

The image features a blue-toned background with a stethoscope in the foreground. A digital network of glowing lines and nodes is visible, with a prominent padlock icon in the center. The logo 'e3' is positioned in the top left corner.

e3

EXPLORER WORKSHOP

Von der Vision zur sicheren und resilienten
Digitalisierung im Gesundheitswesen



Der Explorer Workshop für Entscheidungsträger im Gesundheitswesen

Die Digitalisierung stellt das Gesundheitswesen vor grosse Herausforderungen und Chancen gleichermaßen. Krankenhäuser, Kliniken, Pflegeeinrichtungen und Gesundheitsdienstleister müssen sich an neue technologische Entwicklungen anpassen, um Patientensicherheit, Effizienz und Datenschutz zu gewährleisten.

Wie kann eine digitale Strategie die Patientenversorgung verbessern? Welche IT-Sicherheitsmassnahmen sind erforderlich, um sensible Gesundheitsdaten zu schützen? Welche Technologien sind für Ihr spezifisches Geschäftsfeld relevant? In einem strukturierten Workshop erarbeitet e3 gemeinsam mit Ihnen Antworten auf diese Fragen und entwickelt eine fundierte Strategie für Ihre Einrichtung im Gesundheitswesen.

Über e3

e3 steht für Digitalisierung und IT-Sicherheit – und das seit 25 Jahren. Unsere Kernkompetenz liegt in Cyber Security, Datenschutz und Compliance, um Unternehmen vor Datenverlust und Cyberangriffen zu schützen. Wir begleiten Organisationen auf ihrem Weg zur digitalen Transformation, indem wir sichere, effiziente und regelkonforme digitale Prozesse ermöglichen.

Unsere Lösungen schützen kritische und sensible Daten – sei es in regulierten Branchen oder in Bereichen mit besonderen Sicherheitsanforderungen wie dem Gesundheitswesen. Mit unserer Cyber-Security-Expertise und unserem Compliance-Know-how unterstützen wir Unternehmen dabei, Cyberrisiken zu minimieren und ihre digitale Infrastruktur nachhaltig zu stärken.

Wir behalten die sich wandelnde Bedrohungslandschaft und regulatorischen Vorgaben stets im Blick. Unsere Lösungen sind darauf ausgelegt, nicht nur aktuelle, sondern auch zukünftige Anforderungen an Sicherheit und digitale Innovation zu erfüllen.



Cybersicherheit im Gesundheitswesen

Herausforderungen

Die Digitalisierung im Gesundheitswesen bringt nicht nur Effizienzsteigerungen, sondern auch erhebliche Sicherheitsrisiken mit sich. Studien zeigen, dass Gesundheitsorganisationen verstärkt ins Visier von Cyberangriffen geraten. Besonders problematisch sind:

Veraltete IT-Architekturen

Viele Klinikinformationssysteme (KIS) basieren oft noch auf unsicheren Zwei-Schichten-Architekturen, die eine leichte Angriffsfläche bieten.

Unzureichende Sicherheitsmassnahmen

Die Umsetzung grundlegender Cybersicherheitsmassnahmen wird oft vernachlässigt, was zu erheblichen Risiken führt.

Ransomware-Angriffe

Der Gesundheitssektor ist besonders anfällig für Ransomware-Angriffe, wobei Angriffe oft grosse finanzielle und betriebliche Schäden verursachen.

Mangel an Sicherheitsbewusstsein

Viele Organisationen sind sich der Bedrohungslage nicht ausreichend bewusst und investieren zu wenig in die Cybersicherheit.

Gefahren

Cyberangriffe auf Spitäler nehmen weltweit zu:

Ausfall kritischer Systeme

2024 führte ein Ransomware-Angriff auf ein europäisches Krankenhaus dazu, dass Operationen verschoben werden mussten. Daraus resultierten potenziell lebensbedrohliche Verzögerungen für Patienten.

Datenverlust und Erpressung

In den USA wurden gestohlene Gesundheitsdaten von tausenden Patienten im Darknet verkauft, was massive rechtliche und finanzielle Konsequenzen für die betroffene Klinik hatte.

Manipulation medizinischer Geräte

Sicherheitslücken ermöglichen Cyberkriminellen, Dosierungen von Medikamenten oder Beatmungsgeräte zu verändern – mit potenziell tödlichen Konsequenzen.

