KI-Einsatz und KI-Gesetz

Gefahr für den Mittelstand?

Security Forum
15.1.2026

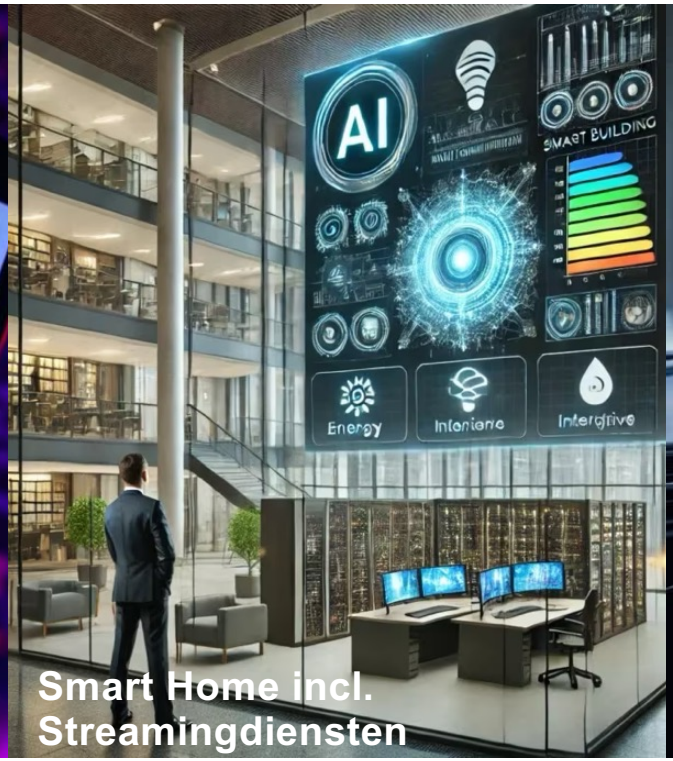
Annegrit Seyerlein-Klug

Dipl.-Ing.; M.Sc.; M.Sc.
Technische Hochschule Brandenburg, Intcube
CEN CENELEC JTC 21Convenor WG 5

1. **Einsatz von KI**
2. **KI-Gesetz**
3. **Gefahr für den Mittelstand ?**

KI ist allgegenwärtig und längst im Mittelstand angekommen

Smart Phone/PC mit Kamera, Sprachassistenz z.B.Siri/Alexa, Textvorschläge



Smart Home incl. Streamingdiensten

Mobilität z.B. Navigation oder Einparkhilfen

https://www.tagesschau.de/faktenfinder/kontext/ki-chatbots-100.html
https://ats.net/wenn-kuenstliche-intelligenz-das-auto-lenkt/
https://elektro-ruedi.de/ki-in-der-gebaeudeautomation-smarte-loesungen-fuer-energieeffiziente-gebaeude/

Wie nutzt der Mittelstand KI heute und morgen?

Typische Einsatzfelder:

Kundenservice
(Chatbots, E-Mail-Automatisierung)

Marketing & Vertrieb
(Personalisierung, Prognosen)

Produktion & Logistik
(Wartung, Qualitätskontrolle)

Verwaltung
(Dokumente, Buchhaltung, Personal)

Neue Trends – cross over

Agentic AI – der selbstständig unabhängig agierende KI Agent vor Ort für z.B.

Low code Programmierung mit KI in der Softwareentwicklung

Multimodale KI-Modelle verarbeiten Sprache, Text und Video

Hyperautomatisierung als Kombination von mehreren KI Technologien z.B. ML; Robotic Process Automation (RPA) …

KI automatisierte Geschäftsprozesse durch Verbindung von Machine Learning mit Workflow-Tools

Mittelstand fühlt sich zwischen Innovationsdruck und Regulierungsangst

Die Frage ist nicht mehr:

Nutzen wir KI ?

sondern:

Nutzen wir KI bewusst und rechtssicher ?

Sind KI und Gesetz für den Mittelstand gefährlich ?

Warum mischt sich der Gesetzgeber ein ?

