sich darüber, wie Ihr Unternehmen mit Ausfallzeiten umgeht, damit Sie auf manuelle Sicherungsverfahren umsteigen können.6.
- Melden Sie mögliche Bedrohungen sofort dem Sicherheitsteam und legen Sie Wert auf eine effektive Speicherung wichtiger Informationen.5.
- Sorgen Sie für eine klare und reibungslose Kommunikation mit den Patienten, um ihr Vertrauen in das Gesundheitssystem aufrechtzuerhalten.
- Nehmen Sie an Cyber-Schulungen teil und bleiben Sie auf dem Laufenden, wie Sie auf Vorfälle reagieren.

5. Weitere Informationen

5.1 Lernmaterialien

- Leitfaden zur Cybersicherheit im Gesundheitswesen (EU-Geltungsbereich) (JGT-7)
- Allgemeine Schulung (71 Infopakete) zu Cybersicherheitsbeschreibungen. Angeboten vom Nationalen Kryptographiezentrum. (JGT-10)
- Eine Infografik über Sicherheits- und Cybersicherheitsgeräte, die in verschiedenen Gesundheitseinrichtungen eingesetzt werden. (IST-38)
- Ein Überblick über Cybersicherheit im Gesundheitswesen mit Schwerpunkt auf der Rolle von KI und ihrem regulatorischen Rahmen. (IST-39)
- Forschungsarbeit zum Thema Cybersicherheit und Intensivpflegepersonal: Eine Mixed-Methods-Studie (PRAMMER-29)
- 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-14)

5.2 Relevante Videos

Dieses Video erklärt klar und einfach, wie DoS-Angriffe (Denial of Service) funktionieren. Es zeigt, dass ein DoS-Angriff versucht, ein System unzugänglich zu machen, was einen der wichtigsten Aspekte der Cybersicherheit darstellt. Dazu werden so viele Anfragen an Server oder Netzwerke gesendet, bis diese nicht mehr reagieren.

Denial-of-Service-Angriffe erklärt
https://youtu.be/bDAY-oUP0DQ?si=uaHS8A80SwxLOaGc

5. 3 Relevante Links

In diesem Artikel heißt es, dass eine Hacktivistengruppe, vermutlich Anonymous, mehrstufige DDoS-Angriffe auf das Boston Children's Hospital startete. Diese Angriffe hätten die vom ISP des Krankenhauses gemeinsam genutzte Infrastruktur und sieben weitere nahegelegene Gesundheitseinrichtungen beeinträchtigen können. Die Angriffe erreichten Spitzengeschwindigkeiten von 28 Gbit/s und störten die elektronische Rezeptweiterleitung, den E-Mail-Versand der Abteilungen und den Zugriff auf Patientenakten. Das Boston Children's Hospital reagierte mit der Aktivierung seines Incident Response Teams und der Nutzung von DDoS-Abwehrdiensten.
https://www.radware.com/security/ddos-experts-insider/ert-case-studies/boston-childrens-hospital-ddos-mitigation-case-study/?utm_source=chatgpt.com

Eine umfassendere Analyse zeigt laut diesem Artikel, dass DDoS-Angriffe auf das Gesundheitswesen seit 2016 deutlich zugenommen haben. Viele Krankenhäuser reagierten nur langsam auf Angriffe und erfuhren oft erst nach längerer Zeit von ihnen. Dies löste bei den Menschen Besorgnis über die wachsende Bedrohung aus.
https://www.healthcareitnews.com/news/denial-service-attacks-healthcare-poised-explode#:~:text=A%20recent%20Neustar%20report%20found,attacks%20than%20its%20global%20counderparts

6. Literaturverzeichnis

Cloudflare. (s. f.).Was ist ein DDoS-Angriff?
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-Bedrohungslandschaft 2022: Juli 2021 bis Juli 2022.Enisa, 43-49.
https://doi.org/10.2824/764318

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

Gesundheit. (s. f.).OECDAbgerufen am 26. August 2025 von
https://www.oecd.org/en/topics/chronic-diseases.html

Datenschutz und Sicherheit. (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

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.