Vertrauensverlust und rechtliche Folgen

Datenschutzverletzungen ziehen hohe Strafen nach sich. Ein Krankenhaus in Frankreich wurde 2023 zur Zahlung von Millionenbeträgen verpflichtet, nachdem Patientendaten ungeschützt im Netz kursierten.





Ein Workshop – massgeschneidert für das Gesundheitswesen

Jede Gesundheitseinrichtung hat individuelle Herausforderungen. Unsere Workshop-Themen umfassen:

IT-Sicherheit & Datenschutz

Schutz sensibler Gesundheitsdaten, DSGVO-/GPDR-Compliance, Cybersecurity-Lösungen basierend auf den neuesten Erkenntnissen aus Sicherheitsanalysen, IT-Grundsicherheitsmassnahmen.

Digitalisierte Patientenversorgung

Elektronisches Patientendossier (EPD), Elektronische Patientenakte (EPA), Elektronische Gesundheitsakte (ELGA), digitale Patientenkommunikation.

Datenmanagement & Interoperabilität

Vernetzung zwischen Spitälern, Praxen, Pflegeeinrichtungen, Krankenkassen, Apotheken optimieren.

Cloud-Strategien für Gesundheitseinrichtungen

Effiziente Nutzung sicherer Cloud-Technologien mit Blick auf IT-Sicherheitsrisiken.

Künstliche Intelligenz & Big Data

Einsatz intelligenter Analysen für bessere Diagnosen und Behandlungen.

Ihr Nutzen

Unsere Experten führen Sie durch einen interaktiven und strukturierten Workshop mit besonderem Fokus auf Digitalisierung, Cybersicherheit und Datenschutz. Gemeinsam erarbeiten wir:

1. Eine **klare Vision** für Ihre Institution im digitalen Gesundheitswesen, mit besonderer Berücksichtigung sicherer IT-Architekturen und Cyberresilienz.
2. Eine **tiefgehende Analyse** Ihrer aktuellen IT- und Prozesslandschaft, einschliesslich potenzieller Sicherheitsrisiken und Schwachstellen.
3. Ein klares **Verständnis der IT-Sicherheitsziele** und die Priorisierung der identifizierten Massnahmen.
4. Die **Entwicklung einer Strategie** für digitale Innovationen unter Berücksichtigung robuster Cybersecurity-Massnahmen.
5. Eine **massgeschneiderte Roadmap** mit konkreten Massnahmen, die Cyberrisiken gezielt adressieren, die Cybersicherheit und den Datenschutz ausbauen, um Cyberangriffe effektiv zu verhindern.



Das Workshop-Modell – Bewährt für mehr Cybersicherheit



Individuelle Vorbereitung	Vision (Onsite Workshop)	Realitätscheck (Onsite Workshop)	Potenzialanalyse	Schliessen von Lücken	Massnahmen (Onsite Workshop)	Ergebnisdokumentation
<p>Im Vorfeld werden telefonische Absprachen mit den teilnehmenden Fachleuten durchgeführt.</p> <p>Ziel: Die e3-Experten nehmen die Ausgangssituation detailliert auf und planen den Workshop.</p>	<p>Sie diskutieren mit uns Ihre Zukunft im digitalen Gesundheitswesen.</p> <p>Wohin soll die Einrichtung sich entwickeln? Welches Potenzial liegt noch brach?</p> <p>Ziel: Alle bringen ihre Ideen uneingeschränkt ein; auch vermeintlich unrealistische Vorschläge haben Platz.</p>	<p>Bestimmung der Ist-Situation.</p> <p>Wo steht Ihre Einrichtung heute? Wie ist diese im Vergleich zu ähnlichen Einrichtungen aufgestellt?</p> <p>Ziel: Ermittlung von Stärken, Schwächen, Bedrohungslage und Chancen.</p>	<p>Abgleich von Vision und Ist-Zustand. Die daraus resultierende Differenz gibt einen ersten Überblick über das Verbesserungs- und Entwicklungspotenzial.</p> <p>Ziel: Identifikation von Optimierungsmöglichkeiten für die sichere digitale Transformation.</p>	<p>Die ermittelte Lücke zeigt, wo die aktuelle Situation und die Vision auseinanderklaffen.</p> <p>Welche Ziele können erreicht werden, welche nicht? (Mögliche Ausschlusskriterien: Budget, Kapazität oder Technologieniveau).</p> <p>Priorisierung: Was muss, soll, kann realisiert werden?</p> <p>Ziel: Sie erarbeiten mit uns eine Strategie zur sicheren Digitalisierung.</p>	<p>Wie sollen die priorisierten Ziele erreicht werden?</p> <p>Definition konkreter Massnahmen: Jede Massnahme mündet in ein konkretes Projekt.</p> <p>Ziel: Wir entwickeln einen klaren Aktionsplan mit realistischen Schritten.</p>	<p>Wir liefern eine erste Einschätzung, eine fundierte Strategie oder ein grundlegendes Konzept – je nach Ihrem Auftrag. Sie erhalten alle Unterlagen aus dem Workshop zur freien Verfügung.</p> <p>Ziel: Ein fundierter Abschlussbericht mit klaren Handlungsempfehlungen.</p>
Workshop-Planung	Entwicklung Zukunftsbild	Cyber Risk Check	Cyberresilienz-Optionscheck	Cyberresilienz-Strategie	Cyberresilienz-Projekte	Cyberresilienz-Report