Aufgabe des Staates:
Schutz des Gemeinwohl und der Grundrechte der Bürger.

- **KI kann Entscheidungen treffen und beeinflussen.**
- **Entscheidungen treffen Personen und ggf. deren Sicherheit und Grundrechte**

Schutz durch den Staat:

vor negativen KI Auswirkungen für Bürger → z.B. durch Gesetze

Chancen mit klaren KI Regeln

Gesetze bieten:

- **Rechtssicherheit für alle** statt Grauzonen besonders für kleinere Unternehmen
- **Schutz vor Haftungsrisiken** und Klärung, wer haftet
- **gleiche Spielregeln für alle**
- große Tech-Firmen sind stärker reguliert als KMU
- mehr Vertrauen bei Kunden

➤ **Für den Mittelstand**
sind Gesetze oft eher Schutz als Bedrohung/ Gefahr

1. Einsatz von KI
2. **KI-Gesetz**
3. Gefahr für den Mittelstand ?

Ziel der KI Verordnung → Schutz vor Hochrisiko-KI-Produkten

EU KI-Verordnung Art. 1

(1) Zweck dieser Verordnung ist es,

– das Funktionieren des Binnenmarkts zu verbessern und

– die Einführung einer auf den **Menschen** ausgerichteten und vertrauenswürdigen künstlichen Intelligenz (KI) zu fördern und gleichzeitig

– ein **hohes Schutzniveau** in Bezug auf

Gesundheit, Sicherheit (Safety) und die in der EU Charta verankerten Grundrechte, einschließlich Demokratie, Rechtsstaatlichkeit und Umweltschutz,

vor schädlichen Auswirkungen von KI-Systemen in der Union zu gewährleisten und

– die Innovation zu unterstützen.

Gesundheit

Sicherheit

EU Charta der Grundrechte

Prüfung mit harmonisierten EU-KI-Standards

EU KI-Verordnung Art. 1

(2) In dieser Verordnung wird Folgendes festgelegt:

a) **harmonisierte Vorschriften** beschreiben die Umsetzung von
- Inverkehrbringen,
- die Inbetriebnahme und
- die Verwendung von KI-Systemen in der Union

Harmonisierte EU Standards für Konformität und zu EU - Gesetzen

- ✓ definieren prüfbare Anforderungen und **Selbstzertifizierung CE**
- ✓ angemessen für Organisationen unterschiedlicher Größe und Komplexität

- ➢ **Der Einsatz der harmonisierten Standards ist freiwillig**
- ➢ **Compliance kann mit eigenen Verfahren nachgewiesen werden und mit externer Zertifizierung**

KI-Verordnung

verpflichtet **ALLE**

Art. 4: Sicherstellung angemessener KI-Kompetenzen !!

Bildquelle: https://gerald-lembke.de/ki-kompetenzen-schulen-ausbilden/

Risikobasierter Ansatz

Verboten

Betrifft den Mittelstand fast nie

z.B. KI, die Menschen manipuliert oder überwacht
- definiert im Gesetz

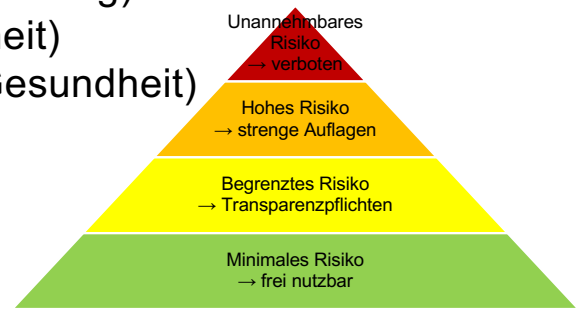
Hohes Risiko

Kann den Mittelstand ggf. betreffen

Art. 6 und Anhang III

strenge Pflichten für Anbieter und Anwender für KI z.B. bei

- Bewerberauswahl (Diskriminierung)
- Kreditvergabe (Diskriminierung)
- medizinischen Entscheidungen (Gesundheit)
- sicherheitskritische Maschinen (Safety, Gesundheit)



