Datensicherheit und KI im Mittelstand: Herausforderungen und Best Practices

Empfehlungen für Mittelstandsunternehmen

von

Prof. Dr. Gerald Lembke

1. Worum geht es?

Die Digitalisierung und der Einsatz von Künstlicher Intelligenz (KI) eröffnen Unternehmen völlig neue Möglichkeiten, Prozesse zu optimieren, innovative Produkte und Dienstleistungen anzubieten und wettbewerbsfähiger zu werden. Insbesondere für den Mittelstand, der häufig mit knappen Ressourcen zu kämpfen hat, können KI-Systeme einen entscheidenden Wettbewerbsvorsprung bedeuten.

Allerdings ist die Nutzung von KI auch mit erheblichen Risiken und Herausforderungen verbunden, vor allem im Bereich der Datensicherheit. KI-Anwendungen basieren auf der Verarbeitung enormer Datenmengen, darunter häufig auch sensible Kunden- und Mitarbeiterdaten. Ein unsachgemäßer Umgang mit diesen Daten kann zu Datenlecks, Cyberangriffen und Verstößen gegen Datenschutzbestimmungen wie die DSGVO führen - mit gravierenden rechtlichen und finanziellen Konsequenzen für die Unternehmen.

Dieser Beitrag beleuchtet die zentralen Herausforderungen bei Datensicherheit und KI im Mittelstand und zeigt anhand von Best Practices und Praxisbeispielen auf, wie Unternehmen diese Hürden überwinden und die Chancen von KI bei gleichzeitiger Minimierung der Risiken nutzen können. Neben technischen und organisatorischen Maßnahmen wird auch auf den Aufbau einer Datenschutzkultur und die Qualifizierung von Mitarbeitern eingegangen. Abgerundet wird der Beitrag durch konkrete Handlungsempfehlungen für Mittelständler.

2. Herausforderungen bei Datensicherheit und KI

Es lassen sich folgende zentrale Herausforderungen bei Datensicherheit und KI im Mittelstand identifizieren:

<u>Mangelnde Datenbasis und -qualität</u>

Für den erfolgreichen Einsatz von KI-Systemen, insbesondere im Machine Learning, ist eine ausreichende Menge an qualitativ hochwertigen Trainingsdaten erforderlich. Viele mittelständische Unternehmen erfassen alle Arten von Daten ohne diese aus Datenschutzperspektive zu differenzieren. Sie sind Stammdaten von Mitarbeiter schützenswert während Fotos von der letzten Weihnachtsfeier weniger schützenswert sind. Bei den benötigten Datenmengen geht es neben der erforderlichen Qualität um Datensensibilitäten.

<u>Fehlende Fachkenntnisse und Ressourcen</u>

Der Aufbau von KI-Kompetenzen erfordert spezialisierte Fachkenntnisse sowie personelle und finanzielle Ressourcen, auch über die Datensensibilität. Hier sind die KMU oft nicht ausreichend ausgestattet. Es mangelt an qualifizierten Data Scientists, KI-Entwicklern und IT-Sicherheitsexperten. Zudem fehlen häufig die Mittel für Investitionen in die erforderliche Hard- und Software sowie Weiterbildungsmaßnahmen.

Bedenken bezüglich Datenschutz und Cybersicherheit

Die Nutzung von KI-Systemen ist oft mit der Verarbeitung sensibler Daten wie Kunden- oder Mitarbeiterdaten verbunden. Dies birgt erhebliche Risiken im Hinblick auf Datenschutz und Cybersicherheit. KMU haben häufig unzureichende Sicherheitsmaßnahmen implementiert und verfügen nicht über die nötige Expertise, um Datenlecks, Hackerangriffe oder Verstöße gegen die DSGVO wirksam zu verhindern.

Hohe Kosten für KI-Datensicherheit

Die Einführung von KI-Sicherheitssystemen ist mit immensen Anfangsinvestitionen verbunden - sowohl für die Beschaffung der erforderlichen Technologien als auch für den Kompetenzaufbau. Gerade für finanzschwache KMU können diese hohen Kosten eine große Hürde darstellen. Zudem ist der Return on Investment oft schwer abzuschätzen, was viele Unternehmen zögern lässt.

Diese Herausforderungen zeigen, dass KMU beim Einsatz von KI vor großen Hürden stehen. Ohne geeignete Gegenmaßnahmen und Unterstützung drohen sie im Wettbewerb abgehängt zu werden. Entsprechende Best Practices und Lösungsansätze sind daher dringend erforderlich.

