Cyber-Sicherheitsrat Deutschland e.V.

Strategischer Leitfaden

Einsatz von Künstlicher Intelligenz im Gesundheitswesen

Version 1.0
Stand: August 2025

Grußwort

Berlin, August 2025

Künstliche Intelligenz ist weit mehr als eine technologische Innovation – sie verändert die Art und Weise, wie wir Medizin denken, gestalten und verantworten. Für das Gesundheitswesen eröffnet sie enorme Chancen: effizientere Prozesse, präzisere Diagnostik und eine individuellere Versorgung. Zugleich fordert sie uns heraus, bestehende Strukturen neu zu denken – rechtlich, ethisch und sicherheitspolitisch.

Gerade im Umgang mit sensiblen Gesundheitsdaten ist Vertrauen die entscheidende Währung. Es entsteht dort, wo Sicherheit, Transparenz und Verantwortung Hand in Hand gehen. Der Cyber-Sicherheitsrat Deutschland e.V. setzt sich daher dafür ein, dass digitale Innovation im Gesundheitswesen immer mit Cybersicherheit und Resilienz verknüpft gedacht wird. Nur wenn Systeme geschützt und Governance-Strukturen klar definiert sind, kann KI ihr volles Potenzial entfalten.

Dieser Leitfaden soll Entscheidungsträgerinnen und Entscheidungsträgern Orientierung geben, wie KI im Gesundheitswesen strategisch, sicher und verantwortungsvoll gestaltet werden kann – als integraler Bestandteil einer modernen, krisenfesten Gesundheitsversorgung.

*Mein besonderer Dank gilt **Jan Arfwedson**, der die inhaltliche Ausarbeitung dieses Leitfadens im Rahmen des eHealth Hubs maßgeblich vorangetrieben und die Gesamtentwicklung entscheidend geprägt hat. Ohne seinen fachlichen Tiefgang, seine Beharrlichkeit und seine ausgezeichnete Koordinationsarbeit wäre diese Veröffentlichung in dieser Qualität nicht möglich gewesen. Ebenso danken wir **André Alexander Bosse** herzlich für seine wertvollen Beiträge und seine engagierte Mitwirkung an der Erstellung des Leitfadens.*

Wer heute die richtigen Weichen stellt, legt die Grundlage für ein widerstandsfähiges, modernes und vertrauenswürdiges Gesundheitssystem. Ich wünsche eine gewinnbringende Lektüre und vor allem: gute, informierte Entscheidungen.

Herzlichst,

Hans-Wilhelm Dünn
Präsident
Cyber-Sicherheitsrat Deutschland e.V.

Jan Arfwedson
Vorsitzender eHealth Hub
Cyber-Sicherheitsrat Deutschland e.V.

Inhalt

1. Executive Summary 4
2. Aktuelle technologische Entwicklungen im Bereich KI 5
3. Chancen und Risiken des KI-Einsatzes 6
4. Technische und Organisatorische Sicherheitsmaßnahmen (TOMs) - Ein Überblick und wichtige Quellen 7
5. Wichtige Institutionen im KI-Gesundheitswesen 8
6. KI-Strategie im Unternehmen: Leitlinien für Führung und Aufsicht 9
7. Überblick: Der EU Artifical Intelligence Act (EU AI Act) für Unternehmensleitungen und Aufsichtsgremien 10
8. KI-Projekte im Unternehmen: Governance und Umsetzung im Überblick 11
9. Marktüberblick: KI-basierte Cybersicherheitslösungen 12
10. Fazit und Empfehlungen: KI als strategischer Kompass für Unternehmensleitungen und Aufsichtsgremien 14
11. Checkliste für Geschäftsleitungen, Beiräte und Aufsichtsräte 15
12. Template zur Erstellung einer internen KI-Strategie 16

1. Executive Summary

Künstliche Intelligenz (KI) verändert die Gesundheitsversorgung tiefgreifend – mit weitreichenden Chancen, aber auch sicherheitsrelevanten Herausforderungen. KI-Anwendungen können dazu beitragen, klinische Abläufe zu optimieren, die diagnostische Präzision zu verbessern und administrative Prozesse zu automatisieren. Gleichzeitig erfordert ihr Einsatz höchste Sorgfalt im Hinblick auf Informationssicherheit, Datenschutz, Resilienz und ethische Verantwortung.

