KI-Sicherheit & Risikomanagement

Wie Sie als Unternehmer die Chancen der KI nutzen und die Risiken beherrschen.

WhatsApp Peer Group

KI ETHIK NEWS

MATERIAL

Arno Schimmelpfennig | November 2025

Selbständige IN BAYERN BDS

70%

...aller KI-Projekte in KMU scheitern. Viele davon verursachen unbemerkte Sicherheitslücken.

🔧 **Praxis-Fall:** Ein Handwerksbetrieb verliert 50.000 € durch eine ungesicherte KI-Schnittstelle in der Kundenverwaltung. Die Kundendaten wurden gestohlen, die Systeme standen wochenlang still.

Kurzumfrage

Was ist aktuell Ihre größte Sorge beim Einsatz von KI?

A) Datendiebstahl & Spionage

B) Manipulation von Ergebnissen

C) Systemausfall & Abhängigkeit

D) Datenschutz & rechtliche Konsequenzen (DSGVO/AI Act)

Die 5 Kernrisiken der KI im Überblick

Datenvergiftung

Angreifer manipulieren Ihre Trainingsdaten, um die KI zu falschen Entscheidungen zu zwingen.

Datenschutzverletzungen

Die KI verarbeitet unbemerkt personenbezogene Daten und verstößt gegen DSGVO oder den AI Act.

Modell-Diebstahl

Ihr wertvolles, trainiertes KI-Modell – Ihr geistiges Eigentum – wird kopiert und von der Konkurrenz genutzt.

