CYBER-RESILIENZ

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 – CYBER-RESILIENZ

1. Definition

Es ist eine OrganisationFähigkeit, sich auf Cyber-Bedrohungen vorzubereiten, darauf zu reagieren und sich davon zu erholen, während gleichzeitig die Patientenversorgung und die Betriebskontinuität aufrechterhalten werden. Der Schwerpunkt liegt auf der Minimierung von Störungen durch Cyberangriffe und der Gewährleistung der Sicherheit sensibler Daten1.

Dieses Konzept kombiniert Geschäftskontinuität, Informationssystemsicherheit und organisatorische Belastbarkeit.Es beschreibt die Fähigkeit, trotz herausfordernder Cyber-Ereignisse weiterhin die beabsichtigten Ergebnisse zu erzielen.2.

2. Allgemeine Bedeutung

Cyber-Resilienz ist aufgrund der digitalen Abhängigkeit in allen Sektoren relevant. Heutzutage verlassen sich Regierungen, Unternehmen und Einzelpersonen auf digitale Systeme für Betrieb, Kommunikation und Datenspeicherung. Diese Abhängigkeit von der Technologie hat zahlreiche Vorteile, wie z. B. schnellen Zugriff auf Informationen, verbesserte Koordination der Gesundheitsversorgung und Ressourcenoptimierung. Allerdings hat sie auch zu einem Anstieg von Cyber-Bedrohungen und -Angriffen in Umfang und Komplexität geführt, sodass die Prävention von Cybersicherheit zu einem vorrangigen Thema geworden ist.

Ein weiterer Faktor, der Cyber-Resilienz zu einem wichtigen Thema macht, das global behandelt werden sollte, ist das Verständnis, dass Sicherheitsverletzungen unvermeidlich sind, und der Fokus darauf, wie man sich nach Vorfällen anpasst, sich davon erholt und erfolgreich ist, nicht nur, sie zu verhindern.3.

Hier sind einige der Vorteile der Cyber-Resilienz3:

- **Geschäftskontinuität:**Stellt sicher, dass kritische Geschäftsabläufe während aktiver Cyber-Vorfälle aufrechterhalten werden können, und reduziert Betriebsunterbrechungen erheblich, selbst wenn herkömmliche Abwehrmaßnahmen beeinträchtigt sind.
- Reduzierte Ausfallzeiten:Reduziert den Zeit- und Ressourcenverlust bei längeren Ausfällen, indem Unternehmen sich schnell von Angriffen und Vorfällen erholen können.

- **Finanzieller Schutz**: Reduziert die Kosten, die mit Systemausfällen, Datenschutzverletzungen und möglichen rechtlichen Konsequenzen verbunden sind, die typischerweise auf erhebliche Sicherheitsvorfälle folgen.
- **Reputationsmanagement**: Es baut das Vertrauen der Stakeholder auf und erhält es aufrecht, indem es die Zuverlässigkeit und Fähigkeit der Organisation demonstriert, unerwartete Sicherheitsherausforderungen zu bewältigen.
- **Einhaltung gesetzlicher Vorschriften**: Garantiert, dass die Unternehmenspraktiken den strengsten Gesetzen entsprechen. Das gerade eingeführte Cyber Resilience unterstreicht die zunehmende regulatorische Aufmerksamkeit, die diesem Thema gewidmet wird.
- **Vorteile auf dem Markt**: Durch die Demonstration strenger Sicherheitsverfahren, die das Unternehmen von weniger vorbereiteten Konkurrenten abheben, zieht es sicherheitsbewusste Kunden und Partner an. unvorbereitete Konkurrenten.

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

Das moderne Gesundheitswesen basiert auf eng verknüpften Systemen. Aufgrund der enormen Menge sensibler Patientendaten und der kritischen Bedeutung seiner Abläufe ist die Gesundheitsbranche zum Hauptziel von Cyberkriminellen geworden.4.