Normalfall im Mittelstand

Begrenztes Risiko **Normalfall im Mittelstand**

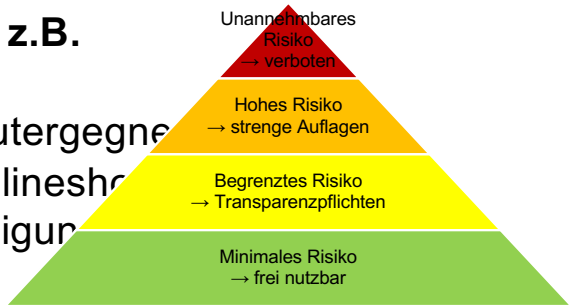
Pflichten für Anbieter und Anwender an
Transparenz/Dokumentation
z.B. **Kennzeichnung** von KI-Einsatz in

- Chatbots, virtuelle Assistenten oder automatisierte Buchungssysteme
- Text- und Bildgeneratoren
- Planung und Analyse-Tools

Minimales Risiko **Normalfall im Mittelstand**

keine Pflichten auf dem Markt und nutzbar z.B.

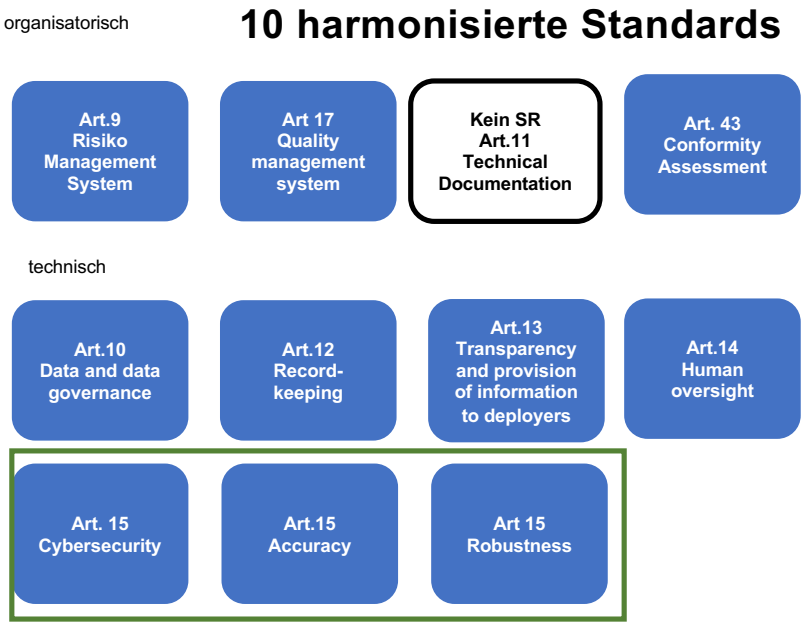
- Spam-Filter in E-Mails.
- KI in Videospielen (z. B. Verhalten von Computergegne
- Suchalgorithmen; Empfehlungssysteme in Onlinesho
- Rechtschreibkorrekturen und Textvervollständigun
- Predictive Maintenance
- Logistikplanung



Anforderungen aus EU-KI-Verordnung (Auszug)
Anbieter/ Hersteller

Pflichten für Anbieter/Hersteller NUR bei Hochrisiko KI u.a.

Art. 16	Pflichten Anbieter von Hochrisiko-KI
Art. 9-15	**Organisatorischen und technischen Anforderungen**
Art. 17	**Qualitätsmanagementsystem**
Art. 11; 18; 19	**Dokumentation und Aufbewahrung**
Art. 43	**Konformitäts**-Assessment;



Anforderungen aus EU-KI-Verordnung (Auszug)
Anwender/ Nutzer

Pflichten von Anwendern/Betreiber NUR bei Hochrisiko-o-KI u.a. zu

Art. 26

- **Bestimmungsgemäße Verwendung** strikt nach bereitgestellten Gebrauchsanweisungen
- **Kontrolle** der verwendeten Daten
- **Menschliche Aufsicht** mit qualifizierte Personen, die überwachen und eingreifen können.
- **Überwachung** im Betrieb auf Anomalien