Als Cyber-Sicherheitsrat Deutschland e. V. ist es unser Ziel, Entscheidungsträgerinnen und Entscheidungsträger im Gesundheitswesen für die sicherheitsrelevanten Aspekte dieser technologischen Transformation zu sensibilisieren. Der vorliegende Leitfaden richtet sich gezielt an Geschäftsleitungen, Beiräte und Aufsichtsgremien von Gesundheitseinrichtungen und -unternehmen.

Er bietet eine strukturierte Orientierung zur Bewertung, Einführung und sicheren Steuerung von KI-Lösungen. Neben den Potenzialen und Risiken werden insbesondere gesetzliche Rahmenbedingungen, technische Schutzmaßnahmen sowie strategische Handlungsfelder für eine resiliente und vertrauenswürdige KI-Nutzung aufgezeigt.

Unser Anliegen ist es, eine verantwortungsvolle, transparente und zukunftsorientierte Anwendung von KI im Gesundheitswesen zu fördern – als Voraussetzung für nachhaltige Innovation und den Schutz sensibler Daten und Infrastrukturen.

2. Aktuelle technologische Entwicklungen im Bereich KI

KI im Gesundheitswesen – Chancen und strategische Implikationen für Führungsgremien

Das deutsche Gesundheitswesen steht vor einem tiefgreifenden Wandel, getrieben durch den rasanten Fortschritt im Bereich KI. Für Unternehmensleitungen und Aufsichtsgremien ist es essenziell, die strategischen Auswirkungen zu erkennen: KI wird nicht nur Prozesse effizienter gestalten, sondern auch Diagnostik, Therapie und Patienteninteraktion grundlegend verändern.

Relevante Anwendungsfelder

- **Klinische Prozesse & Diagnostik:** KI analysiert große Datenmengen (z. B. Bildgebung, Patientenakten) schneller und genauer – mit dem Potenzial, Versorgung und Qualität signifikant zu verbessern.
- **Personalisierte Medizin & Wirkstoffentwicklung:** Durch KI lassen sich individuelle Therapien sowie neue Medikamente schneller und gezielter entwickeln – ein Innovationsmotor für Pharma und Biotech.
- **Verwaltung & Management:** Automatisierung administrativer Aufgaben entlastet Personal und reduziert Kosten.
- **Telemedizin & Monitoring:** KI-basierte Lösungen ermöglichen eine präzisere Fernbetreuung und verbessern die Versorgung in unterversorgten Regionen.

Strategische Herausforderungen

- **Datenschutz & IT-Sicherheit:** Der Schutz sensibler Gesundheitsdaten hat höchste Priorität.
- **Regulatorik & Compliance:** Der Einsatz von KI unterliegt komplexen gesetzlichen Anforderungen, die stetigem Wandel unterliegen und sich zunehmend verschärfen.
- **Ethik & Akzeptanz:** Vertrauen, Transparenz und Fairness in Algorithmen sind zentrale Erfolgsfaktoren.
- **Investitionen & Kompetenzen:** Der Aufbau geeigneter Infrastruktur und qualifizierter Teams ist unerlässlich.
- **Change Management:** Die Einführung von KI erfordert klare Kommunikation und aktive Begleitung des Wandels.

Fazit

KI wird zum strategischen Differenzierungsfaktor im Gesundheitswesen. Wer als Entscheider heute die Weichen stellt – technologisch, organisatorisch und ethisch –, sichert die Zukunftsfähigkeit seiner Organisation bzw. seines Unternehmens und schafft echten Mehrwert für Patienten, Mitarbeitende und Partner.

3. Chancen und Risiken des KI-Einsatzes

Strategische Perspektiven für Unternehmensleitungen und Aufsichtsgremien

KI bietet Unternehmen enorme Potenziale – von Effizienzsteigerung über Innovation bis hin zu Wettbewerbsvorteilen. Gleichzeitig sind strategisch relevante Risiken zu beachten. Ein ausgewogenes Verständnis beider Seiten ist unerlässlich für eine verantwortungsvolle Implementierung.

1. KI in der Office-IT: Effizienz, Automatisierung, neue Arbeitsweisen

Chancen:

- Automatisierung repetitiver Aufgaben (z. B. Terminplanung, E-Mails, Präsentationen) steigert Produktivität.
- Datenanalysen in Echtzeit ermöglichen fundiertere Entscheidungen.
- Chatbots und Übersetzungstools fördern interne Kommunikation und internationale Zusammenarbeit.
- KI-gestützte Weiterbildung passt sich individuell an Mitarbeitende an.

