CYBER-HYGIENE

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-HYGIENE

1. Definition

Bezieht sich auf die einfachen Praktiken und Schritte, die wir alle ergreifen können, um unsere persönlichen Daten und Geräte vor Cyber-Bedrohungen zu schützen. Dazu gehören beispielsweise die Zwei-Faktor-Authentifizierung, die Verwendung sicherer Passwörter, regelmäßige Software-Updates usw.1.

2. Allgemeine Bedeutung

Die meisten Sicherheitsverletzungen sind direkt darauf zurückzuführen, dass böswillige Akteure Lücken ausnutzen, die in den aktuellen Cyber-Hygiene-Praktiken des Unternehmens übersehen wurden. Cyber-Hygiene schützt Ihre Computer, Netzwerke und Daten vor allen möglichen Cybersicherheitsrisiken, einschließlich Malware, Ransomware und anderen Angriffen.2.

Wartung ist entscheidend, da ordnungsgemäß betriebene Systeme effizienter sind. Mangelnde Wartung führt zu Fragmentierung, veralteten Programmen und in der Folge zu Sicherheitslücken. Cyberhygiene verhindert Datenschutzverletzungen und Identitätsdiebstahl und reduziert finanzielle, Reputations- und Betriebsrisiken.1.

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

Cyberhygiene ist im Gesundheitswesen aufgrund der Sensibilität von Patientendaten und der Abhängigkeit von digitalen Systemen für Diagnose, Behandlung und Kommunikation von großer Bedeutung. Genau wie die grundlegende Hygiene in der klinischen Versorgung verhindert Cyberhygiene Cybervorfälle. Daher können Sicherheitsverletzungen zu Ransomware-Angriffen führen, die den Krankenhausbetrieb lahmlegen, private Informationen preisgeben oder die Patientensicherheit gefährden können, wenn medizinische Geräte kompromittiert werden.3.

Die Auswirkungen auf die Qualität der Versorgung führen auch zu einem Vertrauensverlust in Gesundheitseinrichtungen. Dies kann Patienten davon abhalten, wichtige Informationen für ihre Behandlung weiterzugeben. Aus diesen Gründen gewährleistet eine gute Cyberhygiene nicht nur die Qualität der Versorgung, sondern gewährleistet auch die Patientensicherheit und das Vertrauen der Öffentlichkeit.

4. Was kann ich als medizinisches Fachpersonal tun?

- Nutzen Sie vorbeugende Maßnahmen wie sichere Passwörter und aktivieren Sie die Zwei-Faktor-Authentifizierung.
- Aktualisieren Sie Software, Apps und medizinische Geräte regelmäßig.
- Achten Sie auf Cyberbedrohungen (Phishing-E-Mails, verdächtige Links) und melden Sie Unregelmäßigkeiten sofort.
- Nehmen Sie an Schulungen zur Cybersicherheit teil und bleiben Sie auf dem Laufenden, wie Sie auf Vorfälle reagieren und welche Auswirkungen der Schutz von Patientendaten hat.

5. Weitere Informationen

5.1 Lernmaterialien

- Cybersicherheit für Ihre Branche (JGT-1)
- Webseminare zu wichtigen Aspekten der Cybersicherheit (JGT-3)
- Sensibilisierungspaket zur Cybersicherheit in Unternehmen (JGT-4)
- 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 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)
- IT-Sicherheitsanforderungen und Schutzmaßnahmen – Tipps und praktische Beispiele (BBS-42)
- Eine integrierte Strategie zur Sensibilisierung für Cybersicherheit zur Beurteilung von Einstellungen und Verhaltensweisen im Bereich Cybersicherheit im schulischen Kontext (PRAMMER-31)
- 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)
- 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 betont die Bedeutung der Einhaltung grundlegender Sicherheitspraktiken wie regelmäßiger Software-Updates, sicherer Passwörter und regelmäßiger Systeminspektionen als primäre Maßnahme zum Schutz von Informationen.

Was ist Cyberhygiene?
https://youtu.be/J_jjl0iTl4I?si=P8wY4Fy7-mWSVWnI

Das folgende Video erklärt verschiedene Arten von Cyberangriffen und erörtert wirksame Strategien zur Cyberhygiene-Prävention.

Grundlagen der Cybersicherheit im Gesundheitswesen
https://youtu.be/IqhGqZTiLsk?si=oI7UOkMn1qFvIUq7

5. 3 Relevante Links

Eine Studie mit 1.454 Ransomware-Vorfällen (2016–2023) zeigte, dass Organisationen mit unzureichender Cyberhygiene (D oder F) 35-mal häufiger Opfer von Angriffen mit Schadensfolge wurden. Dies zeigt, wie wichtig exzellente Hygienepraktiken sind.
Das folgende Video erklärt verschiedene Arten von Cyberangriffen und erörtert wirksame Strategien zur Cyberhygiene-Prävention.

Eine starke Cyberhygiene, wie regelmäßige Updates und Zugriffskontrollen, ist für den Schutz der Patientendaten und die Gewährleistung kontinuierlicher Pflegeleistungen unerlässlich, ähnlich wie die klinische Händehygiene.
https://www.cambridgehealth.edu/healthcare-cybersecurity-privacy/healthcare-cybersecurity-privacy-information/cyber-hygiene-the-health-of-healthcare-systems-starts-with-you/

Umfragen zufolge erhöhen die Verwendung schwacher Passwörter, die Umgehung von Sicherheitsvorschriften und das Fehlen einer sicheren Geräteverwaltung (wie etwa BYOD-Richtlinien) das Risiko von Cyberangriffen erheblich. Tatsächlich stellen viele Arbeitnehmer Bequemlichkeit vor Sicherheit.
https://www.techtarget.com/healthtechsecurity/news/366594401/Employee-Cyber-Hygiene-Is-Critical-to-Healthcare-Cybersecurity

Experten plädieren dafür, Cyberhygiene in die Ausbildung von Krankenpflegern und im Gesundheitswesen zu integrieren, da sie erkennen, dass gut ausgebildete Mitarbeiter die erste Verteidigungslinie gegen Sicherheitsverletzungen darstellen, die die Patientenversorgung gefährden können.
https://pubmed.ncbi.nlm.nih.gov/37595324/

6. Literaturverzeichnis

Cyber-Hygiene | ENISA. (18. Januar 2018). https://www.enisa.europa.eu/topics/cyber-hygiene

Was ist Cyberhygiene? Definition und Best Practices. (21. März 2025). SecurityScorecard. https://securityscorecard.com/blog/what-is-cyber-hygiene-definition-benefits-best-practices/

Weltgesundheitsorganisation. (2025, 26. März).WHO/Europa veröffentlicht Leitfaden zur Stärkung der Cybersicherheit im digitalen Gesundheitswesen. https://securityscorecard.com/blog/what-is-cyber-hygiene-definition-benefits-best-practices/

Co-funded by the European Union

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.