Art. 50 Transparenz-; Informations- und Meldepflichten bei Vorfällen

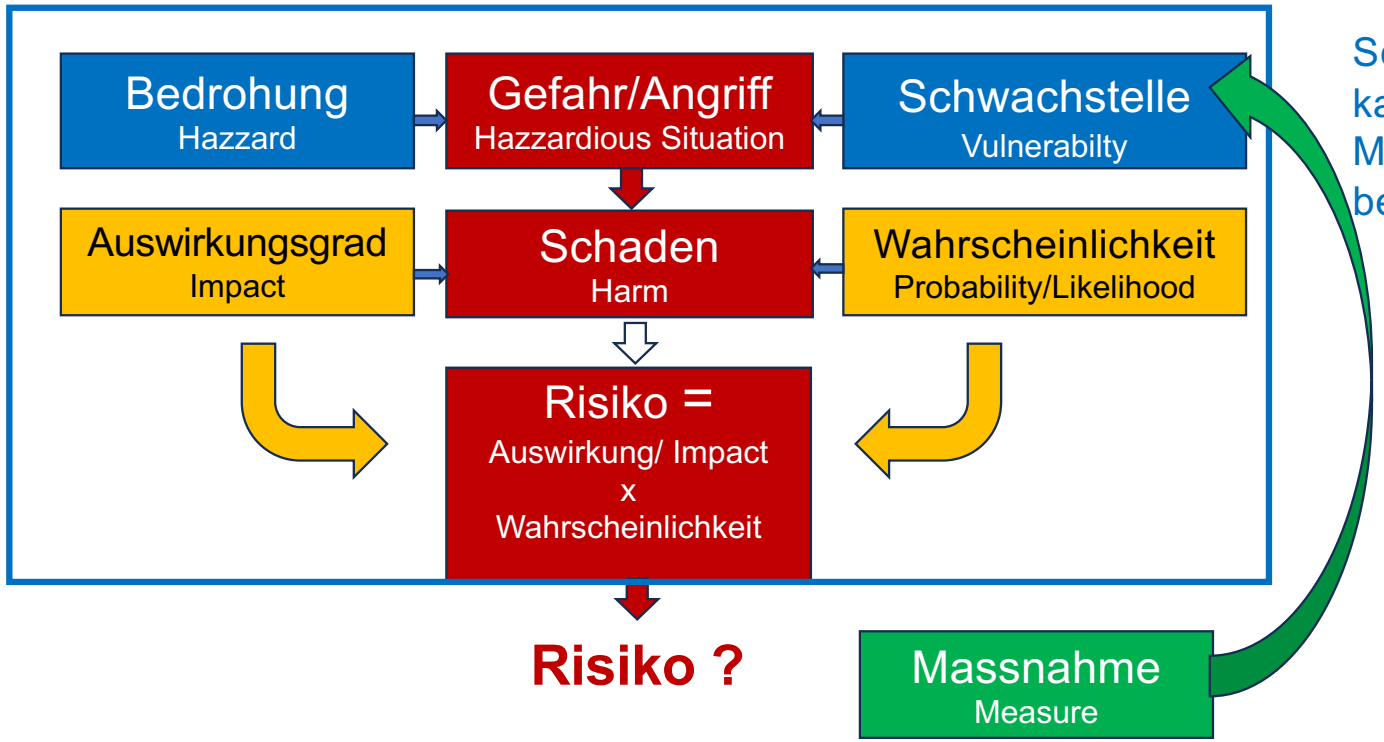
Art. 27 Erstellung einer Grundrechte Folgeabschätzung

1. Einsatz von KI
2. KI-Gesetz
3. **Gefahr für den Mittelstand?**


Warum ist die Gefahr,
in Australien/Queensland
im Meer zu schwimmen,
nicht unbedingt
ein Risiko?
NO SWIMMING
MARINE STINGERS
LIFEGUARD

Gefahr und Risiko-Identifikation und -Analyse

Bedrohungen sind extern und bleiben i.d.R.