Risiken:

- Datenschutz und IT-Sicherheit bei sensiblen Unternehmensdaten müssen gewährleistet sein, um Risiken empfindlicher Bußgelder und Reputationsverluste zu vermeiden oder mind. zu reduzieren.
- Abhängigkeit von externen Cloud-Anbietern kann Datenhoheit und Stabilität gefährden.
- Generative KI birgt das Risiko unzuverlässiger Inhalte („Halluzinationen“).
- Automatisierung verändert Jobprofile und erfordert aktives Change Management.
- Verzerrungen in Algorithmen (Bias) können zu diskriminierenden Entscheidungen führen.

2. KI im medizinischen Kontext: Diagnostik, Pflege, Dokumentation

Chancen:

- Höhere Diagnosesicherheit durch präzise Analyse von Bild- und Labordaten.
- Individuelle Therapieansätze auf Basis umfangreicher Patientendaten.
- Entlastung des medizinischen Personals durch Automatisierung dokumentationsintensiver Prozesse.
- Beschleunigte Medikamentenentwicklung und kosteneffizientere Forschung.
- Optimierte Patientenüberwachung durch KI-gestützte Telemedizin.

Risiken:

- Höchste Anforderungen an Datenschutz und Systemsicherheit bei Patientendaten.
- Unklare Haftungsfragen bei medizinischen Fehlentscheidungen durch KI.
- Regulatorische Anforderungen können Innovationsgeschwindigkeit bremsen.
- Intransparente Algorithmen („Black Box“) erschweren Vertrauen und Erklärbarkeit.
- Potenzielle Ablehnung durch Fachpersonal und Patienten bei unklarer Kommunikation.
- Bias in Trainingsdaten kann zu Versorgungsungleichheiten führen.

Fazit

KI ist ein strategischer Hebel – aber kein Selbstläufer. Unternehmensleitungen und Aufsichtsgremien müssen Chancen gezielt fördern und Risiken aktiv steuern: durch klare Governance-Strukturen, Investitionen in Kompetenzen, ethische Leitlinien und ein begleitendes Change Management. Nur so lässt sich das volle Potenzial von KI nutzen – verantwortungsvoll, sicher und zukunftsgerichtet.

4. Technische und Organisatorische Sicherheitsmaßnahmen (TOMs) - Ein Überblick und wichtige Quellen

Mit der zunehmenden Digitalisierung und dem Einsatz datengetriebener Technologien wie KI steigt die Bedeutung wirksamer Sicherheitsmaßnahmen. Technische und Organisatorische Maßnahmen (TOMs) bilden das Fundament für den Schutz sensibler Unternehmens- und Kundendaten – und damit für Vertrauen, Compliance und Resilienz.

Zwei zentrale Dimensionen:

1. Organisatorische Maßnahmen

Strukturen, Prozesse und Verantwortlichkeiten schaffen die Basis:

- Klare Richtlinien und Rollen für Informationssicherheit
- Schulungen zur Sensibilisierung von Mitarbeitenden
- Zugriffskontrolle, Incident- & Krisenmanagement
- Sicherheitsvorgaben für Dienstleister (z. B. Cloud-Anbieter)

2. Technische Maßnahme

Schutz durch Technologieeinsatz:

- Netzwerkschutz, Verschlüsselung, Zugriffssicherung (z. B. MFA)
- Backup- und Recovery-Konzepte
- Monitoring, Schwachstellenmanagement und regelmäßige Tests

Maßgebliche Standards & Rahmenwerke

- **BSI IT-Grundschutz (Deutschland)**: Praxisorientierte Leitlinien des Bundesamts für Sicherheit in der Informationstechnik
- **ISO/IEC 27001**: Internationaler Standard für Informationssicherheitsmanagement
- **ISO/IEC 42001:** Internationaler Standard für KI-Management
- **DSGVO (EU)**: Verlangt „angemessene“ technische und organisatorische Maßnahmen zum Datenschutz
- **Branchenstandards (z. B. KRITIS, Medical Device Regulation [MDR], IT-Sicherheitsgesetz)**: Je nach Sektor spezifisch zu beachten

Empfehlung an Unternehmensleitungen & Aufsichtsgremien

- **Verankern Sie Informationssicherheit strategisch:** Sie ist kein IT-Thema, sondern Teil der Unternehmensverantwortung.
- **Stellen Sie kritische Fragen:** Kennen wir unsere größten Cyber-Risiken? Sind Verantwortlichkeiten und Budgets klar geregelt? Gibt es regelmäßige Audits und Notfallpläne?
- **Führen Sie über Kultur:** Fördern Sie eine Sicherheitskultur – von oben nach unten.