Um umfangreiche Serviceunterbrechungen zu vermeiden, ist Resilienz entscheidend. Denn der Ausfall einer Komponente kann sich auf die gesamte Versorgungsinfrastruktur auswirken. Lebensgefahr besteht, wenn lebenswichtige Gesundheitssysteme wie elektronische Patientenakten oder medizinische Geräte ausfallen. Um die Sicherheit und Privatsphäre der Patienten zu schützen, sorgt Cyber-Resilienz dafür, dass die Patientenversorgung auch bei Angriffen aufrechterhalten bleibt.

Darüber hinaus hängt die Wahrung des Vertrauens von Partnern, Patienten und der Öffentlichkeit von der Cyber-Resilienz ab. Da Patientendaten äußerst sensible Informationen enthalten, können Störungen oder Beeinträchtigungen dieser Daten dem Ruf von Gesundheitsorganisationen schaden.

4. Was kann ich als medizinisches Fachpersonal tun?

- Sorgen Sie für eine gute Cyber-Hygiene. Mit Maßnahmen wie der Verwendung sicherer Passwörter, der Aktivierung der Zwei-Faktor-Authentifizierung und der ständigen Aktualisierung der Software.
- Schützen Sie Patientendaten. Indem Sie verdächtige Aktivitäten umgehend melden und bei Ihren täglichen Aufgaben sorgfältig mit Informationen umgehen.
- Nehmen Sie an einem Cyber-Training teil.Durch die Teilnahme an Kursen, die sich mit Techniken zur Prävention, Erkennung und Reaktion auf Datenschutzverletzungen befassen.

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)
- Sensibilisierungspaket zur Cybersicherheit in Unternehmen (JGT-4)
- Online-Workshop zur Einrichtung unseres Geräts. (JGT-5)
- Cybersicherheit für KMU und Selbstständige (JGT-6)
- Leitfaden zur Cybersicherheit im Gesundheitswesen (EU-Geltungsbereich) (JGT-7)
- Schulung zur Cybersicherheit durch das Nationale Kryptographiezentrum Spaniens. Nationaler Login erforderlich (JGT-8).
- Allgemeine Schulung (71 Infopakete) zu Cybersicherheitsbeschreibungen. Angeboten vom Nationalen Kryptographiezentrum. (JGT-10)
- Ein Artikel, der den aktuellen Stand der Cybersicherheit im Gesundheitswesen untersucht. (IST-36)
- Ein Artikel über Sicherheitsstrategien für elektronische Patientenakten (IST-37)
- 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)
- Ein Kompendium zur Verarbeitung von Patientendaten auf Online-Plattformen. (IST-40)
- Bildungsprojekt zur sicheren und verantwortungsvollen digitalen Nutzung. (IST-41)
- Regulierung der Cybersicherheit im Gesundheitswesen (BBS-23)
- Cybersicherheit von Krankenhäusern und Gesundheitsdienstleistern (BBS-24)
- Digitale Identitäten – Sicherheit im Fokus (BBS-25)
- Forschungsarbeit zum Thema Cybersicherheit und Intensivpflegepersonal: Eine Mixed-Methods-Studie (PRAMMER-29)
- Eine kritische Überprüfung von Rahmenwerken und Schulungsmodellen zur Sensibilisierung für Cybersicherheit (PRAMMER-30)
- Eine integrierte Strategie zur Sensibilisierung für Cybersicherheit zur Beurteilung von Einstellungen und Verhaltensweisen im Bereich Cybersicherheit im schulischen Kontext (PRAMMER-31)
- Cyberangriffe stellen eine permanente und erhebliche Bedrohung für Gesundheitssysteme dar: Die Ausbildung muss dies widerspiegeln (PRAMMER-32).
- 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)
- Systematische Anwendung von Gamification in Schulungen zur Sensibilisierung für Cybersicherheit: Ein Rahmenkonzept und eine Fallstudienanalyse (PRAMMER-35)
- Videotraining für Fachleute und Studierende (FIRDA-13)
- Videotraining für Fachleute und Studierende (FIRDA-14)
- Digitales Training in Cybersicherheit, unterhaltsame und schnelle Fragen (FIRDA-15)
- Kostenlose Kurse zur Verbesserung der digitalen Kompetenzen von Mitarbeitern im Gesundheitswesen (FIRDA-18)
- Online-Lektion zum Thema Cybersicherheit (FIRDA-20)

5.2 Relevante Videos

Dieses Video befasst sich mit der Herausforderung, Cyber-Resilienz im Gesundheitswesen zu erreichen, und diskutiert den ständigen Wandel der digitalen Gesundheitslandschaft. Es betont außerdem die Bedeutung des Aufbaus starker Cybersicherheitsmaßnahmen, die sich in Echtzeit anpassen und wiederherstellen können.

