Eine Übersicht und Leitfaden

Cyber-Bedrohungen im europäischen Gesundheitswesen:

Schutz vor Phishing und Betrug durch Awareness-Training

Zusammenfassung

Gesundheitssysteme in der DACH-Region (Deutschland, Österreich, Schweiz) sind mit einer Zunahme von Cyberangriffen konfrontiert, wobei Phishing und Social Engineering zu den häufigsten und gefährlichsten Bedrohungen zählen. Da medizinische Organisationen zunehmend sensible Patientendienste und -daten digitalisieren, nutzen Cyberkriminelle zunehmend menschliches Versagen als schwächstes Glied in der Sicherheitskette aus.

Insbesondere Phishing-Angriffe umgehen weiterhin technische Abwehrmechanismen und zielen mit ausgeklügelten, mehrsprachigen Täuschungsversuchen auf Mitarbeitende im Gesundheitswesen. Trotz erhöhter Investitionen in Cybersicherheits-Produkte werden die meisten Datenschutzverletzungen im Gesundheitswesen immer noch durch Mitarbeitende verursacht, die auf bösartige Links klicken oder unabsichtlich Zugangsdaten preisgeben. [1][2].

Awareness-Trainings haben sich als eine der wirksamsten und skalierbarsten Maßnahmen zur Risikominderung erwiesen. Programme, die rollenbasierte Schulungen, realitätsnahe Phishing-Simulationen und verhaltensorientierte Module enthalten, können die Erfolgsquote von Phishing-Angriffen um bis zu 70 % senken. Angesichts des strengen regulatorischen Umfelds (z. B. DSGVO, nationale Datenschutzgesetze) und der hohen Kosten von Cybervorfällen müssen Führungskräfte im Gesundheitswesen den menschlichen Faktor in der Cybersicherheit priorisieren. [3].

Strukturierte, kontinuierliche Schulungen – angepasst an lokale Sprachen und Rollen im Gesundheitswesen – bieten eine unmittelbare Möglichkeit, Risiken zu senken, regulatorischen Anforderungen gerecht zu werden sowie die Resilienz der Organisation zu stärken.

Anbieter im Gesundheitswesen der DACH-Region sollten eine kontinuierliche, lokal angepasste Sicherheitsbewusstseins-Strategie als zentralen Pfeiler ihres Cyber-Risikomanagements etablieren.

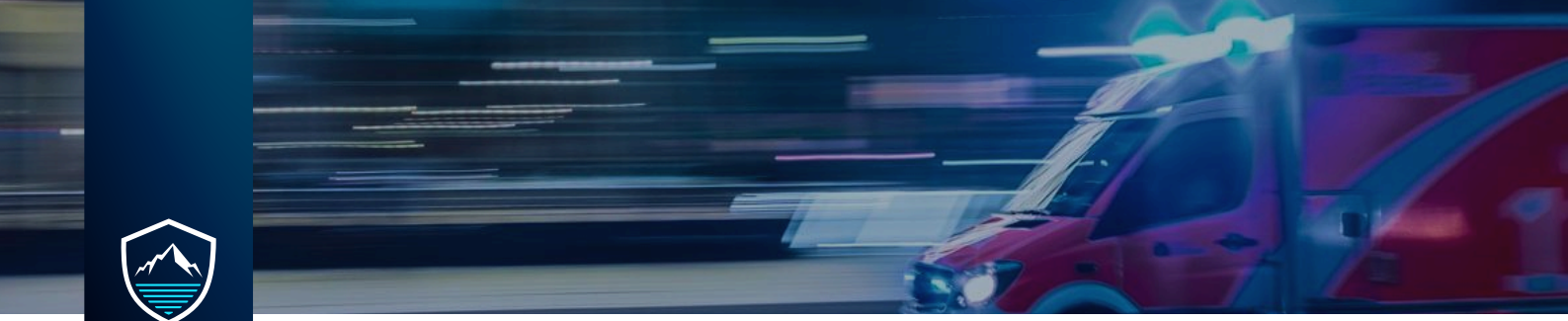
Schulen Sie Ihre Mitarbeiter. Stärken Sie Ihre Frontlinie.

Krankenhaus in Gefahr

Menschliches Versagen als Sicherheitslücke

Schulungen verringern Phishing-Erfolg

1. **ENISA-Bedrohungslandschaft für das Gesundheitswesen, 2023** – https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-healthcare-sector
2. **BSI „Die Lage der IT-Sicherheit in Deutschland 2023“** – https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.pdf
3. **Lucy Security Benchmarking Report, 2024** – https://lucysecurity.com (interne Kundenleistungsdaten)



Einleitung:

Das Gesundheitswesen als Hochwert- und Hochrisikosektor

Gesundheitseinrichtungen in der DACH-Region nehmen eine besonders gefährdete Stellung im Bereich der Cybersicherheit ein. Krankenhäuser, Kliniken, Versicherer und Dienstleister verwalten große Mengen hochsensibler Daten – von elektronischen Patientenakten (ePA), Versicherungsnummern bis hin zu Studiendaten und Medikationshistorien. Dies macht sie zu attraktiven Zielen für Cyberkriminelle, die finanzielle Gewinne erzielen, Identitäten stehlen oder Zugriff auf kritische Infrastruktur für weiterreichende Angriffe erlangen wollen.

Gleichzeitig befindet sich der Sektor in einem rasanten digitalen Wandel. In Deutschland etwa treibt das Krankenhauszukunftsgesetz (KHZG) die Modernisierung klinischer IT-Systeme mit über 4,3 Milliarden Euro an Fördermitteln voran. Auch Österreich und die Schweiz folgen diesem Trend – mit wachsender Nutzung von Telemedizin, cloudbasierten Plattformen und elektronischer Dokumentation.

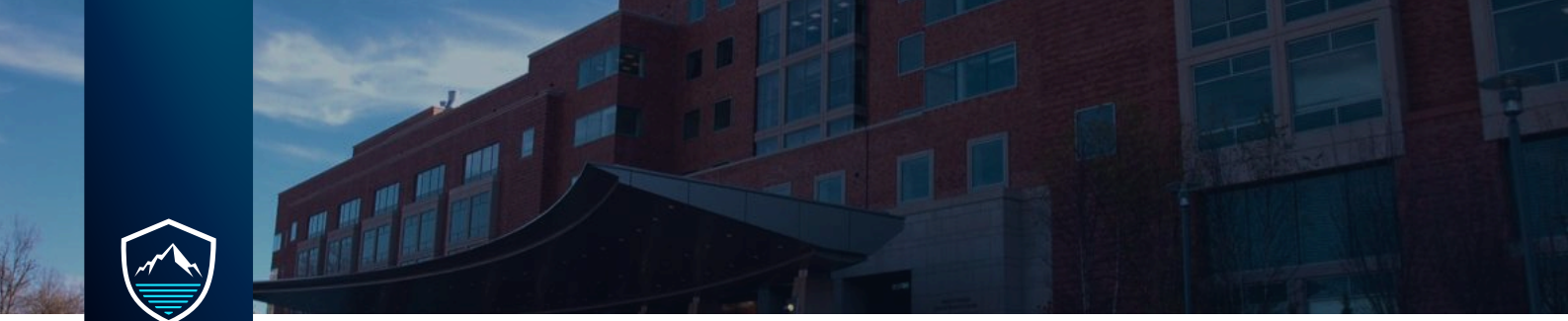
Allerdings schreitet diese Digitalisierung häufig schneller voran als die Umsetzung robuster Cybersicherheitsmaßnahmen. Viele Einrichtungen im Gesundheitswesen arbeiten noch mit veralteten Systemen, überholter E-Mail-Infrastruktur und unzureichend ausgestattetem IT-Personal. Da E-Mail weiterhin das dominierende Kommunikationsmittel im klinischen Alltag ist, steigt das Risiko erfolgreicher Phishing-Angriffe.

Ein entscheidender, oft unterschätzter Risikofaktor ist Zeitdruck. Medizinisches Fachpersonal arbeitet in stressreichen, hektischen Umgebungen, in denen schnelle Reaktionen unerlässlich sind. Ärztinnen und Ärzte lesen E-Mails zwischen Patiententerminen oder während ihrer Schicht – perfekte Bedingungen für unüberlegte Klicks und unzureichende Prüfung verdächtiger Inhalte. Angreifer nutzen diese Hektik aus, indem sie Phishing-Nachrichten gestalten, die wie interne Mitteilungen, Laborergebnisse oder dringende Verwaltungsanfragen erscheinen.