Fazit

TOMs sind kein technisches Detail, sondern ein strategisches Führungsinstrument. Wer (Cyber-)Sicherheit als Führungsaufgabe versteht, stärkt nicht nur die Resilienz des Unternehmens bzw. der Organisation, sondern schützt auch Reputation, Marktposition und Haftungsebene.

5. Wichtige Institutionen im KI-Gesundheitswesen

Orientierungshilfe für Unternehmensleitungen und Aufsichtsgremien

Der Einsatz von KI im Gesundheitswesen erfordert neben technischer Expertise auch regulatorisches und strategisches Know-how. Verschiedene Institutionen bieten hierzu wertvolle Unterstützung.

Zentrale Ansprechpartner:

- **BSI (Bundesamt für Sicherheit in der Informationstechnik):**
  Nationale Cyber-Sicherheitsbehörde. Relevante Leitlinien zur IT- und KI-Sicherheit – insbesondere für Betreiber kritischer Infrastrukturen (z. B. Kliniken).
- **gematik GmbH:**
  Verantwortlich für die Telematikinfrastruktur (TI) im Gesundheitswesen. Schlüsselakteur für Interoperabilität und sichere Datenverarbeitung bei KI-Anwendungen.
- **BfArM (Bundesinstitut für Arzneimittel und Medizinprodukte):**
  Zuständig für Zulassungsfragen bei KI-basierten Medizinprodukten. Wichtig für regulatorische Klarheit im Bereich MDR.
- **DKG (Deutsche Krankenhausgesellschaft):**
  Interessensvertretung der Krankenhäuser. Praxisnahe Perspektive für die Einführung neuer Technologien in Klinikstrukturen.
- **KBV (Kassenärztliche Bundesvereinigung):**
  Relevanter Partner für die ambulante Versorgung. Bringt Perspektive niedergelassener Ärztinnen und Ärzte in die Diskussion zur Digitalisierung und KI ein.
- **acatech (Deutsche Akademie der Technikwissenschaften):**
  Strategischer Think Tank. Bietet wissenschaftlich fundierte Empfehlungen zu Technologieeinsatz und ethischen Rahmenbedingungen.
- **KI Park Deutschland e. V. & Forschungszentren:**
  Netzwerke und Kompetenzzentren (z. B. DFKI), die Zugang zu Know-how, Partnern und Forschung im Bereich KI bieten.
- **Landesdatenschutzbeauftragte:**
  Wichtige Ansprechpartner bei Fragen zur DSGVO-konformen Verarbeitung sensibler Gesundheitsdaten.

Empfehlung an Führungsgremien

- Nutzen Sie diese Institutionen nicht nur als Informationsquelle, sondern aktiv im Dialog.
- **Warum es sich lohnt:**
  - Frühzeitige Einbindung erleichtert Compliance
  - Bessere Einschätzung regulatorischer Entwicklungen
  - Zugang zu Wissen, Netzwerken und Best Practices

Fazit

Der Austausch mit diesen Stellen stärkt strategische Entscheidungsfähigkeit und ermöglicht einen sicheren und zukunftsfähigen KI-Einsatz im Gesundheitswesen.

6. KI-Strategie im Unternehmen: Leitlinien für Führung und Aufsicht

Der gezielte Einsatz von KI erfordert eine unternehmens- bzw. organisationsspezifische Strategie, die Chancen und Risiken klar adressiert. Für Unternehmensleitungen und Aufsichtsgremien ist dies eine zentrale Führungsaufgabe.

1. Ziele und Anwendungsfelder definieren

- **Frage:** Was soll KI im Unternehmen bewirken – Effizienzsteigerung, neue Services, bessere Entscheidungsfindung?
- **Fokus:** Identifizieren Sie prioritäre Bereiche (z. B. Medizin, Verwaltung, Vertrieb), in denen KI echten Mehrwert stiften kann.
- **Relevanz:** Eine klare Zieldefinition schafft strategische Orientierung und verhindert isolierte Einzelinitiativen.