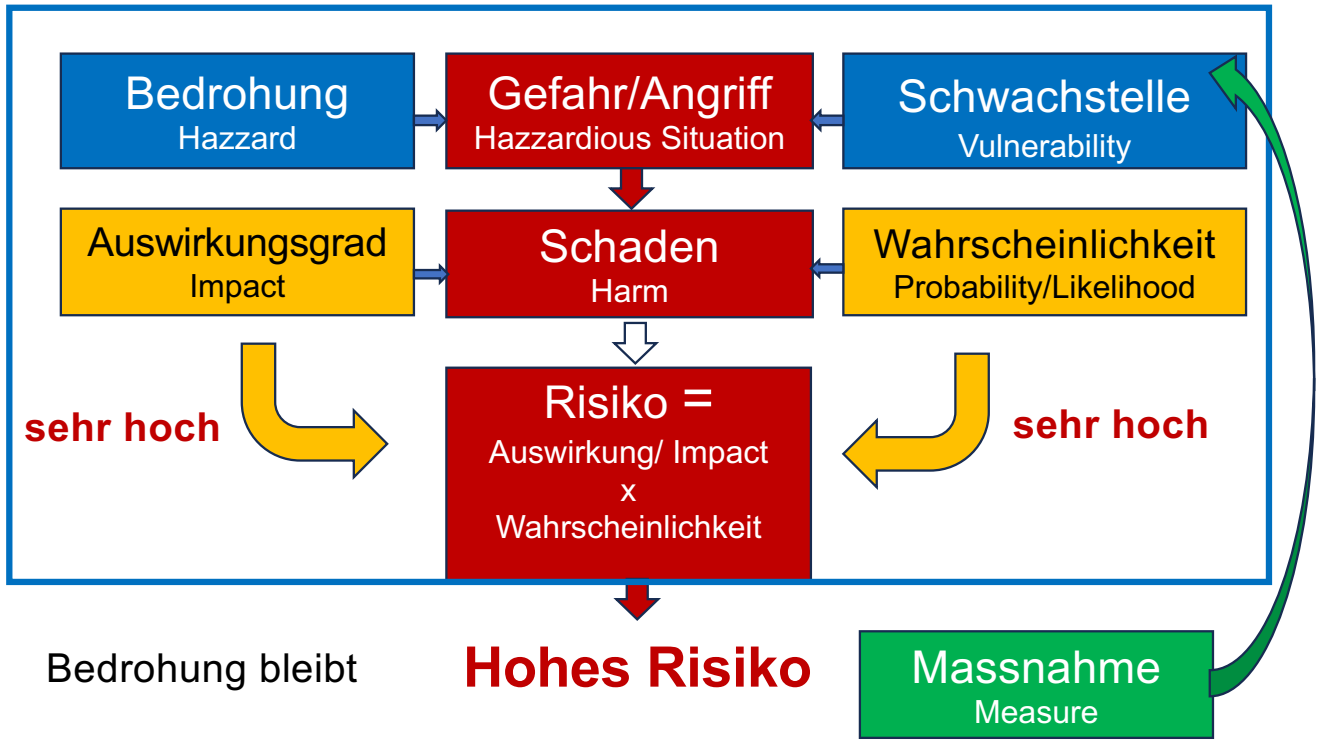
Schwachstellen kann man mit Massnahmen beeinflussen

Risiko Identifikation und Analyse

Person in Badekleidung kann beim Schwimmen im Meer Kontakt mit Marine Stinger haben und Schaden nehmen

Giftige Marine Stingers/ Jelly fish leben an dieser Küste.

Kontakt mit Tentakelgift = massive Schmerzen bis Tod



Empfindlichkeit für Gift von Marine Stingers.