Zusätzlich müssen Gesundheitsdienstleister komplexe rechtliche Rahmenbedingungen einhalten, darunter die Datenschutz-Grundverordnung (DSGVO) der EU sowie nationale Gesetze wie das deutsche Bundesdatenschutzgesetz (BDSG), das österreichische Datenschutzgesetz und das revidierte Datenschutzgesetz der Schweiz (revDSG). Diese verlangen nicht nur technische Schutzmaßnahmen, sondern auch nachweisliche Schritte zur Schulung und Absicherung des Personals.

In einem Umfeld, das durch sensible Daten und hohen Druck gekennzeichnet ist, erweist sich Awarness-Trainings als strategische Notwendigkeit – nicht bloß als eine Pflicht zur Einhaltung von Vorschriften.

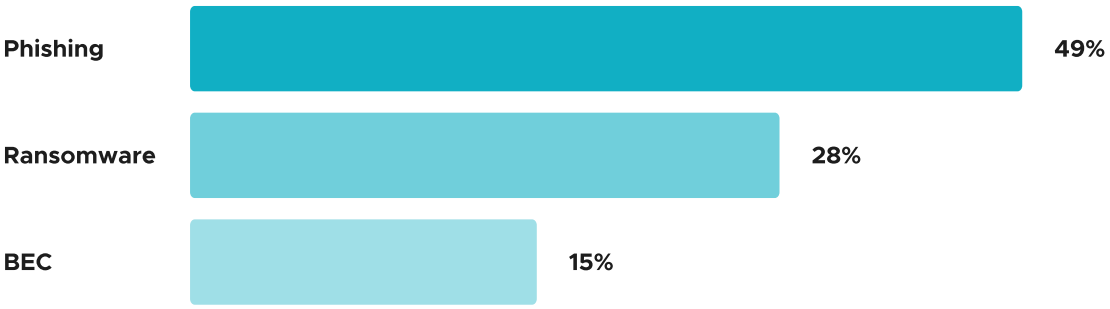
1. **ENISA-Bedrohungslandschaft für das Gesundheitswesen, 2023** – https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-healthcare-sector
2. **Bundesministerium für Gesundheit – Krankenhauszukunftsgesetz (KHZG)** – Krankenhauszukunftsgesetz (KHZG) – https://www.bundesgesundheitsministerium.de/krankenhauszukunftsgesetz
3. **BSI-Jahresbericht 2023** – https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.pdf
4. **Ponemon Institute: Die Auswirkungen von Cyber-Unsicherheit auf die Gesundheitsversorgung , 2022** – https://www.proofpoint.com/sites/default/files/pfpt-us-tr-report-ponemon-impact-cyber-insecurity-healthcare.pdf



Bedrohungslage im Gesundheitswesen der DACH-Region

Gesundheitsdienstleister in Deutschland, Österreich und der Schweiz sehen sich einer zunehmend feindlichen Cyber-Bedrohungslage ausgesetzt. Öffentliche wie private medizinische Einrichtungen, Versicherer und Anbieter von Gesundheits-IT werden nicht nur aus finanziellen Gründen angegriffen, sondern auch aufgrund ihrer systemrelevanten Rolle in der nationalen Infrastruktur. In den letzten Jahren haben Cyberangriffe in Frequenz und Raffinesse deutlich zugenommen – mit Phishing und Ransomware als führenden Bedrohungen. [1].

Häufigste Angriffsarten im Gesundheitswesen



1. **Phishing & Credentials -Klau:**
   E-Mail-basierte Angriffe sind der häufigste Einstiegspunkt. Medizinisches- und Verwaltungsersonal wird oft mit gefälschten E-Mails angegriffen, die sich als Labore, Personalabteilungen, Versicherer oder interne IT ausgeben. Viele dieser Köder sind in lokalen Sprachen (Deutsch, Französisch, Italienisch) verfasst und somit besonders überzeugend.

2. **RansomwareAngriffe:**
   Krankenhäuser und Kliniken sind besonders stark von Ransomware-Angriffen betroffen. Die Angreifer nutzen Sicherheitslücken oder gestohlene Zugangsdaten um Schadsoftware zu installieren, die kritische Daten verschlüsseln um Lösegeld zu fordern. Solche Angriffe können den Klinikbetrieb komplett lahmlegen, Operationen verzögern oder die Umleitung von Rettungsdiensten erzwingen. [2].

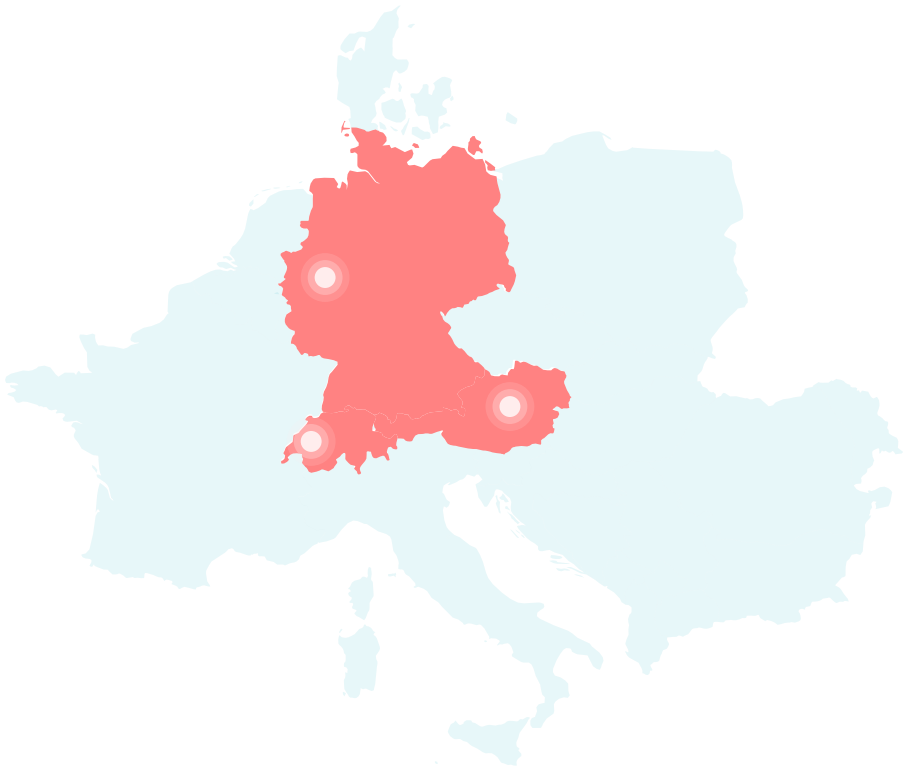
3. **E-Mail-Betrug und Business-E-Mail-Compromise (BEC):**
   Cyberkriminelle setzen zunehmend auf Social Engineering indem sie sich als Führungskräfte, Lieferanten oder öffentliche Institutionen ausgeben. 2023 wurden in mehreren deutschen Kliniken Gehaltsumleitungsbetrügereien gemeldet, bei denen Angreifer Personalabteilungen täuschten um Gehaltszahlungen auf betrügerische Konten umzuleiten. [3].

Reale Vorfälle in der DACH-Region

Universitätsklinikum Düsseldorf (Deutschland, 2020): Ein Ransomware-Angriff legte die Notaufnahme lahm. Eine Patientin verstarb, nachdem sie in eine andere Klinik verlegt wurde - ein Vorfall, der weltweit Aufmerksamkeit auf die physischen Gefahren von Cyberangriffen lenkte. [4].

Angriff auf Krankenversicherer (Österreich, 2023): Mehrere österreichische Gesundheitskassen wurden Ziel einer Phishing-Kampagne, die sich als staatliche COVID-Information ausgab. Tausende Zugangsdaten wurden gestohlen, einige führten zu Betrugsversuchen bei der Abrechnung. [5].

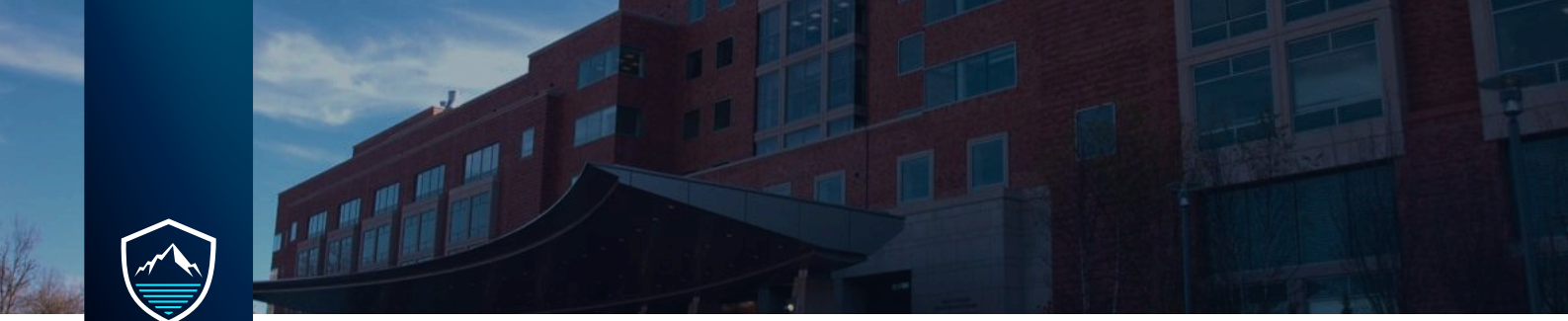
Schweizer Ärztezentrum (Schweiz, 2022): In einer kleinen Klinik im Kanton Waadt kam es zu einer Datenpanne, bei dem Patientenakten offengelegt wurden, was eine umfassende Datenschutzprüfung und eine Benachrichtigungsrunde der Patienten zur Folge hatte [6].