2. Regulatorische Anforderungen frühzeitig prüfen

- **DSGVO:** Datenschutz bei Datennutzung und Modelltraining ist zwingend.
- **EU AI Act:** Kommende Vorschriften zu Transparenz, Risikoklassifikation und menschlicher Aufsicht.
- **MDR:** Gilt für KI-Anwendungen im medizinischen Bereich.
- **Führungspflicht:** Proaktive Compliance schützt vor rechtlichen, finanziellen und Reputationsrisiken.

3. Risiken analysieren – Stakeholder einbinden

- **Risiken:** Technische Fehler, ethische Probleme (Bias, Intransparenz), Change-Probleme oder fehlender ROI.
- **Stakeholder:** Frühzeitige Einbindung von Mitarbeitenden, Patientenvertretungen und anderen relevanten Gruppen.
- **Nutzen:** Akzeptanz schaffen, Perspektiven integrieren, Risiken früh adressieren.

4. Integration in bestehende Systeme

- **ISMS (z. B. ISO 27001):** Absicherung der KI-Systeme gegen Cyberbedrohungen.
- **AIMS (ISO 42001):** KI-Anwendungen organisationsweit in ein ganzheitliches KI-Management integrieren.
- **QMS (z. B. ISO 9001 / ISO 13485):** Qualität und Nachvollziehbarkeit von KI-Outputs sichern.
- **Datenschutzmanagement:** DPIA, Privacy by Design – unverzichtbar bei personenbezogenen Daten.
- **Ziel:** KI nicht isoliert betreiben, sondern sicher, compliant und effizient im Unternehmen verankern.

Fazit

Eine KI-Strategie ist Führungsaufgabe. Sie muss rechtliche, technologische und organisatorische Aspekte verbinden. Nur so lassen sich Wertschöpfungspotenziale heben und Risiken beherrschbar machen. Aufsichtsgremien kommt dabei eine wichtige Rolle in der strategischen Kontrolle und Begleitung zu.

7. Überblick: Der EU Artifical Intelligence Act (EU AI Act) für Unternehmensleitungen und Aufsichtsgremien

Der EU AI Act schafft erstmals einen verbindlichen Rechtsrahmen für den Einsatz von KI in Europa. Ziel ist es, Innovation zu ermöglichen und gleichzeitig Risiken für Gesundheit, Sicherheit und Grundrechte zu begrenzen.

Zentrales Prinzip: Risikobasierter Ansatz

Je höher das Risiko einer KI-Anwendung, desto strenger die regulatorischen Anforderungen. Unternehmen müssen ihre KI-Anwendungen einer dieser vier Kategorien zuordnen:

Verbotene KI (inakzeptables Risiko) **Beispiele:** Social Scoring, Echtzeit-Biometrie im öffentlichen Raum, manipulative Systeme **Konsequenz:** Diese Anwendungen sind in der EU grundsätzlich verboten.	**Hochrisiko-KI** **Beispiele:** KI in Gesundheitswesen, HR (Recruiting, Bewertung), Kritis, Bildung, Finanzwesen **Anforderungen:** ○ Risikomanagement ○ Datenqualität & -governance ○ Transparenz und menschliche Aufsicht ○ Cybersicherheit ○ Konformitätsbewertung vor Markteintritt **Konsequenz:** Erhebliche Anforderungen an Compliance, Prozesse und Dokumentation.
Begrenztes Risiko **Beispiele:** Chatbots, Deepfakes **Pflicht:** Nutzer müssen über KI-Einsatz informiert werden (Transparenzkennzeichnung).	**Minimales Risiko** **Beispiele:** Spamfilter, Empfehlungssysteme **Pflicht:** Keine gesetzlichen Vorgaben, freiwillige Standards empfohlen.

Implikationen für Unternehmensleitungen & Aufsichtsgremien

- **Strategischer Handlungsbedarf:** Identifizieren Sie frühzeitig Hochrisiko-KI in Ihren Geschäftsprozessen.
- **Investitionen in Compliance:** Rechnen Sie mit Ressourcenbedarf für Datenschutz, IT-Sicherheit, Risiko- & Qualitätsmanagement.
- **Governance-Rolle:** Begleiten Sie aktiv die Entwicklung und Nutzung von KI – unter Einbezug von IT, Recht und Fachbereichen.
- **Vertrauen & Marktposition:** Frühzeitige und transparente Umsetzung schafft Vertrauen und kann ein klarer Wettbewerbsvorteil sein.