Was ist nötig, um im Gesundheitswesen echte Cyber-Resilienz aufzubauen?
https://youtu.be/BNsD1jKZ8Es?si=wcFCbn65VHv3aLzH

Das nächste Video befasst sich mit dem Aufbau von Cyber-Resilienz im Gesundheitswesen. Es bietet praktische Ratschläge zur Integration und Stärkung der Datensicherheit klinischer Systeme in einer sich schnell entwickelnden digitalen Gesundheitslandschaft. Der Vorschlag besteht darin, Sicherheitsmaßnahmen in den Gesundheitsbetrieb zu integrieren, um sicherzustellen, dass die Systeme gegenüber ständigen Bedrohungen widerstandsfähig bleiben.

Wie man Cyber-Resilienz im Gesundheitswesen aufbaut | HealthSec 2025 Keynote
https://youtu.be/U7LIBdQi78k?si=aKhDfOr3aMyzQB32

5. 3 Relevante Links

Dieser Artikel betont, wie Untätigkeit und Unterinvestitionen in die IT-Resilienz angesichts der wachsenden Bedrohung durch Cyberangriffe und technische Ausfälle im Gesundheitswesen die Patientenversorgung, die Betriebskontinuität und die Sicherheit ernsthaft beeinträchtigen.
https://www.mckinsey.com/industries/healthcare/our-insights/tech-resilience-for-healthcare-providers-inaction-has-a-heavy-toll?utm_source=chatgpt.com

Um die Kontinuität der Patientenversorgung auch im Falle von Cyberangriffen zu gewährleisten, betont der Artikel, wie wichtig es ist, dass Gesundheitsorganisationen der Cyber-Resilienz Priorität einräumen. Dies kann erreicht werden, indem man über Prävention hinausgeht und durch koordinierte Wiederherstellungsplanung und eine starke Infrastruktur auf die Bereitschaft vorbereitet.
https://www.rubrik.com/blog/company/25/7/cyber-resilience-in-healthcare-preparing-for-the-inevitable-attack?utm_source=chatgpt.com

Im Mai 2021 wurde der irische Gesundheitsdienst HSE Opfer eines verheerenden Conti-Ransomware-Angriffs, der die IT-Systeme des Landes lahmlegte. Dadurch wurden Gesundheitsdienste lahmgelegt, sensible Daten offengelegt und eine langwierige Wiederherstellung mit einem Notruf und einer gründlichen Überprüfung nach dem Vorfall erforderlich.“
https://en.wikipedia.org/wiki/Health_Service_Executive_ransomware_attack?utm_source=chatgpt.com

6. Literaturverzeichnis

Susnjara, S., & Smalley, I. (13. August 2025). Cyber-Resilienz.IBMAbgerufen am 18. August 2025 von https://www.ibm.com/think/topics/cyber-resilience

Tashi, K., & Beato, F. (1. Februar 2024). Das Gesundheitswesen zahlt von allen Sektoren den höchsten Preis für Cyberangriffe – deshalb ist Cyber-Resilienz von entscheidender Bedeutung.Weltwirtschaftsforum.Abgerufen am 18. August 2025 von https://www.weforum.org/stories/2024/02/healthcare-pays-the-highest-price-of-any-sector-for-cyberattacks-that-why-cyber-resilience-is-key/?utm_source=chatgpt.com

Was ist Cyber-Resilienz und warum ist sie wichtig? | Fortinet. (s. f.). Fortinet. https://www.fortinet.com/resources/cyberglossary/cyber-resilience?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.