3. Best Practices zum Schutz sensibler Daten

Es lassen sich folgende Best Practices für den Schutz sensibler Daten in mittelständischen Unternehmen in der mittelständischen Wirtschaftspraxis identifizieren:

Umsetzung von Privacy by Design und Privacy by Default

Der Datenschutz muss bereits bei der Entwicklung von Produkten, Dienstleistungen und Prozessen von Anfang an mitgedacht werden (Privacy by Design). Mittelständler sollten Datenschutzaspekte frühzeitig in die Planungs- und Konzeptionsphase einbeziehen und technische sowie organisatorische Maßnahmen (TOMs) ergreifen, um Risiken zu minimieren. Dazu gehören beispielsweise:

- Datenminimierung durch Anonymisierung und Pseudonymisierung
- Verschlüsselung sensibler Daten
- Zugriffskontrolle und Berechtigungskonzepte
- Transparenz über Datenverarbeitungsvorgänge

Zudem sollten datenschutzfreundliche Voreinstellungen (Privacy by Default) die Standardeinstellung sein, sodass Daten nur auf Basis aktiver Entscheidungen verarbeitet werden.

Risikomanagement und Datenschutz-Folgenabschätzung

Mittelständler müssen Risiken im Zusammenhang mit der Verarbeitung sensibler Daten systematisch analysieren und bewerten. Eine Datenschutz-Folgenabschätzung (DSFA) ist bei Hochrisiko-Verarbeitungen gesetzlich vorgeschrieben und sollte frühzeitig durchgeführt werden. Dabei sind mögliche Gefahren wie Datenlecks, Datenmissbrauch oder Compliance-Verstöße zu identifizieren und Gegenmaßnahmen zu planen.

Aufbau von Datenschutz- und IT-Sicherheitskompetenzen

Viele Mittelständler haben Defizite bei Datenschutz- und IT-Sicherheitskompetenzen. Durch gezielte Weiterbildungen, Zertifizierungen und die Einstellung von Experten müssen diese Fähigkeiten aufgebaut werden. Zudem ist eine enge Zusammenarbeit zwischen Datenschutzbeauftragten, IT-Sicherheitsverantwortlichen und Fachbereichen erforderlich.

Sensibilisierung und Schulung der Mitarbeiter

Die Mitarbeiter sind oft die "schwächste Glieder" in Sachen Datensicherheit. Regelmäßige Schulungen zu Themen wie Passwortsicherheit, Phishing-Erkennung und Umgang mit sensiblen Daten sind essenziell. Zudem muss eine Kultur der Sicherheit und Wertschätzung von Daten geschaffen werden.

Technische Sicherheitsmaßnahmen

Mittelständler müssen in moderne Sicherheitstechnologien investieren, um Daten effektiv zu schützen:

- Firewalls und Zugriffskontrolle
- Verschlüsselung von Daten in Übertragung und Ruhezustand
- Backup- und Wiederherstellungskonzepte
- Kontinuierliches Monitoring und Schwachstellenanalysen
- Endpoint-Sicherheit für mobile Geräte

Auditierung und kontinuierliche Verbesserung

Datenschutz und Datensicherheit sind kontinuierliche Prozesse. Regelmäßige Audits, Penetrationstests und die Auswertung von Vorfällen sind nötig, um Schwachstellen zu erkennen. Zudem müssen Sicherheitskonzepte und Maßnahmen ständig an neue Bedrohungen und Technologien angepasst werden.

Durch die Umsetzung dieser Best Practices können Mittelständler die Sicherheit sensibler Daten deutlich erhöhen und mögliche Compliance-Verstöße, Bußgelder sowie Vertrauensverluste bei Kunden vermeiden. Allerdings erfordert dies erhebliche Investitionen in Technologie, Prozesse und Kompetenzen.

4. Erfolgsfaktoren und Praxisbeispiele für Mittelstandsunternehmen

Auf Grund eigener Erfahrungen lassen sich folgende zentrale Erfolgsfaktoren und Best Practices für den Schutz sensibler Daten und Mitarbeiterdaten in mittelständischen Unternehmen identifizieren:

Aufbau einer Datenschutzkultur und Mitarbeitersensibilisierung

Eine der wichtigsten Voraussetzungen ist der Aufbau einer Datenschutzkultur im Unternehmen. Alle Mitarbeiter müssen für das Thema sensibilisiert und geschult werden, damit ein verantwortungsvoller Umgang mit Daten zur Selbstverständlichkeit wird. Regelmäßige Schulungen, klare Richtlinien und eine offene Kommunikation sind hier zentral.