Fazit

Der EU AI Act ist keine reine IT-Regelung, sondern ein strategischer Ordnungsrahmen mit klarer Relevanz für Führung und Aufsicht. Jetzt ist der richtige Zeitpunkt, die Weichen im Unternehmen zu stellen.

8. KI-Projekte im Unternehmen: Governance und Umsetzung im Überblick

Nach der strategischen Ausrichtung ist für die Unternehmensführung entscheidend, dass klare Leitplanken für die Umsetzung von KI-Projekten bestehen. Dazu gehören verbindliche Governance-Vorgaben und Checklisten, um Risiken zu beherrschen, Compliance zu sichern und den Projekterfolg zu gewährleisten.

1. Governance-Vorgaben: Führung und Kontrolle von KI-Projekten

- **Verantwortlichkeiten festlegen:**
  Benennen Sie Verantwortliche für KI auf Management-Ebene (z. B. CIO, Chief AI Officer) und etablieren Sie interdisziplinäre Gremien.
- **Genehmigungsprozesse definieren:**
  Legen Sie fest, welche KI-Projekte einer Freigabe durch welche Instanzen bedürfen.
- **Ethische Leitlinien verankern:**
  Formulieren Sie Grundsätze zu Fairness, Transparenz, Nichtdiskriminierung und menschlicher Kontrolle.
- **Risikomanagement integrieren:**
  Verknüpfen Sie KI-spezifische Risikoanalysen mit dem Unternehmensrisikomanagement.
- **Dokumentation sicherstellen:**
  Klare Vorgaben zu Nachvollziehbarkeit und Transparenz – insbesondere bei Hochrisiko-KI.
- **Compliance-Checks & Audits:**
  Planen Sie regelmäßige Überprüfungen der Einhaltung von EU AI Act, DSGVO & Co.

2. Checklisten: Praktisches Instrument für Projektsteuerung

Checklisten sorgen dafür, dass keine zentralen Anforderungen übersehen werden – insbesondere bei Hochrisiko-KI.

Wichtige Prüfpunkte (Auswahl):

- Ist der Nutzen des KI-Einsatzes klar definiert?
- Liegen geeignete, rechtskonforme Trainingsdaten vor?
- Wurde Bias geprüft und reduziert?
- Sind Kontrollmechanismen zur menschlichen Aufsicht eingeplant?
- Gibt es Prozesse für Monitoring, Wartung und ggf. Deaktivierung?

Fazit

Governance-Vorgaben und Checklisten sind kein operatives Detail, sondern ein zentrales Führungsinstrument. Sie ermöglichen strategische Kontrolle, minimieren rechtliche und ethische Risiken und sorgen dafür, dass KI-Initiativen tatsächlich Mehrwert schaffen – verantwortungsvoll und regelkonform. Fordern Sie deren konsequente Implementierung – und lassen Sie sich regelmäßig über den Status berichten.

9. Marktüberblick: KI-basierte Cybersicherheitslösungen

Strategischer Schutz in der digitalen Transformation

KI wird zum Schlüsselinstrument moderner Cybersicherheit. Sie ermöglicht es Unternehmen, komplexe Angriffe frühzeitig zu erkennen, schneller zu reagieren und Sicherheitsressourcen effizienter einzusetzen.

Warum KI in der Cybersicherheit unverzichtbar ist

- **Erkennung unbekannter Bedrohungen:** KI identifiziert Muster und Anomalien in Echtzeit – auch bei Zero-Day-Angriffen.
- **Automatisierte Reaktion:** Systeme können infizierte Geräte isolieren oder IPs blockieren – innerhalb von Millisekunden.
- **Weniger Fehlalarme:** KI reduziert "Alarmmüdigkeit", indem sie zwischen echten Angriffen und harmlosen Vorgängen unterscheidet.
- **Effizienz im Security Operations Center (SOC):** KI priorisiert Warnungen, automatisiert Analysen und unterstützt menschliche Experten.
- **Prävention:** KI erkennt potenzielle Bedrohungen frühzeitig durch Mustererkennung aus historischen Daten.