Wachsende Bedrohung

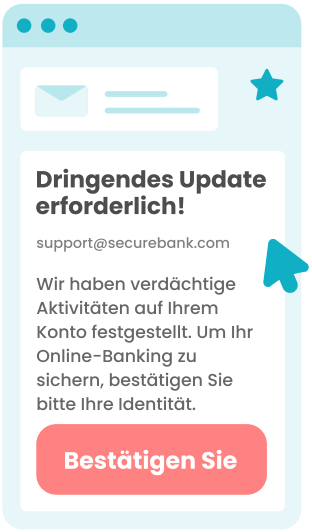
Laut ENISA war das Gesundheitswesen im Jahr 2023 die zweitmeist angegriffene Branche in Europa. Der zunehmende Einsatz vernetzter medizinischer Geräte und Fernzugriffslösungen – beschleunigt durch die Digitalisierung während der COVID-Pandemie – hat die Angriffsfläche weiter vergrößert. **Das deutsche BSI berichtete über einen Anstieg von 92 % bei gemeldeten Cybervorfällen im Gesundheitswesen zwischen 2021 und 2023.**

1. **ENISA-Bedrohungslandschaft 2023** – https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023
2. **BSI IT-Sicherheitslagebericht 2023** – https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.pdf
3. **CERT.at Jahresbericht 2023** – https://www.cert.at/assets/files/docs/report_2023.pdf
4. **BBC News: „Cyberangriff auf deutsches Krankenhaus führte zum Tod eines Patienten“** – https://www.bbc.com/news/technology-54204356
5. **Der Standard (Österreich): „Phishing-Welle trifft Gesundheitskassen“** – https://www.derstandard.at/story/2000133703346/phishing-welle-trifft-oesterreichische-gesundheitskassen
6. **RTS Info (Schweiz): „Cyberangriff gegen ein medizinisches Zentrum Waadtland“** – https://www.rts.ch/info/regions/vaud/13224936-cyberattaque-contre-un-centre-medical-vaudois.html
7. **BSI: Branchenspezifischer Sicherheitsstandard für die Gesundheitsversorgung** – https://www.bsi.bund.de/DE/Themen/Kritische-Infrastrukturen/Gesundheitsversorgung



Phishing: Immer noch der gefährlichste Einstiegspunkt

Trotz technologischer Fortschritte in der Cybersicherheit bleibt Phishing die gefährlichste Eintrittsmethode bei Cybervorfällen im Gesundheitswesen. Angreifer wissen, dass technische Schutzmaßnahmen – wie Spamfilter oder Endpunktschutz – durch gut gemachte, psychologisch wirksame E-Mails umgangen werden können. In stressreichen medizinischen Umgebungen, in denen Mitarbeitende täglich Dutzende Nachrichten bearbeiten, ist diese Taktik weiterhin erfolgreich.



Gefälschte E-Mail

Hinweise zum Social Engineering

- **Dringlichkeit**
  Dringendes sofortiges Handeln
- **Branding**
  gibt sich als legitime Entität aus
- **Sprache**
  verwendet die Muttersprache des Empfängers
- **Namensübereinstimmung**
  enthält vertraut aussehende E-Mail

Warum Phishing im Gesundheitswesen funktioniert

1. **Imitation vertrauenswürdiger Quellen:**
   Phishing-E-Mails geben sich häufig als bekannte Absender aus - z.B. Labore, Personalabteilungen, Behörden oder die interne IT. Die Angreifer verwenden echte Logos, lokale Domains und dringende Betreffzeilen wie "Neues COVID-Protokoll", um sofortige Reaktionen auszulösen.

2. **Mehrsprachige, rollenbasierte Täuschung**
   Die Mehrsprachigkeit in der DACH-Region (Deutsch, Französisch, Italienisch, Englisch) wird gezielt ausgenutzt. 2023 berichtete das Schweizer NCSC über Phishing-Angriffe, die sich an die bevorzugte Sprache des Empfängers anpassten - was die Klickrate erheblich steigerte.

Auch die Inhalte werden an berufliche Rollen angepasst: Ärztinnen und Ärzte erhalten gefälschte Laborwarnungen, Verwaltungspersonal fingierte Rechnungen, IT-Mitarbeitende angebliche Sicherheitsalarme. [1].

3. **Umgehung technischer Kontrollen**
   Viele Phishing-Kampagnen verwenden Techniken wie:

- **Gefälschte Domänen**, die echten Domänen von Gesundheitsorganisationen ähneln
- **Payload-freie Methoden** (z. B. reine Credential-Abfragen)
- **QR-Code-Phishing** wird zunehmend eingesetzt, um E-Mail-Filter zu umgehen.

Diese Methoden umgehen Perimeterschutzmaßnahmen leicht und sind auf menschliches Versagen angewiesen, um erfolgreich zu sein [2].

Beobachtete Beispieltechniken

Gefälschte Terminbestätigungen: Werden an Krankenschwestern oder Verwaltungspersonal gesendet mit der Aufforderung zur Anmeldung zur Überprüfung von Patientenerminen.

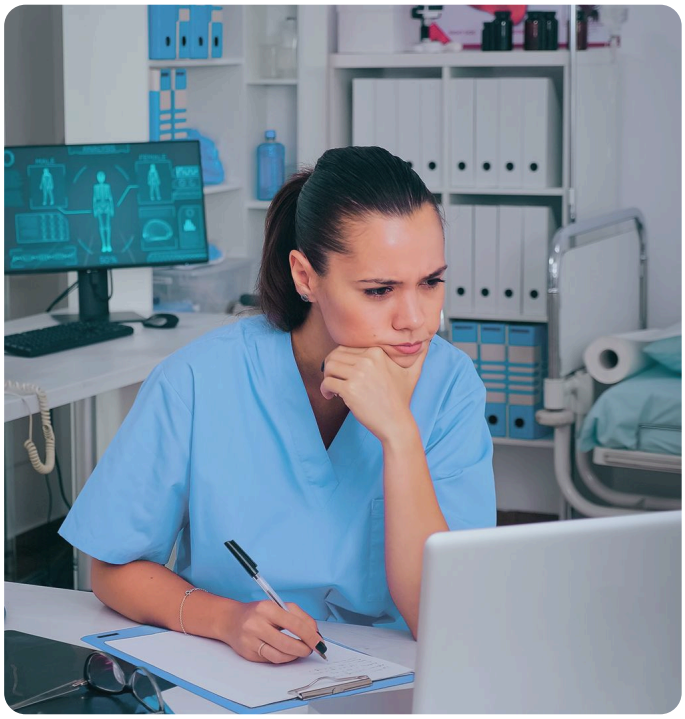
Credential Harvesting-Webseiten: Leiten Mitarbeitende auf gefälschte Login-Portale mit echtem Klinik-Branding weiter.

QR-Code-Phishing: Phishing-E-Mails mit QR-Codes, die angeblich Links zu sicheren Patientenportalen oder Impf-Updates führen.