Klare Rollen, Prozesse und Dokumentation

Es müssen klar definierte Rollen, Verantwortlichkeiten und Prozesse für den Datenschutz geschaffen werden. Dazu gehören ein Berechtigungs- und Löschkonzept, Verfahrensanweisungen sowie eine lückenlose Dokumentation aller Verarbeitungstätigkeiten.

Technische und organisatorische Maßnahmen

Neben organisatorischen Maßnahmen sind auch technische Sicherheitsvorkehrungen zum Schutz sensibler Daten erforderlich. Dazu zählen Verschlüsselung, Zugriffskontrolle, Firewalls, Backups sowie Schwachstellenanalysen und Monitoring.

Risikomanagement und Datenschutz-Folgenabschätzung

Mittelständler müssen Risiken im Zusammenhang mit der Datenverarbeitung systematisch analysieren und bewerten. Eine Datenschutz-Folgenabschätzung ist bei Hochrisiko-Verarbeitungen gesetzlich vorgeschrieben.

Auswahl vertrauenswürdiger IT-Partner

Gerade für den Mittelstand ist es oft sinnvoll, externe Experten wie Datenschutzbeauftragte oder IT-Sicherheitsdienstleister einzubinden. Bei der Auswahl ist jedoch höchste Sorgfalt geboten, um Datenlecks zu vermeiden.

Praxisbeispiele für Best Practices

- Das Maschinenbauunternehmen Ruhrbau nutzt ein Datenschutz-Managementsystem und hat einen externen Datenschutzbeauftragten bestellt. Mitarbeiter werden kontinuierlich geschult.

- Der Automobilzulieferer Marquardt hat eine Datenschutzorganisation aufgebaut und Prozesse für Risikobewertungen und Dokumentation implementiert.

- Die Stadtwerke Karlsruhe haben ein Informationssicherheits-Managementsystem nach ISO 27001 eingeführt mit Richtlinien, Rollen und technischen Kontrollen.

- Das Logistikunternehmen Dachser setzt auf Verschlüsselung, Zugriffskontrolle und Mitarbeiterschulungen zum Datenschutz.

Durch die Kombination technischer und organisatorischer Maßnahmen sowie eine starke Datenschutzkultur können Mittelständler die Sicherheit sensibler Daten deutlich erhöhen. Best Practices aus der Praxis zeigen, dass dies mit den richtigen Konzepten und Partnern gut umsetzbar ist.

5. Handlungsempfehlungen

Folgende zentrale Handlungsempfehlungen lassen sich für Datenschutz und KI im Mittelstand ableiten:

Aufbau einer Datenschutz- und KI-Governance

Mittelständler sollten frühzeitig eine Governance-Struktur für Datenschutz und KI-Nutzung aufbauen. Dazu gehören:

- Benennung eines Datenschutzbeauftragten und KI-Verantwortlichen
- Schaffung einer Datenschutzorganisation mit klaren Rollen und Prozessen
- Entwicklung einer Datenschutz- und KI-Strategie mit konkreten Zielen
- Einrichtung eines Risikomanagements und Kontrollen
- Kontinuierliches Monitoring und Audits

Eine solche Governance-Struktur stellt sicher, dass Datenschutz und KI-Aspekte von Anfang an mitgedacht und Compliance-Risiken minimiert werden.

Investition in Mitarbeiterqualifizierung

Der Kompetenzaufbau bei Mitarbeitern ist entscheidend. Mittelständler sollten in Schulungen und Weiterbildungen investieren:

- Grundlagen Datenschutz und Informationssicherheit
- Umgang mit Kundendaten und Mitarbeiterdaten
- Verständnis von KI-Technologien und Anwendungen
- Ethische und rechtliche Aspekte von KI

Nur mit qualifizierten und sensibilisierten Mitarbeitern lassen sich Datenschutz und KI-Systeme effektiv umsetzen.

Technische Sicherheitsmaßnahmen

Investitionen in moderne Sicherheitstechnologien sind unerlässlich:

- Verschlüsselung von Daten in Übertragung und Speicherung
- Zugriffskontrolle und Berechtigungskonzepte
- Firewalls und Netzwerksicherheit
- Endpoint-Sicherheit für mobile Geräte
- Kontinuierliches Monitoring und Penetrationstests

Mittelständler sollten Sicherheitsstandards wie ISO 27001 anwenden.