Marktsegmente & Anbieter (Auswahl)

Anwendungsfeld	Zweck	Beispiele
EDR/XDR (Endgeräte & Netzwerk)	Angriffe erkennen & stoppen	– CrowdStrike – SentinelOne – Microsoft Defender
Netzwerkanalyse	Anomalien im Datenverkehr	– Cisco Secure Analytics – Darktrace – Vectra AI
Next-Gen SIEM	Sicherheitsdaten korrelieren & analysieren	– Splunk – IBM QRadar – Google Chronicle
Threat Intelligence	Globale Bedrohungsdaten analysieren	– Recorded Future
E-Mail-Sicherheit	Phishing & BEC erkennen	– Proofpoint – Microsoft

Implikationen für Unternehmensleitungen & Aufsichtsgremien

- **Cybersicherheit ist Führungsaufgabe:** Die zunehmende Komplexität der Bedrohungslage verlangt eine strategische Einbindung von KI in die Sicherheitsarchitektur.
- **Investition in Resilienz:** KI-Lösungen bedeuten nicht nur Schutz, sondern sind auch ein Wettbewerbsvorteil.
- **Transparenz & Kontrolle:** Achten Sie auf erklärbare KI (Explainable AI, XAI), um Entscheidungen nachvollziehbar zu halten.
- **Integration statt Insellösungen:** Die Lösungen sollten modular integrierbar sein und bestehende Systeme ergänzen.
- **Fachkräfte weiterentwickeln:** Menschen bleiben entscheidend – KI ist ein Werkzeug, kein Ersatz.

Fazit

KI-basierte Sicherheitslösungen sind essenziell, um Ihr Unternehmen bzw. Ihre Organisation resilient gegenüber heutigen und zukünftigen Cyberbedrohungen aufzustellen. Für Führungskräfte heißt das: Jetzt die Weichen für Investitionen, Governance und Integration stellen.

10. Fazit und Empfehlungen: KI als strategischer Kompass für Unternehmensleitungen und Aufsichtsgremien

KI ist heute keine Zukunftsvision mehr, sondern eine transformative Kraft, die Geschäftsmodelle und insbesondere das Gesundheitswesen grundlegend verändert. Für Unternehmensleitungen und Aufsichtsräte bedeutet das: Jetzt handeln, um Chancen zu nutzen und Risiken zu steuern.

Kernbotschaft

KI ist ein strategisches Imperativ. Wer nicht aktiv wird, verliert Wettbewerbsfähigkeit. Effizienzsteigerung, Innovation und verbesserte Patientenversorgung sind erreichbar – aber nur mit verantwortungsvollem Umgang, Compliance und Datensicherheit.

Empfehlungen für die nächsten Schritte

1. KI als Top-Management-Thema etablieren

- KI-Initiativen gehören auf die Führungsebene, nicht nur in die IT.
- Benennen Sie einen KI-Verantwortlichen oder Lenkungsausschuss.
- Halten Sie sich kontinuierlich über Entwicklungen und Regularien auf dem Laufenden.

2. Unternehmensspezifische KI-Roadmap entwickeln

- Identifizieren Sie konkrete Anwendungsfälle mit hohem Mehrwert.
- Berücksichtigen Sie frühzeitig Risiken, insbesondere Hochrisiko-KI gemäß EU AI Act.

3. Gezielt in Daten, Sicherheit und Kompetenz investieren

- Datenqualität und Governance als Grundlage jeder KI.
- Stärken Sie Cybersicherheitsmaßnahmen zum Schutz Ihrer KI-Systeme.
- Steigern Sie die Akzeptanz innerhalb des Transformationsprozesses durch aktive Weiterbildungs- und Sensibilisierungsmaßnahmen.

4. Governance und Compliance proaktiv gestalten

- Klare Verantwortlichkeiten entlang des KI-Lebenszyklus definieren.
- KI als ganzheitlichen Ansatz in bestehende Managementsysteme (ISMS, QMS) integrieren.
- Transparente und ethische Kommunikation sicherstellen.

Die Einführung von KI ist ein langfristiger Prozess, der strategische Weitsicht, Anpassungsfähigkeit und aktives Leadership erfordert. Setzen Sie jetzt die richtigen Prioritäten, um Ihr Unternehmen bzw. Ihre Organisation erfolgreich in die digitale Zukunft zu führen.

11. Checkliste für Geschäftsleitungen, Beiräte und Aufsichtsräte

Diese Checkliste hilft Führungsgremien dabei, eine fundierte Beurteilung über den KI-Einsatz im Unternehmen vorzunehmen und Verantwortlichkeiten strategisch zu verankern.

1. Strategische Verankerung

- ☐ Gibt es eine definierte Unternehmensstrategie zum Einsatz von KI?
- ☐ Wurden Ziele, Nutzen und Grenzen des KI-Einsatzes klar formuliert?
- ☐ Wurde eine Risikobewertung für die relevanten Anwendungsfelder durchgeführt?