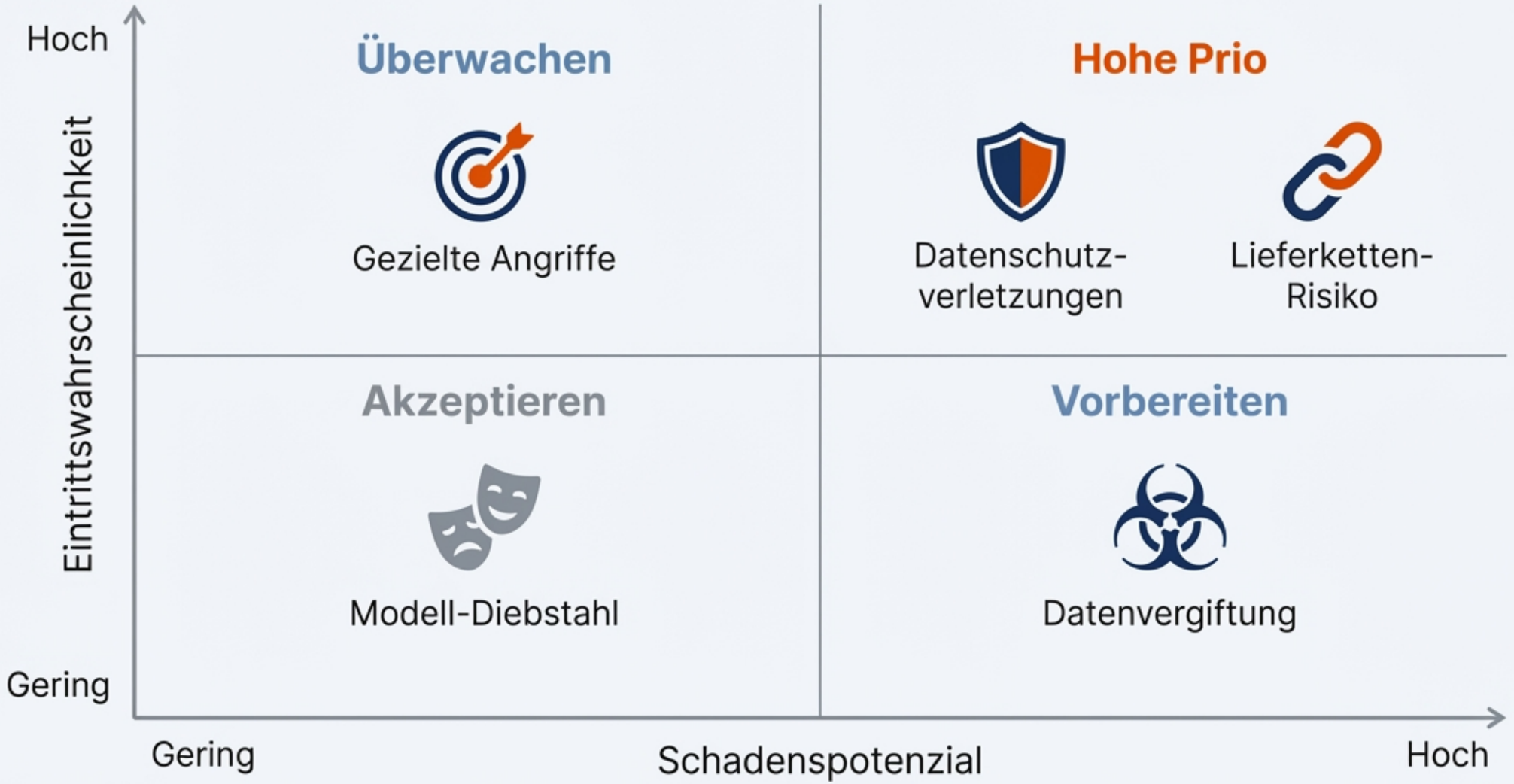
Gezielte Angriffe

Angreifer nutzen speziell präparierte Eingaben, um die KI gezielt auszutricksen (z.B. Spamfilter umgehen).

Lieferketten-Risiko

Eine von Ihnen genutzte KI-Komponente eines Drittanbieters ist unsicher und wird zum Einfallstor.

Risiken priorisieren



Was beschreibt das “Lieferketten-Risiko” bei KI am besten?

A) Die KI bestellt autonom die falschen Rohstoffe.

B) Eine zugekaufte KI-Software hat eine unentdeckte Sicherheitslücke.

C) Der Strom für das KI-Rechenzentrum fällt aus.

D) Der Entwickler der KI kündigt und nimmt sein Wissen mit.

Publikum

50/50

Experte

Was ist ein typisches Beispiel für “Datenvergiftung” (Data Poisoning)?

A) Ein Virus verschlüsselt die Datenbank der KI.

B) Die KI lernt aus Versehen vulgäre Sprache aus dem Internet.

C) Ein Angreifer fügt tausende falsche Bilder in den Datensatz ein, um die Bilderkennung zu sabotieren.

D) Die KI vergisst alte Daten und wird ungenauer.


Publikum


50/50


Experte

Welches Gesetz regelt europaweit den Umgang mit KI und deren Risikoklassen?

A) Die DSGVO

B) Das IT-Sicherheitsgesetz 2.0

C) Der EU AI Act

D) Das Telemediengesetz

Publikum 50/50 Experte

Eine KI zur Kreditwürdigkeitsprüfung lehnt systematisch Anträge aus bestimmten Stadtteilen ab. Welches Risiko liegt hier vor?

A) Modell-Diebstahl

B) Technischer Systemausfall

C) Ungewollter ‘Bias’ (Verzerrung) und Diskriminierung

D) Gezielter Angriff


Publikum


50/50


Experte

Was ist die effektivste einzelne Maßnahme, um das Risiko von unautorisiertem Zugriff auf KI-Systeme zu minimieren?

A) Eine teure Cyber-Versicherung abschließen.

B) Regelmäßige Mitarbeiterschulungen durchführen.

C) Eine starke Firewall installieren.

D) Multi-Faktor-Authentifizierung (MFA) für alle Zugänge erzwingen.