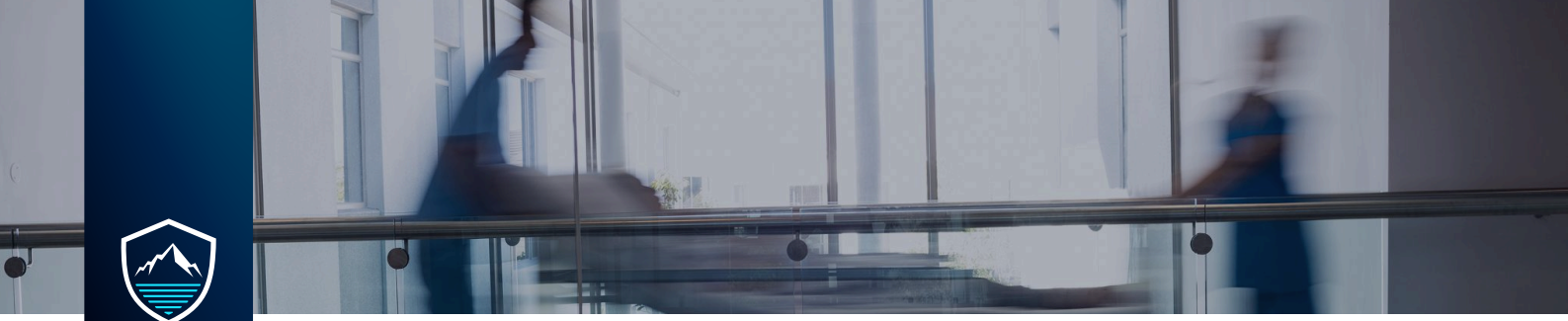
Eine anhaltende Bedrohung

Laut dem SANS Security Awareness Report 2023 bewerten **32 % der Gesundheitsorganisationen Phishing und Credential-Diebstahl** als ihre größte Cyberbedrohung – noch vor Ransomware oder Insider-Risiken. [3]. Gleichzeitig zeigt der Verizon Data Breach Investigations Report, dass **über 60 % der Phishing-E-Mails im Gesundheitswesen bestehende technische Schutzmaßnahmen umgehen**. [4].

Der Mensch bleibt die wichtigste Verteidigungslinie – was die Notwendigkeit kontinuierlicher, realitätsnaher Schulungen unterstreicht. Im Gesundheitswesen können Phishing-Angriffe nicht nur zu Datenverlust, sondern auch zu lebensbedrohlichen Zwischenfällen führen.



1. **Schweizer NCSC-Jahresbericht 2023 –** https://www.ncsc.admin.ch/ncsc/en/home/dokumentation/reports/annual-reports.html
2. **ENISA-Bedrohungslandschaft 2023 –** https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023
3. **SANS Sicherheitsbewusstseinsbericht 2023 –** https://www.sans.org/blog/2023-security-awareness-report
4. **Verizon Data Breach Investigations Report 2023 – Einblicke in den Gesundheitssektor –** https://www.verizon.com/business/resources/reports/dbir/



Die Kosten der Untätigkeit

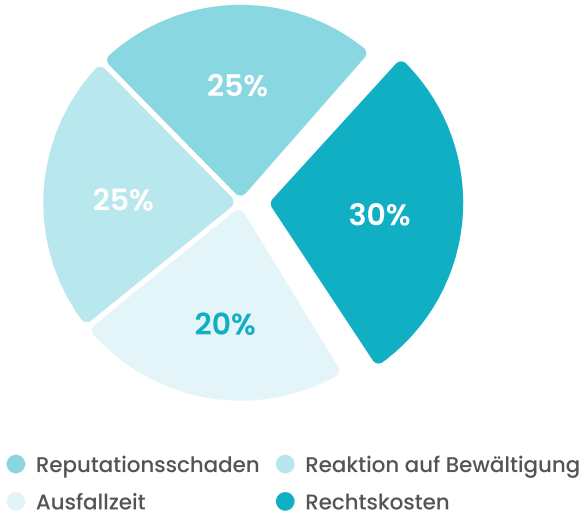
Die Folgen eines erfolgreichen Cyberangriffs im Gesundheitswesen reichen weit über finanzielle Verluste hinaus. In der DACH-Region erhöht die Kombination aus regulatorischem Druck, öffentlicher Verantwortung und Patientensicherheitsrisiken die Kosten des Nichthandelns erheblich.

Finanzielle Auswirkungen

Die durchschnittlichen Kosten eines Datenschutzverstoßes im europäischen Gesundheitswesen werden auf **4–6 Millionen Euro pro Vorfall geschätzt**, wobei Reaktionsaufwand, Ausfallzeiten, Rechtskosten und langfristige Reputationsschäden berücksichtigt wurden [1]. In größeren Krankenhausverbünden oder grenzüberschreitenden Vorfällen kann diese Zahl deutlich höher ausfallen, da Koordination und Wiederherstellung länger dauern.

Ein Beispiel aus 2022: Ein Ransomware-Angriff auf eine mittelgroße Klinik in Bayern verursachte eine Wiederherstellungsrechnung von **1,2 Millionen Euro – einschließlich Notfall-IT-Dienste**, Systemwiederaufbau und verzögerter Patientenversorgung. [2]. Die Versicherung übernahm nur einen Teil der Kosten, die Prämien stiegen danach erheblich.

Kostenaufschlüsselung einer Datenschutzverletzung im Gesundheitswesen



Regulatorische Bußgelder und rechtliche Konsequenzen

Laut DSGVO und nationalen Datenschutzgesetzen (z. B. BDSG in Deutschland, DSG in der Schweiz) müssen Verstöße gemeldet und vorbeugende Maßnahmen – inklusive Schulungen – nachgewiesen werden.Bei Nichteinhaltung drohen Geldbußen von bis zu 20 Millionen Euro oder **4% des weltweiten Umsatzes**, je nachdem, welcher Betrag höher ist [3]. Mehrere deutsche Gesundheitseinrichtungen mussten bereits sechsstellige Bußgelder zahlen, weil sie bei Datenschutzverstößen nicht ausreichend vorgegangen waren oder ihre Mitarbeiter nicht ausreichend zum Datenschutz geschult hatten [4].

Betriebsunterbrechungen und Patientensicherheit

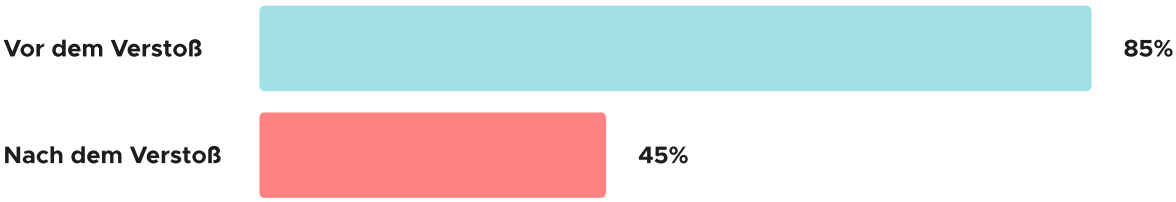
Cyberangriffe führen oft zu IT-Ausfällen, die den Klinikbetrieb massiv beeinträchtigen. In einem Fall 2023 musste ein österreichisches Krankenhaus aufgrund von Ransomware 11 Tage lang auf Papierbetrieb umstellen. Operationen, Labore und Patientenerfassung waren stark verzögert. [5] Im schlimmsten Fall können solche Ausfälle Leben kosten: Beim Angriff auf das Uniklinikum Düsseldorf 2020 musste eine Notfallpatientin umgeleitet werden – sie verstarb unterwegs. [6].

Zeitleiste der Krankenhausausfälle (Tag 1–11)

Reputationsschäden und Versicherungsausfälle

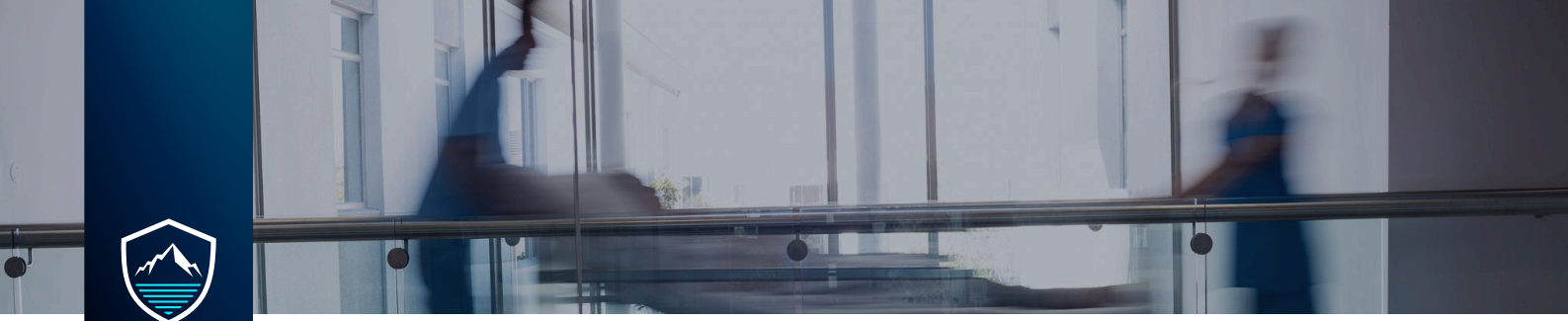
Patientinnen und Patienten erwarten höchste Standards beim Schutz ihrer Daten. Die öffentliche Meldung von Verstößen – heute meist gesetzlich vorgeschrieben – erschüttert das Vertrauen und kann zu Patientenverlust, Klagen oder negativer Berichterstattung führen.