Kontaktmöglichkeit Im Meer

Schutzmassnahmen
Risikobehandlung = Senkung der Gefahr

100%

20 %

90 %

97 %

KI-VO Stufe 1 KI-Risiko für eine Person

Anwender/Nutzer müssen NUR bei Hochrisiko

eine KI-Risikofolgenabschätzung für Personen erstellen

Frage:

besteht ein Risiko im Sinne der KI-VO für Personen bei Nutzung/Anwendung der KI,
basierend auf

- vorhandenen Schwachstellen/Handlungsmöglichkeit bei der Person
- bekannten Bedrohungen durch KI für die Person die zu Schäden an Gesundheit, Sicherheit und den Grundrechte führen können
- und unter gegebenen situativen Umständen/Einsatz/Funktion

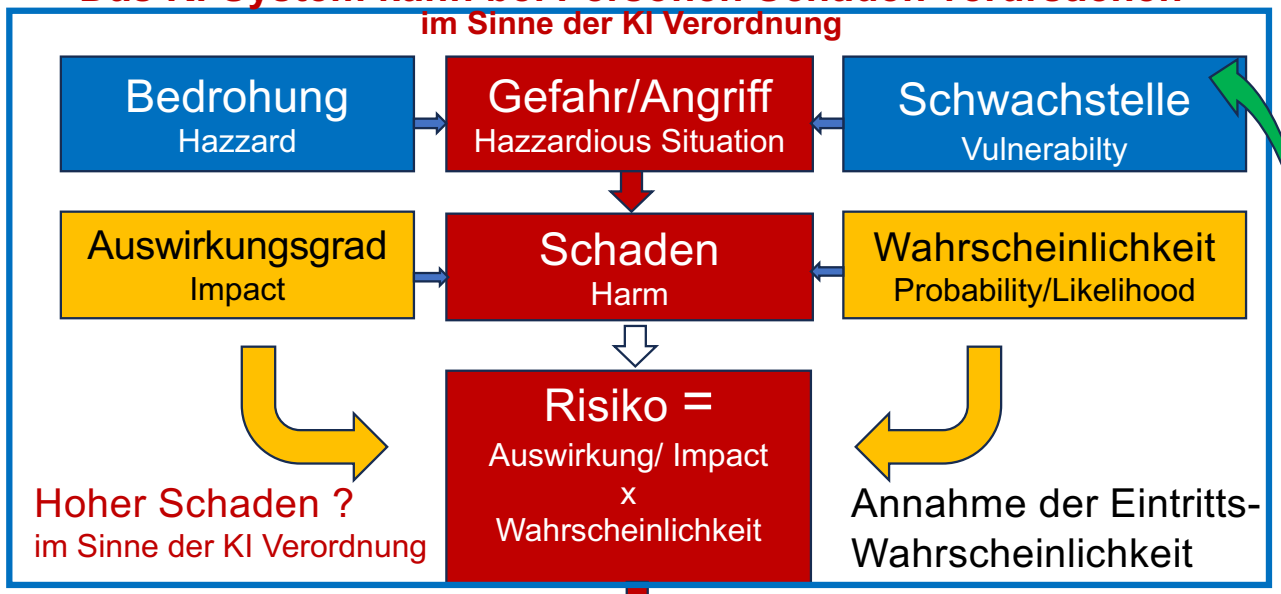
Gefahr, Bedrohung und Risiko ?
– es kommt darauf an

Gefahr:
Das KI-System kann bei Personen Schäden verursachen
im Sinne der KI Verordnung

Das KI-System kann durch seine Funktion und Missfunktion Personen schaden?

z.B. Diskrimierung

Schaden:
Keine Zulassung
Falsche Diagnose..



Hohes Risiko ?
im Sinne der KI -Verordnung

Massnahme KI VO

Möglichkeiten der betroffenen Person gegen Bedrohungen

keine Kenntnis, dass KI mit Dis-kriminierung im Einsatz ist

100%

KI-VO Stufe 2 Risiken

Anbieter/Hersteller müssen NUR bei Hochrisiko

1. **KI-Risikomanagement für das KI-System im Sinne der KI-Verordnung** einsetzen sowie
2. **Cybersecurity Risiken** für das KI-System im Sinne der KI-Verordnung ermitteln.

