RANSOMWARE

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 – RANSOMWARE

1. Definition

Es handelt sich um eine Art von Malware, die Dateien verschlüsselt und unzugänglich macht. Um sie wiederherzustellen, verlangen Angreifer ein Lösegeld im Austausch für die Entschlüsselung. Zu den möglichen Aktionen gehören die vollständige Sperrung des Computers, Datendiebstahl, -verschlüsselung oder -löschung oder die Drohung, alle gestohlenen Informationen preiszugeben.1.

2. Allgemeine Bedeutung

Ransomware verursacht schwerwiegende Betriebsstörungen, indem sie unter anderem Ausfallzeiten, finanzielle Verluste, Rufschädigungen und Kundenunzufriedenheit verursacht. Es handelt sich um eine lukrative Cyberkriminalität, die das Leben von Patienten gefährdet. Darüber hinaus sind die globalen Kosten von Ransomware enorm und können kritische Abläufe in der Fertigung, Lieferketten, Energieversorgung oder im öffentlichen Dienst lahmlegen.

Angreifer haben ihre Methoden durch doppelte und dreifache Erpressung verbessert: Sie verschlüsseln nicht nur Daten, sondern drohen auch damit, diese zu veröffentlichen oder Partner anzugreifen3.

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

Das Gesundheitswesen ist für Patientenakten, Diagnostik und Behandlungen größtenteils auf digitale Systeme angewiesen. Ransomware kann Gesundheitsplattformen lahmlegen und zu tragischen Folgen wie einer Zunahme von Notfällen führen.2(einschließlich Schlaganfällen und Herzstillständen), Verzögerungen bei Laborergebnissen und ausgesetzten Diagnosen und Behandlungen.

Quellen wie Microsoft4nennen die folgenden Folgen von Ransomware-Angriffen, die in vier Krankenhäusern stattfanden, zwei davon wurden angegriffen, zwei waren nicht angegriffen:

1. Anstieg der Schlaganfallfälle.
2. Zunahme von Herzstillständen.
3. Verringerte Überlebensrate bei günstigen neurologischen Ergebnissen.
4. Zunahme der Ankunft von Krankenwagen.
5. Die Patientenzahl steigt stark an.
6. Zusätzliche Störungen in der Pflege,

Dies wirkt sich direkt auf die Qualität der Versorgung aus. Behandlungsabsagen und eingeschränkter Zugriff auf wichtige Patientendaten sind nur einige Beispiele. Manuelle, papierbasierte Arbeitsabläufe sind zudem fehleranfällig, weniger sicher und erhöhen den Stress des Personals.5.

Tatsächliche Vorfälle zeigen, dass Ransomware die Sterblichkeitsrate in Krankenhäusern in betroffenen Gebieten erhöhen kann6

4. Was kann ich als medizinisches Fachpersonal tun?

- Ergreifen Sie vorbeugende Maßnahmen, z. B. die Verwendung sicherer Passwörter, die Aktualisierung der Software, die Aktivierung der Zwei-Faktor-Authentifizierung usw.
- Vermeiden Sie die Weitergabe von Anmeldedaten auf ungesicherten Geräten und seien Sie vorsichtig, wenn Sie vertrauliche Informationen zwischen Kollegen austauschen.
- Achten Sie auf Cyberbedrohungen (Phishing-E-Mails, verdächtige Links) und melden Sie Unregelmäßigkeiten sofort.
- Nehmen Sie an Cyber-Schulungen teil und bleiben Sie auf dem Laufenden, wie Sie auf Vorfälle reagieren.

5. Weitere Informationen

5.1 Lernmaterialien

- Cybersicherheit für Ihre Branche (JGT-1)
- Aufeinanderfolgende Videos zu allgemeinen Themen der Cybersicherheit (JGT-2)
- Webseminare zu wichtigen Aspekten der Cybersicherheit (JGT-3)
- Leitfaden zur Cybersicherheit im Gesundheitswesen (EU-Geltungsbereich) (JGT-7)
- Interaktive Lernumgebung zur Entwicklung von Cybersicherheitskompetenzen. Erfordert einen nationalen Ausweis (JGT-9).
- Allgemeine Schulung (71 Infopakete) zu Cybersicherheitsbeschreibungen. Angeboten vom Nationalen Kryptographiezentrum. (JGT-10)
- Ein Überblick über Cybersicherheit im Gesundheitswesen mit Schwerpunkt auf der Rolle von KI und ihrem regulatorischen Rahmen. (IST-39)
- Bildungsprojekt zur sicheren und verantwortungsvollen digitalen Nutzung. (IST-41)
- 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)

5.2 Relevante Videos

In diesem Video wird erklärt, was Ransomware-Angriffe sind, wie sie beginnen, welche Auswirkungen sie auf Unternehmen haben, wie viel sie kosten, welche Branchen am stärksten gefährdet sind und welche Schritte unternommen werden können, um sie zu vermeiden.