IT-Sicherheit neu denken – Ihr Weg zur sicheren digitalen Gesundheitseinrichtung

Ihr Praxis-Workshop für IT-Sicherheit und digitale Innovation

2024: Cyberangriffe bedrohen das Gesundheitswesen

- » Ransomware-Angriffe auf Krankenhäuser haben OPs lahmgelegt
- » Patientendaten wurden im Darknet veröffentlicht – mit erheblichem Reputationsverlust
- » Notaufnahmen mussten schließen – der Spitalbetrieb wurde auf manuelle Prozesse umgestellt

Ist Ihre Gesundheitseinrichtung ausreichend geschützt?

Strukturierter Workshop – Ihr Weg zur Cyberresilienz

- » Teilnehmer: 6 – 8 Expertinnen und Experten aus Ihrer Einrichtung
- » Fokus: IT-Sicherheit, Datenschutz, digitale Transformation & Cyberresilienz
- » Ziel: Identifikation von Risiken & Entwicklung einer massgeschneiderten Sicherheitsstrategie

Ergebnis: Klare Roadmap und konkrete Massnahmen für die digitale Sicherheit Ihrer Einrichtung

In wenigen Tagen zur Cyber-Security-Strategie

- » 10 Tage mit e3-Experten für eine umfassende Analyse
- » 2 Tage Onsite-Workshop mit praxisnahen Ergebnissen
- » Begleitende Zwischenschritte & Nachbereitung für maximale Wirksamkeit

Detaillierter Abschlussbericht als Entscheidungsgrundlage für die Geschäftsleitung

Ihr Mehrwert – Warum dieser Workshop?

- » Praxisnah: Von der Analyse zur konkreten Sicherheitsstrategie
- » Massgeschneidert auf Ihre Einrichtung: IT-Sicherheit, Compliance und Innovation kombiniert
- » Zielorientiert: Der Weg zur maximalen Cyberresilienz

Schützen Sie Ihre Einrichtung, Patienten, Daten und Prozesse – bevor es zu spät ist!





Lassen Sie uns gemeinsam Ihre sichere Zukunft gestalten!

e3 steht für IT-Sicherheit – seit 25 Jahren. Unsere Stärke sind zukunftssichere Softwarelösungen zum Schutz vor Cyberangriffen und Datenverlusten. Wir machen Ihre Gesundheitseinrichtung fit für die digitale Transformation und helfen Ihnen, Ihre Daten gemäss den geltenden Vorschriften zu schützen und zu verwalten.

Wir unterstützen Krankenhäuser, Kliniken, Pflegeeinrichtungen und Gesundheitsdienstleister bei der Stärkung ihrer Cyberresilienz. Mit unseren Lösungen sind Sie für die Herausforderungen von morgen gerüstet.

e3 AG Schweiz – Zürich

Binzstrasse 24
CH-8045 Zürich

- » engage@e3ag.ch
- » +41 44 400 46 56

e3 AG Schweiz – Bern

Falkenplatz 3
CH-3012 Bern

- » engage@e3ag.ch
- » +41 31 305 46 56

Internationale Standorte

- » Brasilien
- » Deutschland
- » Niederlande



[e3ag.ch](https://www.e3ag.ch)



[LinkedIn](#)