Frage:

welche Risiken bestehen generell **für Personen durch** die Nutzung/Anwendung der KI,

.....

welche Risiken bestehen generell **für das KI-System** über den Lebenszyklus, basierend auf

- vorhandenen Schwachstellen des KI-Systems
- bekannten **Cybersecurity** Bedrohungen gemäß der KI Verordnung,
- und unter gegebenen situativen Umständen/Einsatz/Funktion

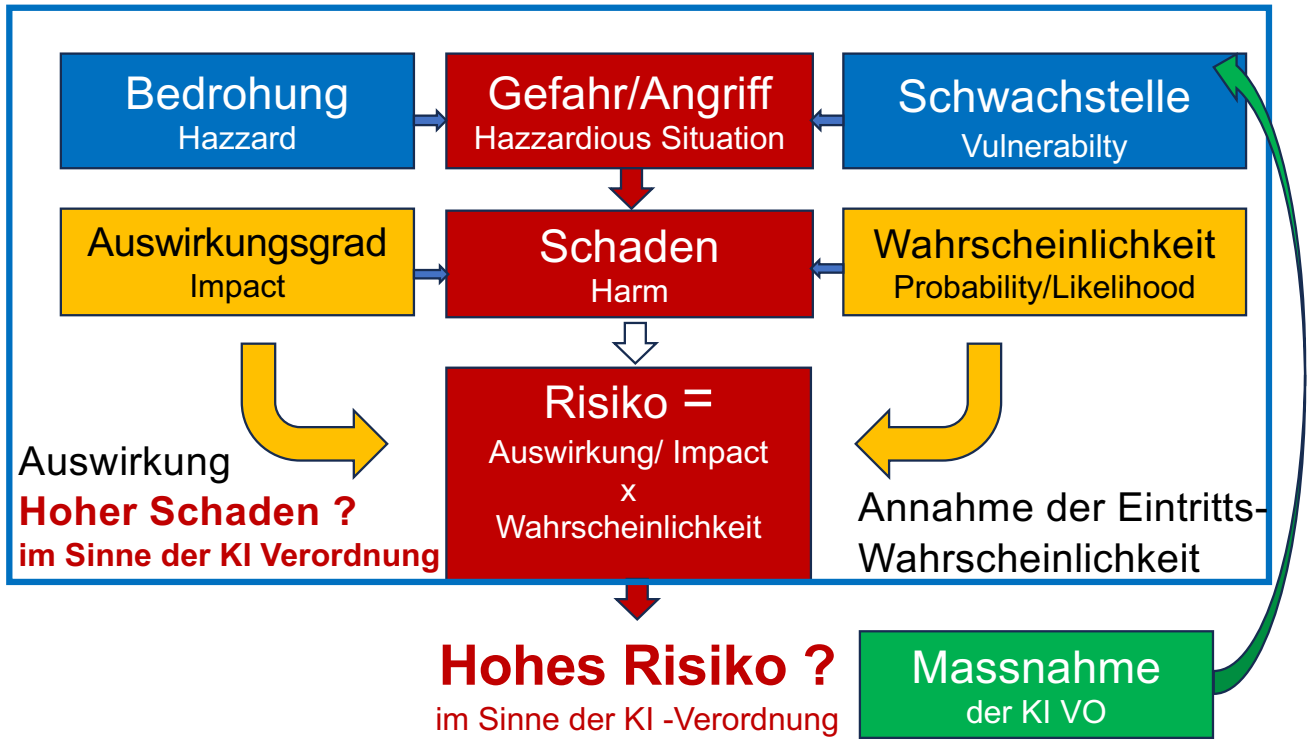
Safety ? gemeinsam ? Cybersecurity

Cybersecurity – Risiken für das KI-System ?