Gleichzeitig verschärfen Versicherungen ihre Anforderungen. Organisationen ohne Schulungen oder Reaktionsprotokolle sehen sich mit reduziertem Schutz oder abgelehnten Schadensfällen konfrontiert – besonders nach wiederholten Vorfällen. [7].



Vertrauensbarometer: Vertrauen vor versus nach einem Verstoß

1. **IBM-Bericht zu den Kosten einer Datenschutzverletzung 2023 – Gesundheitssektor –** https://www.ibm.com/reports/data-breach
2. **Heise Online: "Ransomware-Angriff auf Klinik in Bayern" –** https://www.heise.de/news/Ransomware-Angriff-auf-Klinik-in-Bayern
3. **GDPR Text – Article 83 –** https://gdpr-info.eu/art-83-gdpr/
4. **BfDI Annual Report 2022 –** https://www.bfdi.bund.de/DE/Service/Publikationen/Taetigkeitsberichte/
5. **ORF.at: "Spitalsbetrieb nach Cyberangriff tagelang gestört" –** https://orf.at/stories/3293602/
6. **BBC News: "German hospital cyber-attack led to patient death" –** https://www.bbc.com/news/technology-54204356
7. **SwissRe Institute: Cyber-Versicherung im Gesundheitswesen: Ein sich verhärtender Markt , 2023 –** https://www.swissre.com/institute/research/topics-and-risk-dialogues/technology/cyber-risk.html



Aufbau einer menschlichen Firewall: Die Rolle von Awareness-Training

Während Firewalls, Endpunktschutz und E-Mail-Filter weiterhin essenziell sind, reichen sie allein nicht mehr aus, um ausgeklügelte Phishing-Angriffe abzuwehren. Im Gesundheitswesen – wo Mitarbeitende in Sekundenbruchteilen Entscheidungen treffen und täglich mit sensiblen Daten umgehen – **sind Menschen die neue Sicherheitsgrenze.** Arwareness-Training stattet diese Mitarbeitende mit dem Wissen und den Fähigkeiten aus, um sich proaktiv zu schützen – und so eine sogenannte „menschliche Firewall“ zu bilden.

Kernkomponenten eines effektiven Awareness-Programms

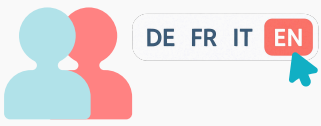
1. **Simulierte Phishing-Kampagnen**
   Realitätsnahe Simulationen helfen dem Personal, typische Phishing-Techniken zu erkennen – ohne echte Risiken einzugehen. Mit der Zeit schärfen diese Übungen das Bauchgefühl und verbessern das Meldeverhalten.

** Organisationen, die alle 4–6 Wochen Phishing-Simulationen durchführen, verzeichnen bis zu 67 % weniger echte Klicks [1].*

2. **Rollenbasierte Microlearning-Module**
   Kurze, zielgerichtete Trainingsinhalte – abgestimmt auf die jeweilige Rolle (z. B. Pflege, Verwaltung, IT) – erhöhen die Relevanz und das Behalten des Gelernten.

Mitarbeitende mit rollenspezifischem Training erkennen Phishing-Versuche 45 % häufiger. [2].

3. **Verhaltensanalytik**
   Fortschrittliche Plattformen erfassen Abschlussquoten, Klickverhalten und Lernfortschritt. Diese Daten ermöglichen die gezielte Weiterentwicklung des Programms – etwa zur Fokussierung auf Hochrisikogruppen.



4. **Lokalisierter und mehrsprachiger Inhalt**
   In der mehrsprachigen DACH-Region erhöhen native Schulungen in Deutsch, Französisch, Italienisch und Englisch die Teilnahme und Akzeptanz erheblich.

**Lucy Security berichtet von 60 % höheren Abschlussraten bei lokalisierter Schulung in Gesundheitseinrichtungen. [3].*

Kulturwandel beginnt mit Bewusstsein

Technische Kontrollen stoppen Malware. Doch nur Menschen können Manipulation erkennen und stoppen. Eine Sicherheitskultur, in der Mitarbeitende Verantwortung für Cybersicherheit übernehmen und sich beim Melden verdächtiger Vorfälle sicher fühlen, ist der Schlüssel zu nachhaltigem Schutz.

Dies erfordert die Zustimmung, Kommunikation und Rückhalt der Führungsebene – nicht nur einmalige Schulungen. Krankenhäuser und Versicherer, die Sensibilisierung in Onboarding-, Compliance-Programme und Führungsbesprechungen integrieren, sind besser gerüstet, um Bedrohungen frühzeitig zu erkennen und darauf zu reagieren.

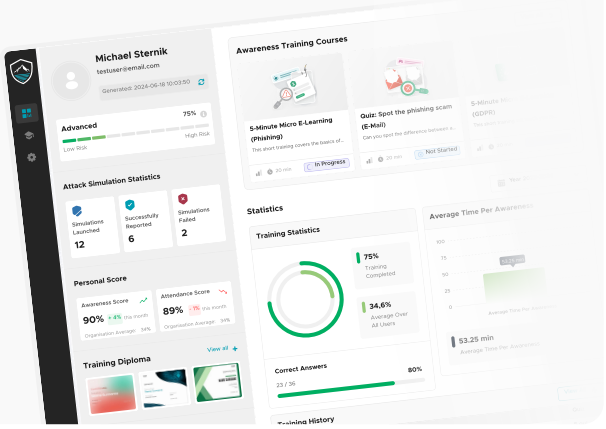
> **“Security Awareness ist keine einmalige Kampagne. Es ist ein kontinuierlicher Prozess, um Cyberhygiene in die täglichen Routinen und Entscheidungen auf allen Ebenen des Gesundheitswesens zu integrieren.“**
>
> — ENISA-Bedrohungslandschaft für das Gesundheitswesen, 2023 [1]

Buchen Sie noch heute eine LUCY-Demo

enquiries@lucysecurity.com

www.lucysecurity.com

Termin buchen



1. **ENISA-Bedrohungslandschaft für das Gesundheitswesen, 202 –** https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-healthcare-sector
2. **SANS Sicherheitsbewusstseinsbericht 2023 –** https://www.sans.org/blog/2023-security-awareness-report
3. **Lucy Security-Kundenbereitstellungsdaten, 2024 –** https://lucysecurity.com

Checkliste: 10 konkrete Schritte für Gesundheitsanbieter in der DACH-Region

Angesichts der Bedrohung durch Phishing, Ransomware, Credential Theft und Social Engineering muss Sicherheitsbewusstsein praxisnah, rollenspezifisch und kontinuierlich sein. Diese Checkliste zeigt zentrale Maßnahmen zur Risikominimierung und Stärkung der Mitarbeitenden als erste

1. **Lokalisiete Schulungen und Simulationen in Landessprachen**
   Inhalte und simulierte Phishing-Nachrichten sollten auf Deutsch, Französisch, Italienisch und Englisch verfügbar sein. Mehrsprachigkeit fördert Verständnis und Inklusion in diversen Teams.

2. **Rollenbasierte Inhalte für Verwaltung, Klinikpersonal, IT und Führung**
   Jede Unternehmensrolle wird mit anderen Angriffstaktiken konfrontiert. Trainieren Sie gezielt mit Szenarien wie gefälschte Entlassungspapiere für Pflegekräfte oder manipulierte Lieferanten-Mails für den Einkauf.

3. **Hohe Trainingsfrequenz etablieren (z. B. monatliche Mikro-Lerneinheiten)**
   Kurze, regelmäßige Schulungen zu aktuellen Bedrohungen (z. B. Social Engineering, Ransomware, MFA-Umgehung) stärken langfristig das Sicherheitsverhalten.

4. **Phishing-Simulationen alle 4–6 Wochen durchführen**
   Nutzen Sie verschiedene Taktiken (z. B. gefälschte Logins, Dokumentköder, Antwort-Phishing), um echte Angriffsmuster realistisch abzubilden.

   **Organisationen mit häufigen Simulationen verzeichnen bis zu 67 % weniger reale Vorfälle.* [1].

5. **Fehlerfreundliche Meldekultur fördern**
   Schaffen Sie eine Kultur, in der Mitarbeitende verdächtige Aktivitäten ohne Angst melden. Auch Fehlalarme oder Fehlklicks sollten frühzeitig gemeldet werden – Schnelligkeit ist entscheidend.

   **Eine positive Meldekultur führt zu einer dreimal höheren Erkennungsrate von Vorfällen* [2].

6. **Awareness in Onboarding und Compliance integrieren**
   Integrieren Sie grundlegendes Wissen zu Phishing und Datenschutz in die Einarbeitung neuer Mitarbeitender. Nutzen Sie GDPR-konforme Wiederholungsschulungen zur Auffrischung.