Aufbau einer Dateninfrastruktur

Eine solide Dateninfrastruktur ist Grundvoraussetzung für KI. Mittelständler müssen in folgende Bereiche investieren:

- Datenintegration aus verschiedenen Quellen
- Zentrale Datenhaltung und Datenqualitätsmanagement
- Analyseplattformen und KI-Werkzeuge
- Skalierbare Cloud-Infrastruktur für rechenintensive Anwendungen

Der Aufbau einer skalierbaren Dateninfrastruktur ist oft mit hohen Anfangsinvestitionen verbunden.

Kooperation mit Partnern und Experten

Viele Mittelständler haben nicht die erforderlichen Ressourcen. Daher ist die Zusammenarbeit mit externen Partnern sinnvoll:

- IT-Sicherheitsdienstleister und Managed Service Provider
- Beratungsunternehmen für Datenschutz und KI
- Universitäten und Forschungseinrichtungen
- Branchenverbände und Netzwerke

Durch die Einbindung von Experten lassen sich Kompetenzen und Best Practices effizient nutzen.

Kontinuierliche Verbesserung und Anpassung

Datenschutz und KI sind dynamische Themen. Mittelständler müssen Prozesse für kontinuierliche Verbesserung implementieren:

- Regelmäßige Risikobewertungen und Kontrollen
- Anpassung an neue Technologien, Bedrohungen und Regularien
- Lessons Learned aus Vorfällen und Fehlern
- Einbindung von Mitarbeiterfeedback

Nur wer am Puls der Zeit bleibt, kann Datenschutz und KI-Nutzung auf Dauer sicherstellen.

Durch die Umsetzung dieser Handlungsempfehlungen können Mittelständler die Chancen von KI voll ausschöpfen und gleichzeitig Datenschutzrisiken minimieren. Allerdings erfordert dies erhebliche Investitionen in Technologie, Prozesse und Kompetenzen - eine Herausforderung für viele KMU.

6. Fazit

Der Einsatz von Künstlicher Intelligenz (KI) bietet gerade für den Mittelstand enorme Chancen, Prozesse zu optimieren, innovative Produkte und Dienstleistungen zu entwickeln und wettbewerbsfähiger zu werden. Allerdings ist die Nutzung von KI-Systemen auch mit erheblichen Risiken und Herausforderungen im Bereich der Datensicherheit verbunden.

Die Verarbeitung sensibler Daten wie Kunden- und Mitarbeiterdaten durch KI-Anwendungen birgt die Gefahr von Datenlecks, Cyberangriffen und Verstößen gegen Datenschutzbestimmungen. Viele mittelständische Unternehmen haben Defizite bei Datenschutz- und IT-Sicherheitskompetenzen sowie unzureichende technische Schutzmaßnahmen implementiert. Zudem mangelt es häufig an qualifizierten Fachkräften und finanziellen Ressourcen für Investitionen in diesem Bereich.

Um die Potenziale von KI voll auszuschöpfen und gleichzeitig Datenschutzrisiken zu minimieren, müssen Mittelständler eine Reihe von Maßnahmen ergreifen. Dieser Beitrag hat zentrale Best Practices sowie organisatorische und technische Handlungsempfehlungen aufgezeigt. Der Schlüssel liegt in der Schaffung einer Datenschutz-Governance, dem Kompetenzaufbau bei Mitarbeitern, Investitionen in Sicherheitstechnologien und Infrastrukturen sowie der kontinuierlichen Verbesserung von Prozessen.

7. Quellen

1. Bitkom (2022). Leitfaden Künstliche Intelligenz im Mittelstand. https://www.bitkom.org/leitfaden-ki-mittelstand

2. Dachser (2019). Technische Sicherheitsmaßnahmen zum Datenschutz. Internes Whitepaper.

3. Datenschutzexperte.de (2023). ChatGPT & Datenschutz: Risiken und Herausforderungen. https://www.datenschutzexperte.de/blog/datenschutz-im-unternehmen/chatgpt-datenschutz/

4. Deloitte (2021). Studie: Künstliche Intelligenz im Mittelstand 2021. https://www2.deloitte.com/de/de/pages/technology/articles/ki-im-mittelstand.html

5. DSGVO.EXPERTENgruppe (2020). Whitepaper: Datenschutz und KI. https://www.dsgvo-experten.de/whitepaper/datenschutz-ki/

6. Fraunhofer IESE (2023). Leitfaden: Datenschutz bei KI-Systemen. https://www.iese.fraunhofer.de/datenschutz-ki-leitfaden.html