2. Governance & Verantwortlichkeiten

- ☐ Ist eine übergreifende Steuerungsstruktur für KI-Fragen eingerichtet (z. B. KI-Steuerungsgremium)?
- ☐ Gibt es benannte Verantwortliche für Datenschutz, IT-Sicherheit und medizinische Qualität im Kontext von KI?
- ☐ Sind Geltungsbereich und Auswirkungen auf die Organisationsstrukturen (Business Impact) durch den KI-Einsatz ausreichend geplant und berücksichtigt?
- ☐ Besteht ein Eskalationsmechanismus bei sicherheitskritischen oder ethisch heiklen Entscheidungen?

3. Rechtliche & regulatorische Konformität

- ☐ Wurde eine Bewertung der eingesetzten KI-Systeme nach dem EU AI Act vorgenommen?
- ☐ Liegen Datenschutz-Folgenabschätzungen (DSFA) für KI-Anwendungen vor?
- ☐ Ist die Einhaltung von MDR, DSGVO und branchenspezifischen Sicherheits-standards (z. B. B3S) gewährleistet?

4. Technische und organisatorische Maßnahmen

- ☐ Sind technische Schutzmaßnahmen (Modellüberwachung, Logging, Zugangskontrolle) implementiert?
- ☐ Ist die KI-Anwendung in das bestehende ISMS integriert?
- ☐ Gibt es ein Incident-Response-Konzept für KI-Fehlfunktionen?

5. Transparenz & Nachvollziehbarkeit

- ☐ Werden betroffene (Mitarbeitende, Kunden, Patienten) ausreichend über den Einsatz von KI informiert?
- ☐ Werden Entscheidungen der KI-Systeme für medizinisches Personal und Patienten nachvollziehbar dokumentiert?
- ☐ Besteht ein Verfahren zur regelmäßigen Validierung der KI-Modelle (Bias, Aktualität, Relevanz)?

6. Markt- und Partnerprüfung

- ☐ Wurden die Anbieter auf Vertrauenswürdigkeit und Konformität geprüft (Zertifikate, Referenzen, Sicherheitsstandards)?
- ☐ Liegt ein Nachweis über eine dokumentierte Konformitätsbewertung bei Hochrisiko-KI vor?

7. Mitarbeiterqualifizierung

- ☐ Gibt es Schulungen für den Umgang mit KI-Tools im medizinischen und administrativen Kontext?
- ☐ Ist die Belegschaft in die Einführung und Nutzung der Systeme eingebunden (Change Management)?

12. Template zur Erstellung einer internen KI-Strategie

1. Einleitung

- Motivation und Ziele des Unternehmens beim Einsatz von KI
- Bedeutung von KI für Innovation, Effizienz und Patientenversorgung

2. Anwendungsbereiche

- Office-IT (z. B. Automatisierung, Textverständnis)
- Klinische Nutzung (z. B. Bilddiagnostik, Anamnese-Tools)
- Forschung & Entwicklung (z. B. KI-gestützte Studienauswertung)

3. Bewertung der Chancen und Risiken

- Chancen: Qualitätssteigerung, Zeitgewinn, Kosteneffizienz
- Risiken: Datenschutz, Fehlinterpretationen, regulatorische Haftung

4. Regulatorischer Rahmen

- Anwendung des EU AI Acts: Einstufung der genutzten KI-Systeme
- Berücksichtigung der DSGVO, MDR, B3S, ISO 42001

5. Governance-Struktur

- Benennung einer KI-Verantwortung (z. B. "KI-Koordinator")
- Gremienstruktur und Reportinglinien

6. Technische und organisatorische Maßnahmen

- Schutzmaßnahmen gegen Manipulation, Fehlfunktionen und Datenabfluss
- Integration in bestehende Sicherheits- und QM-Systeme

7. Beschaffung und Marktanalyse

- Kriterienkatalog für KI-Produkte
- Due-Diligence-Prüfung der Anbieter

8. Kommunikation und Akzeptanz

- Transparente Kommunikation gegenüber Mitarbeitenden und Patienten
- Interne Schulungs- und Fortbildungsprogramme

9. Überprüfung und Weiterentwicklung

- Regelmäßige Reviews der KI-Nutzung
- Anpassung an technologische und regulatorische Entwicklungen