7. Simulationen mit realitätsnahen Bedrohungen gestalten
Verwenden Sie aktuelle Angriffsmuster wie QR-Code-Phishing, Business E-Mail Compromise (BEC), gefälschte Terminbuchungen oder Impfbenachrichtigungen.

8. Teilnahme und Risikoentwicklung teamweise analysieren
Nutzen Sie Dashboards, um Simulationsergebnisse, Schulungsabschlüsse und Phishing-Klickraten nach Abteilungen zu verfolgen. Identifizieren Sie Ausreisser und fördern Sie gezielte Verbesserungen.

9. Kampagnen an neu auftretenden Bedrohungen ausrichten (Ransomware, Insider-Risiken, MFA-Bypass)
Thematische Schwerpunkte wie Ransomware, privilegierter Zugriff oder Social Engineering gegen Supportpersonal, erhöhen die Aktualität und Wirkung.

10. Führungskräfte aktiv einbinden
Führungskräfte und Abteilungsleiter sollten an Schulungen teilnehmen, deren Bedeutung vermitteln und sicheres Verhalten vorleben. Das Engagement der Führungskräfte erhöht die Glaubwürdigkeit und Reichweite des Programms.

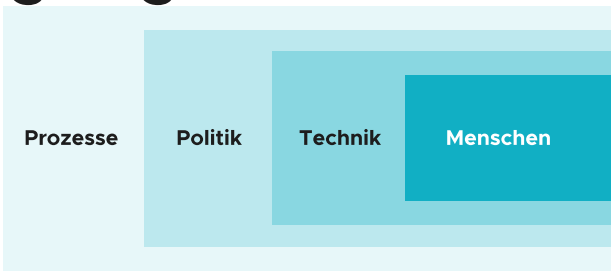
Ein starkes Awareness-Programm verhindert nicht nur Phishing, sondern baut organisatorische Resilienz auf. Regelmäßige Schulungen, realistische Simulationen (z. B. QR-Codes, medizinische Täuschungen) und rollenspezifisches Training in allen Sprachen machen den Unterschied.

Awareness ist nicht länger optional sondern operative Verteidigung.

1. **SANS Sicherheitsbewusstseinsbericht 2023 –** https://www.sans.org/blog/2023-security-awareness-report
2. **Interne Benchmarking-Daten von Lucy Security, 2024 –** https://lucysecurity.com

Ergänzende Maßnahmen für eine widerstandsfähige Verteidigung

Awareness-Training reduziert menschliches Risiko erheblich – doch es wirkt am besten im Zusammenspiel mit einer breiteren Cybersecurity-Strategie. Für Gesundheitsanbieter in der DACH-Region entsteht echte Resilienz durch das Zusammenwirken von Technik, Prozessen, Richtlinien und Menschen.



1. Technische Schutzmaßnahmen stärken

Das Bewusstsein muss durch robuste technische Schutzmaßnahmen unterstützt werden, die das Risiko verringern und Bedrohungen stoppen, bevor sie die Benutzer erreichen.

Erweiterte E-Mail-Filterung und Bedrohungserkennung:

Verwenden Sie KI-gestützte E-Mail-Sicherheitssysteme, die schädliche Links, Spoofing-Muster und Anhänge schon vor der Zustellung erkennen.

Multi-Faktor-Authentifizierung (MFA)

Erzwingen Sie MFA für alle Remote-Zugriffs- und E-Mail-Systeme - so werden kompromittierte Passwörter allein nutzlos.

Endpunktschutz und Patch-Management

Sorgen Sie für eine Echtzeitüberwachung und regelmäßige Patch-Zyklen, insbesondere bei älteren klinischen Systemen, mit erhöhtem Angriffsrisiko.

Netzwerksegmentierung:

Trennen Sie sensible medizinische Geräte und Patientendatenspeicher von allgemeinen Netzwerk, um laterale Bewegung im Angriffsfall zu begrenzen.

2. Sicherheitsrahmen einhalten

Setze auf anerkannte Standards, um Maßnahmen dokumentierbar und auditierbar zu machen:

BSI IT- Grundschutz (Deutschland):

Berücksichtigt Security Awareness explizit und fordert integrierte, risikobasierte Schutzkonzepte. [1].

ISO/IEC 27001:

Internationaler Standard mit Awareness-Kontrollen in Anhang A.7, passend für Informationssicherheits-Managementsysteme (ISMS).

Vorbereitung auf die NIS2-Richtlinie:

Organisationen in kritischen Infrastrukturen müssen seit 2025 sowohl technische als auch organisatorische Schutzmassnahmen nachweisen. [2].

Grafische Cybersicherheitsanforderungen in DACH: ISO/IEC 27001, BSI IT-Grundschutz, NIS2

Kontrollbereich	ISO/IEC 27001:2022	BSI IT-Grundschutz	NIS2-Richtlinie
Sensibilisierungstraining	🟠 Die Mitarbeiter müssen sich ihrer Sicherheitsverantwortung und der Konsequenzen von Verstößen bewusst sein (Abschnitt 7.3, A.6.3). [4].	🟠 Schulungen sind eine grundlegende Maßnahme (Standard 200-2). [5].	🟢 Artikel 21(2)(e): Schulung der Mitarbeiter und Führungskräfte. [6].
Risikobewertung	🟠 Informationssicherheitsrisiken müssen identifiziert, analysiert und bewertet werden (Abschnitt 6.1.2).	🟠 Kernprozess zur Anpassung des Schutzbedarfs.	🟢 Unternehmen müssen Cybersicherheitsrisiken bewerten und managen.
Reaktion auf Vorfälle	🟠 Vorfälle müssen geplant, bewertet, beantwortet und daraus gelernt werden (Anhang A.5.24–A.5.28).	🟠 Definiert Rollen und Workflows für die Vorfallbehandlung.	🟢 Artikel 21(2)(d): Reaktionspläne, Übungen und Berichterstattung.
Managementrolle	🟠 Die Führung muss die ISMS-Leistung unterstützen, Ressourcen zuweisen und sicherstellen (Klauseln 5.1–5.3).	🟠 Klare Zuweisung der Verantwortlichkeiten erforderlich.	🟢 Artikel 20(2): Führungskräfte müssen Maßnahmen überwachen und genehmigen.
Dokumentation	🟠 Halten Sie Richtlinien, Verfahren, Risikobewertungen und Nachweise aufrecht (Klauseln 7.5, 9.1).	🟠 ISMS erfordert eine strukturierte und aktuelle Dokumentation.	🟢 Es müssen dokumentierte Richtlinien und Pläne zur Cybersicherheit vorliegen.
Kontinuierliche Verbesserung	🟠 Das ISMS muss durch Audits und Überprüfungen kontinuierlich verbessert werden (Abschnitt 10.2).	🟠 Es wird eine laufende Überprüfung und Optimierung der Kontrollen erwartet.	🟡 Es wird empfohlen, die Maßnahmen regelmäßig zu aktualisieren.

🟢 **Obligatorisch** – Gesetzlich vorgeschrieben; die Nichteinhaltung führt zu rechtlichen oder behördlichen Sanktionen.
🟠 **Erforderlich** – Unverzichtbar für die Zertifizierung oder Einhaltung des Standards/Frameworks.
🟡 **Empfohlen** – Wird dringend empfohlen, aber nicht strikt durchgesetzt; bewährte Vorgehensweise.

3. Awareness in Notfallplanung einbetten

Sensibilisierung sollte Teil des Business Continuity Managements sein:

- Simuliere Phishing-basierte Vorfälle in Notfallübungen
- Verankere Awareness-Checklisten in Wiederherstellungsplänen
- Schulen von Führungs- und Klinikpersonal zu Kommunikationsstrategien nach Sicherheitsvorfällen

4. Richtlinien mit Kultur verbinden

Technische Richtlinien reichen nicht – sie müssen verstanden und gelebt werden:

- Klare Kommunikation der Cybersecurity- und Meldepflichten bei Einstellung und jährlich wiederholen
- Erwartungen positiv vermitteln, z. B. durch Poster, interne Mails, Führungsvorbilder
- Awareness-Elemente in bestehende Qualitäts- und Zertifizierungsprozesse (z. B. ISO 9001) integrieren

1. **BSI IT- Grundschutz -Kompendium, Ausgabe 2023 –** https://www.bsi.bund.de/DE/Themen/ITGrundschutz
2. **EU-NIS2 -Richtlinie Zusammenfassung –** https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
3. **ISO/IEC 27001:2022 Standard –** https://www.iso.org/standard/27001
4. **ISO/IEC 27001 Abschnitt 7.3 und Anhang A.6.3** – ISMS.online
5. **BSI IT-Grundschutz Standard 200-2** – BSI Germany
6. **NIS2-Richtlinie Artikel 21(2)(e)** – EUR-Lex