7. Kompetenzzentrum Kommunikation (2022). Künstliche Intelligenz (KI) für den Mittelstand. https://www.kompetenzzentrum-kommunikation.de/artikel/kuenstliche-intelligenz-ki-fuer-den-mittelstand-3484/

8. Lembke, G. (2024). KI in Unternehmen erfolgreich einführen. https://gerald-lembke.de/ki-einfuehren-unternehmen/

9. Lembke, G. (2024). KI-Toolparty.de - Regelmäßige Updates zum KI-Einsatz in Mittelstandsunternehmen. https://KI-Toolparty.de

10. Lembke, G. & Meil, C. (2022). Smartes Marketing mit Künstlicher Intelligenz. Verlag Neue Wirtschaftsbriefe.

11. Marquardt (2021). Datenschutz bei Marquardt. Internes Whitepaper.

12. Mittelstand-Digital (2022). Webinar: Künstliche Intelligenz und Datensicherheit für KMU. https://www.mittelstand-digital.de/webinare/ki-datensicherheit.html

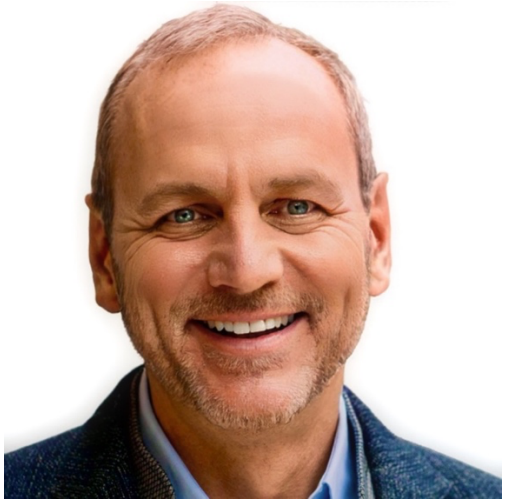
13. Ruhrbau (2022). Datenschutz-Managementsystem bei Ruhrbau. Internes Dokument.

14. Stadtwerke Karlsruhe (2020). Informationssicherheits-Managementsystem nach ISO 27001. Interner Bericht.

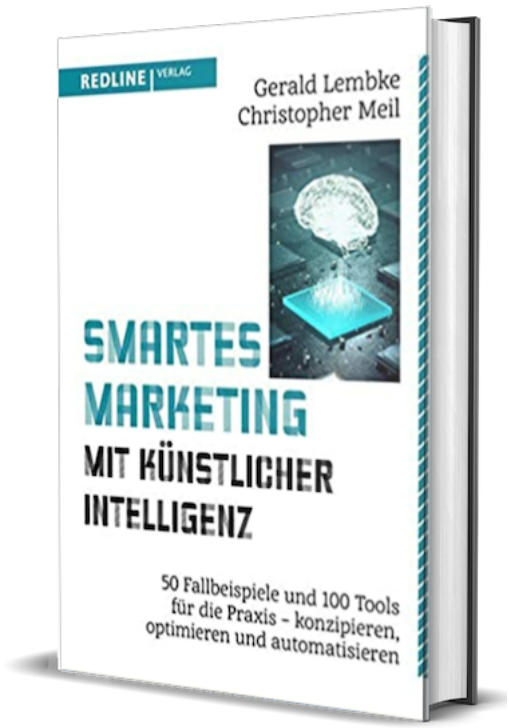
---

8. Autor

Gerald Lembke ist Professor für Digitale Medien und Digital- und Medienmanagement, ausgewiesener Experte, Speaker, Unternehmer und Berater für die Nutzung von digitalen Medien und künetlischer Intelligenzen in Unternehmen Mit 13 Büchern, zahllosen Fachartikeln und Vorträgen geniesst er höchste Reputation bei Digitalfreunden und -Gegnern. Für die Beratung und Umsetzung von Digitalen Medienprojekten und Nutzung von künstlichen Intelligenzen leitet er das Steinbeis Transferzentrum für digitale Medien und Management in Weinheim. https://Gerald-Lembke.de



Buch von Gerald Lembke und Christopher Meil: Smartes Marketing mit Künstlicher Intelligenz



Regelmäßige Updates zum KI-Einsatz in Mittelstandsunternehmen und Lernvideos gibt es auf https://KI-Toolparty.de .