So sieht ein echter Ransomware-Angriff aus
https://youtu.be/jl8K0VJraX4?si=XQBMPv4PAOAWwpVB

Das nächste Video zeigt uns konkrete Möglichkeiten, wie sich Menschen vor Ransomware schützen können.

Schützen Sie sich vor Ransomware
https://youtu.be/eizn9TC68E8?si=iMeXQ_AZAs0_lFzb

5. 3 Relevante Links

Dieser Artikel beschreibt einen realen Fall, bei dem ein Ransomware-Angriff St. Margaret's Health, ein kleines, ländliches Gesundheitssystem in Illinois, in eine finanzielle Abwärtsspirale stürzte. Der Angriff machte es dem 44-Betten-Krankenhaus in Spring Valley unmöglich, sich nach wochenlangem Ausfall zu erholen, sodass es endgültig geschlossen werden musste.
https://www.hipaajournal.com/ransomware-attack-key-factor-in-decision-to-close-rural-illinois-hospital/

Dem Artikel zufolge meldete UC San Diego Health einen Phishing-Angriff, der zwischen dem 9. und 22. Januar 2024 stattfand. Bei diesem Angriff wurden die E-Mail-Konten zweier Mitarbeiter kompromittiert, wodurch sensible Patientendaten von 1.642 Personen gefährdet wurden.
https://www.hipaajournal.com/march-13-2023-healthcare-data-breaches/

Der Artikel beschreibt, wie ein Ransomware-Angriff auf Ascension Health im Mai 2024 den Betrieb im gesamten Krankenhausnetzwerk durcheinanderbrachte. Er führte zur manuellen Patientenaktenführung, zu Umleitungen von Krankenwagen und zu Verzögerungen bei der Behandlung. Am Ende waren rund 5,6 Millionen Patientenakten kompromittiert.
https://www.hipaajournal.com/ascension-cyberattack-2024/#:~:text=The%20May%202024%20ransomware%20attack,paper%20to%20record%20patient%20information.

Der Ransomware-Angriff auf Change Healthcare zeigt, wie schwach das US-Gesundheitssystem insgesamt ist. Er verursachte enorme finanzielle Verluste, erschwerte den Leistungserbringern die Arbeit und verdeutlichte, wie dringend die Cyber-Resilienz des gesamten Sektors verbessert werden muss.
https://www.csoonline.com/article/3484304/the-cyber-assault-on-healthcare-what-the-change-healthcare-breach-reveals.html

6. Literaturverzeichnis

Nationales Zentrum für Cybersicherheit. (s. f.).Ein Leitfaden zu Ransomware. https://www.ncsc.gov.uk/ransomware/home

Reed, J. (2025, 31. März). Wenn Ransomware Angriffe auf Gesundheitseinrichtungen vereitelt.IBM. https://www.ibm.com/think/insights/when-ransomware-kills-attacks-on-healthcare-facilities?utm_source=chatgpt.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

US-Gesundheitswesen in Gefahr: Stärkung der Widerstandsfähigkeit gegen Ransomware-Angriffe. (o.D.). Microsoft-Sicherheit. Abgerufen am 1. August 2025 von https://www.microsoft.com/en-us/security/security-insider/threat-landscape/us-healthcare-at-risk-strengthening-resiliency-against-ransomware-attacks?utm_source=chatgpt.com

Burgess, M. (2024, 24. Juni). Bürokratie verschlimmert Ransomware-Angriffe auf Krankenhäuser.VERDRAHTET. https://www.wired.com/story/ransomware-health-care-assurance-letters/?utm_source=chatgp.com

Freed, A. M. (27. Februar 2025). Die wichtigsten Faktoren, die den Gesundheitssektor durch Ransomware-Angriffe gefährden.Halcyon. https://www.halcyon.ai/blog/top-factors-that-put-healthcare-sector-at-risk-from-ransomware-attacks?utm_source=chatgpt.com

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.