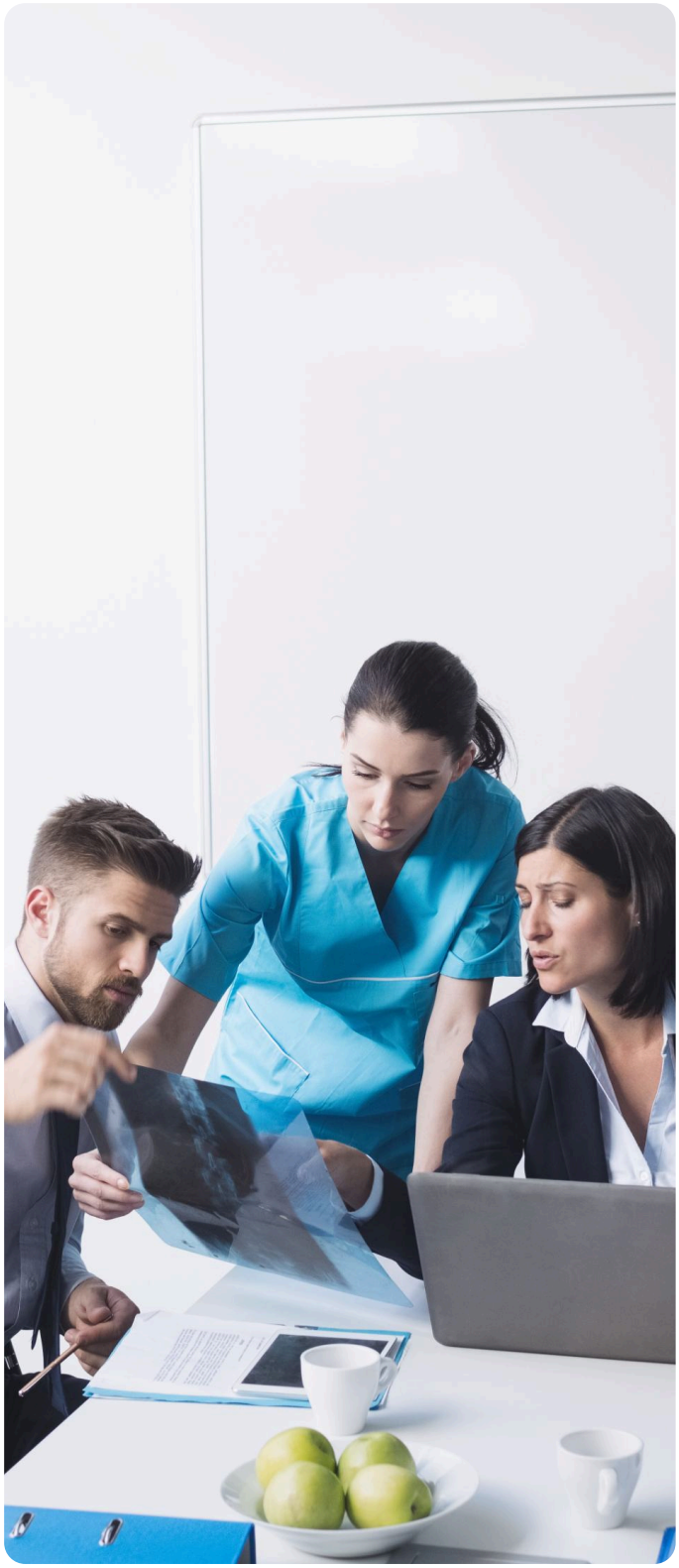
Fazit

Gesundheitsdienstleister in der DACH-Region stehen unter wachsendem Druck – durch Cyberkriminelle, gesetzliche Vorgaben und die steigenden Erwartungen der Öffentlichkeit. Mit dem Fortschritt der Digitalisierung wächst auch die Angriffsfläche. Phishing, E-Mail-Betrug und Social Engineering bleiben die häufigsten Einstiegspunkte für Cyberangriffe – sie zielen gezielt auf das unberechenbarste Element: den Menschen.

Diese Schwachstelle ist zugleich eine Chance.

Durch gezielte, strukturierte und kontinuierliche Awareness-Schulungen – lokal angepasst an Sprache und Rolle – können Gesundheitsorganisationen ihr Risiko deutlich reduzieren. Sensibilisierung ist kein reiner Compliance-Punkt, sondern eine strategische Fähigkeit, die interne Resilienz aufbaut und Patientendaten, Klinikbetrieb und Vertrauen schützt.

Angesichts von Schäden in Millionenhöhe und realen Gefahren für die Patientenversorgung ist die Argumentation für proaktive, menschenzentrierte Cybersicherheit stärker denn je.



Cybersicherheit im Gesundheitswesen beginnt beim Menschen.
Und die Befähigung dieser Menschen beginnt mit Awareness.

Kosten-Nutzen-Analyse & Auswahlhilfe

Die Wirtschaftlichkeit von Awareness-Training

Sicherheitsbewusstsein ist nicht nur eine Sicherheitsmaßnahme – es fördert das Geschäft. Bedenken Sie die potenziellen Vorteile:

Niedrigere Versicherungsprämien: Cyberversicherer berücksichtigen zunehmend Trainingsdaten und Phishing-Simulationsergebnisse bei der Prämiengestaltung. [1].

Regulatorische Nachweise: Dokumentierte Schulungen und Tests sind ein klarer Vorteil bei Datenschutzprüfungen und Post-Breach-Ermittlungen nach DSGVO, revDSG oder NIS2.

Weniger gravierende Sicherheitsvorfälle: Studien zeigen: Geschultes Personal reduziert Phishing-Erfolgsquoten um 60-70% - was Millionen an Folge- und Wiederherstellungskosten einsparen kann. [2].

Höheres Vertrauen und stärkere Sicherheitskultur: Geschulte Mitarbeitende verhalten sich sicherer, melden schneller und tragen zu einem offenen Sicherheitsklima bei.

Trainingsmodell: Eigenbetrieb vs. Managed Service

Für viele Gesundheitseinrichtungen, insbesondere mittelgroße Krankenhäuser oder regionale Kliniken, ist die Wahl der Schulungsmethode ebenso wichtig wie die Entscheidung, sie überhaupt durchzuführen. Organisationen können zwischen zwei Modellen wählen:

Lizenziertes Produkt (Inhouse-Modell)

Erwerben Sie Ihre eigene Produktlizenz, um ein vollständig personalisiertes Kampagnenprogramm unter Ihrer eigenen Kontrolle durchzuführen. In den meisten Branchen erfolgt dies als SaaS (Software as a Service) und wird vom Anbieter innerhalb der EU gehostet. Sie können das Produkt auch auf Ihrer eigenen IT-Infrastruktur (On-Premise) installieren. Diese Option ist im Gesundheitswesen und im Bankensektor beliebt.

Natürlich kann Ihr Anbieter Sie mit Managed Services beim Betrieb des Systems unterstützen, aber oft werden Sie die Bedienung selbst übernehmen, was durch automatisierte Kampagnen und die Erstellung von Benutzerrisikoprofilen sehr gut möglich ist. Dieser Ansatz eignet sich in der Regel für größere Organisationen mit eigenen IT-Ressourcen, typischerweise über 1.000 Mitarbeitern.

Managed Awareness Service (Outsourced-Modell)

Kleinere oder ressourcenbeschränkte Unternehmen können sich für einen **vollständig verwalteten Awareness-Service entscheiden**, bei dem Phishing-Simulationen, Reporting, Schulungsupdates und sogar die Compliance-Verfolgung von einem externen Anbieter übernommen werden. Dies reduziert den internen Aufwand und erfüllt gleichzeitig die regulatorischen und Audit-Anforderungen. Dies eignet sich am besten für Unternehmen mit 10 bis 1.000 Mitarbeitern.

Lucy Security und ihre Partner können Sie bei allen dreien (SaaS, On-Premise und MSP) unterstützen und bieten Gesundheitsdienstleistern Flexibilität basierend auf ihrer Sicherheitsreife und Teamkapazität.

1. **Swiss Re Institute – Cyber-Versicherung und Risikomodelle im Gesundheitswesen –** https://www.swissre.com/institute/research/topics-and-risk-dialogues/technology/cyber-risk.html
2. **ENISA-Bedrohungslandschaft für das Gesundheitswesen, 2023 –** https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-healthcare-sector

Nächster Schritt: Worauf Sie bei einer Awareness-Lösung achten sollten

Die Wahl der richtigen Schulungsplattform oder des richtigen Managed Services ist eine strategische Entscheidung – insbesondere für Gesundheitsdienstleister, bei denen Zeitdruck, mehrsprachige Umgebungen und strenge Compliance eine Rolle spielen. Nachfolgend finden Sie eine von Experten zusammengestellte Checkliste mit unverzichtbaren Funktionen, gruppiert nach Kategorien. Sie hilft Ihnen bei der Auswahl von Lösungen, die Ihren Personalbereich effektiv schützen.