Publikum


50/50


Experte

Ihr 5-Punkte-Schutzschild

- **Regelmäßige Rechteprüfung:** Wer darf auf welche Daten und KI-Modelle zugreifen? Prinzip der minimalen Rechte anwenden.
- **Datenklassifizierung & -verschlüsselung:** Wissen, welche Daten sensibel sind, und diese sowohl im Ruhezustand als auch bei der Übertragung verschlüsseln.
- **Kontinuierliche Überwachung & Audits:** KI-Systeme auf ungewöhnliche Aktivitäten überwachen. Regelmäßige externe Sicherheits-Audits durchführen.
- **Mitarbeitersensibilisierung:** Ihr Team ist die erste Verteidigungslinie. Schulen Sie regelmäßig zu Phishing, Social Engineering und sicherem Umgang mit KI-Tools.
- **Sorgfältige Anbieterauswahl:** Prüfen Sie die Sicherheitsstandards von externen KI-Anbietern genau. Bestehen Sie auf einem Auftragsverarbeitungsvertrag (AVV).

Live-Check: Wo stehen Sie wirklich?

- **Scannen Sie den QR-Code** mit Ihrem Smartphone.
- **Beantworten Sie 5 kurze Fragen** zu Ihrer aktuellen Situation.
- Sie erhalten sofort eine **automatisierte Risiko-Einschätzung (in %).**
- **Dauer:** 2 Minuten. Ihre Antworten sind anonym.

Plan für den Ernstfall: Ihre 3 Phasen der Reaktion

PHASE 1: SOFORTREAKTION

- Systeme isolieren (Netzwerkverbindung trennen)
- Krisenteam einberufen (Geschäftsführung, IT)
- Kommunikationssperre (Keine Ad-hoc-Aussagen)

PHASE 2: ANALYSE & EINDÄMMUNG

- Externen Experten hinzuziehen
- Schadensausmaß und Ursache ermitteln
- Meldepflichten prüfen (z.B. Datenschutzbehörde)

PHASE 3: WIEDERHERSTELLUNG & LERNEN

- Gesicherte Backups einspielen
- Sicherheitslücke schließen
- Post-Mortem-Analyse: Was haben wir gelernt? Notfallplan anpassen.

Was zahlt im Ernstfall? Ein Blick auf Versicherungen

Versicherungstyp	Deckt typischerweise ab...	Geschätzte Kosten (KMU)
Cyber-Versicherung	Eigenschäden (Betriebsausfall, Wiederherstellung), Drittschäden (Datenschutzverletzungen), Kosten für IT-Forensik & Krisen-PR.	ab 800 € / Jahr
D&O-Versicherung	Persönliche Haftung der Geschäftsführung bei Managementfehlern (z.B. mangelnde Sicherheitsvorkehrungen).	ab 1.200 € / Jahr
Betriebshaftpflicht	Oft nur Basis-Schutz bei digitalen Schäden. KI-spezifische Risiken sind meist nicht abgedeckt.	**Prüfung notwendig!**

Ihr Fahrplan für die Umsetzung

MORGEN

Bestimmen Sie eine Person in Ihrem Unternehmen, die für KI-Sicherheit verantwortlich ist. (Dauer: 10 Min)

IN 3 TAGEN

Setzen Sie ein 30-minütiges Meeting mit Ihrem Team an, um über die 5 Kernrisiken zu sprechen.

IN 7 TAGEN

Überprüfen Sie Ihren Versicherungsstatus mit Ihrem Makler und holen Sie ein Angebot für eine Cyber-Versicherung ein.

Welchen EINEN dieser Schritte werden Sie bis morgen Abend umgesetzt haben? Schreiben Sie es für sich auf.

Danke!

- KI ist eine riesige Chance, wenn Risiken aktiv gemanagt werden.
- Ihr Schutzschild: Rechte, Verschlüsselung, Überwachung, Team & Partner.
- Starten Sie morgen mit dem ersten kleinen Schritt.

Arno Schimmelpfennig
Arno Schimmelpfennig
info@arno-schimmelpfennig.de | arno-schimmelpfennig.de

BDS.Bayern - KI Community
WhatsApp-Gruppe

Für Austausch & Fragen:
Treten Sie unserer KI-Community bei!
Treten Sie unserer KI-Community bei!