Phishing-Simulation und Bedrohungsreplikation	
Unterstützung für verschiedene Angriffszenarien:	• ✉️ E-Mail • 📱 QR-Code-Phishing (Scan-and-Click-Angriffe) • 💬 Nachrichtenbasierte Köder (WhatsApp und SMS-Phishing/„Smishing“ sind ein Muss) • 🔌 Physisches Gerät (USB-Angriffe)
Simulation von Phishing-Angriffsarten:	• 🔐 Erfassung von Anmeldeinformationen • 🏢 Business Email Compromise (BEC) • 💸 Gefälschte Zahlungs-/Rechnungsaufforderungen • 🦠 Ransomware-Köder (anhangsbasiert)
Erweiterte Simulationsfunktionen	• 🧪 Klonen von echten Phishing-Attacken oder reale Posteingangsangriffe fürTrainingssimulationen • 👥 Rollenbasierte Angriffsvorlagen (z. B. medizinische Warnungen, gefälschte HR-Benachrichtigungen, IT-Ticket-Spoofing) • © Möglichkeit, reale Landingpages zu klonen, um realitätsnahe Angriffe zu erstellen • 🌍 Lokalisierte und mehrsprachige Phishing-Vorlagen (DE, FR, IT, EN) • 📈 Skalierung des Phishing-Schwierigkeitsgrads (Anfänger bis Fortgeschrittene) • 📆 Automatisierte Kampagnenplanung (wöchentliche/monatliche Abläufe) • 💣 Angriffs-Randomisierung (automatische Variation der Sendefrequenz sowie der Angriffsauswahl) • 🚦 Risikobewertungn und Feedback zur Generierung nachfolgender Kampagnen

Awareness-Trainung und Microlearning	
Lernformate	• ⏱️ Kurze Module (5–10 Min.) für vielbeschäftigte klinische und administrative Rollen • 👶 Rollenbasierte Lernpfade (z. B. Kliniker, Finanzen, IT, Führungskräfte) • 🌐 Mehrsprachige, auf regionale Gesundheitssysteme zugeschnittene Kursinhalte
Compliance-Ausrichtung	• 📚 Inhalte im Einklang mit Compliance-Frameworks (z. B. DSGVO, ISO 27001) • 🧠 Interaktive Formate (Quizze, Szenarien, Gamification) • 🧩 Maschinenbasiertes, adaptives Lernen basierend auf Leistungshistorie und/oder Risikobewertung

Betrieb, Compliance und Reporting

Flexible Bereitstellungsoptionen:	• 🏢 On-Premise-Hosting für volle Datenkontrolle • ☁️ Cloudbasierte Optionen (in der EU gehostet) für Skalierbarkeit und Benutzerfreundlichkeit
Analyse und Reporting	• 🗒️ Auditfähiges Reporting zur Einhaltung der DSGVO • 📊 Dashboards zur Verhaltensanalyse und Überwachung des Benutzerrisikos, der Kampagnenleistung sowie von Trends
Endbenutzerportal, wo Mitarbeiter:	• 🔎 Den eigenen Risikowert oder Fortschritt sehen können • 🎯 Auf zugewiesene und optionale Schulungsmodule zu greifen können • 📔 Überprüfung vonSimulationsverlauf und Feedback
Weitere Funktionen	• Integration mit Identitätsplattformen (z. B. Azure AD, Okta, LDAP) für Benutzerverwaltung und SSO • Anpassbare Benutzerrisikobewertung basierend auf Verhalten, Rolle und Simulationsergebnissen • Managed-Service-Option für Organisationen ohne dedizierte Awareness- oder SOC-Teams • Datenhosting innerhalb der EU oder Vor-Ort-Optionen (für Umgebungen mit sensiblen Gesundheitsdaten)

Unterstützung bei Zwischenfällen

Support-Optionen	• 🆘 Integration der Schaltfläche „Phishing melden“ in E-Mail-Clients (Outlook, Gmail usw.) • 📄 Tipps und Hilfestellung nach dem Klick (was ist schiefgelaufen ist und auf was es ankommt) • 🦾 Awarnesskampagnen-Kits (Plakate, interne E-Mails, digitale Beschilderung) • 🧭 Module zur Schulung und Sensibilisierung von Führungskräften • 🥷 Anonyme oder unkomplizierte Meldewege zur Förderung sicherer Verhaltensmuster

Tipp 1:
Wähle Sie einen Anbieter mit Erfahrung im Gesundheitswesen, echter Mehrsprachigkeit und realistischer Angriffsnachbildung.

Tipp 2:
Vermeiden Sie Lösungen, die Awareness mit irrelevanten Services bündeln (z. B. Dark-Web-Monitoring). Spezialisierte Awareness-Lösungen bieten höhere Mehrwerte und Nutzen.

Referenzen und weiterführende Literatur

Nachfolgend finden Sie eine kuratierte Liste maßgeblicher Quellen, die diesem Bericht zugrunde liegen. Dazu gehören regionale Cybersicherheitsbehörden, wissenschaftliche Studien, politische Rahmenbedingungen der EU und branchenspezifische Bedrohungsanalysen – alle ausgewählt aufgrund ihrer Neutralität, Relevanz und Glaubwürdigkeit im europäischen Gesundheitswesen.

Cybersicherheitsberichte und Bedrohungsinformationen

1. **ENISA-Bedrohungslandschaft für das Gesundheitswesen (2023)**
   Agentur der Europäischen Union für Cybersicherheit – Sektorspezifische Analyse der sich entwickelnden Bedrohungen für das Gesundheitswesen.
   https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-healthcare-sector
2. **BSI – Die Lage der IT-Sicherheit in Deutschland (2023)**
   Jährlicher Cybersicherheitsbericht des Bundesamtes für Sicherheit in der Informationstechnik.
   https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.pdf
3. **CERT.at-Jahresbericht (2023)**
   Überblick über Vorfalltrends und Reaktionen in Österreich.
   https://www.cert.at/assets/files/docs/report_2023.pdf
4. **Schweizer NCSC-Jahresbericht zur Cybersicherheit (2023)**
   Nationales Zentrum für Cybersicherheit der Schweiz – Vorfälle, Phishing-Trends und Empfehlungen.
   https://www.ncsc.admin.ch/ncsc/en/home/dokumentation/reports/annual-reports.html
5. **Verizon Data Breach Investigations Report – Einblicke in den Gesundheitssektor (2023)**
   Globale Bedrohungsmuster und Daten zu Datenschutzverletzungen mit Schwerpunkt auf Gesundheitsorganisationen.
   https://www.verizon.com/business/resources/reports/dbir/

Regulatorische und politische Rahmenbedingungen

1. **Datenschutz-Grundverordnung (DSGVO) – Artikel 83.**
   Einzelheiten zu Meldepflichten und Bußgeldern bei Verstößen.
   https://gdpr-info.eu/art-83-gdpr/
2. **BSI IT- Grundschutz- Kompendium (2023)**
   Rahmenwerk zur Umsetzung der Informationssicherheit in öffentlichen und privaten Einrichtungen.
   https://www.bsi.bund.de/DE/Themen/ITGrundschutz
3. **ISO/IEC 27001:2022 – Information Security Management**
   Internationaler Standard für ISMS, einschließlich Sensibilisierungs- und Schulungsanforderungen (Anhang A.7).
   https://www.iso.org/standard/27001
4. **EU-NIS2-Richtlinie – Zusammenfassung für kritische Einrichtungen.**
   Neue Verpflichtungen für Anbieter digitaler und medizinischer Infrastruktur in der EU.
   https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

Bewusstsein und menschliches Risiko

1. **SANS Security Awareness Report (2023)**
   Umfrage und Analyse von Trends bei Sensibilisierungsprogrammen und menschenzentrierten Sicherheitsdaten.
   https://www.sans.org/blog/2023-security-awareness-report
2. **Lucy Security Benchmarking- und Simulationsdaten (2024)**
   Aggregierte Leistungskennzahlen aus Phishing-Simulationen und Schulungen im Gesundheitswesen.
   https://lucysecurity.com
3. **Swiss Re Institute – Cyber-Versicherung im Gesundheitswesen: Risiko- und Resilienztrends (2023)**
   Einblicke in den Einfluss von Schulung und Vorbereitung auf Versicherungsschutz und Prämien.
   https://www.swissre.com/institute/research/topics-and-risk-dialogues/technology/cyber-risk.html

LUCY
AWARENESS

enquiries@lucysecurity.com

www.lucysecurity.com