Gefahr: Das KI System kann durch Cybersecurity Bedrohungen zu Schäden kommen im Sinne der KI Verordnung

Identifikation + Analyse:
Kann die Funktion des KI-Systems gestört und attackiert werden durch

- Data poisoning,
- Model poisoning,
- Adversarials, Evasion
- in Confidentiality
- durch Model Flaws



Identifikation + Analyse:
Hat das das KI-System, bezogen auf die KI-Cyber-Bedrohungen, technische und organisatorische Mängel

Risiken und Gefahr für den Mittelstand ?

Beispiel für den Mittelstand:
Risikoabschätzung in Bezug auf den Einsatz von KI und die Gesetzgebung

Frage:

welche Risiken bestehen für den Mittelstand bei Einsatz von KI durch die KI-VO,
basierend auf

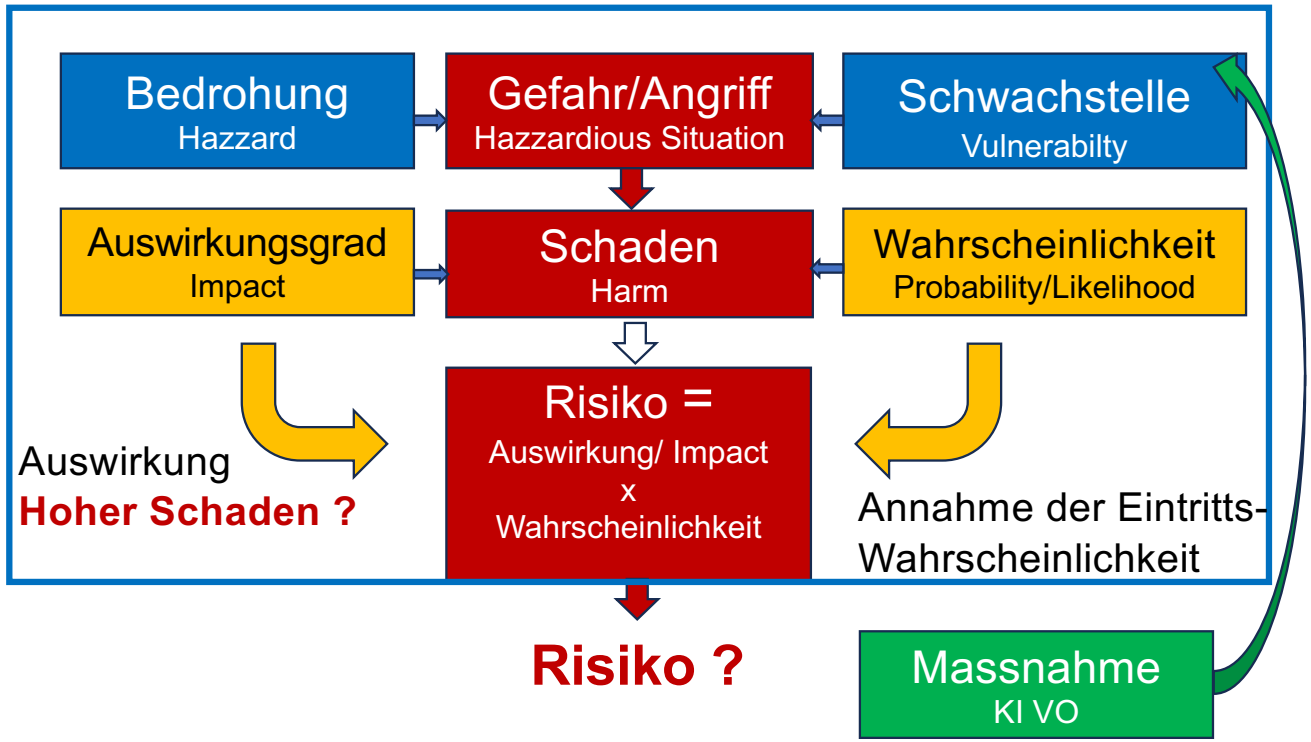
- vorhandenen Schwachstellen des Mittelstandes
- Bedrohungen durch die KI-Verordnung beim Einsatz von KI
- unter den gegebenen situativen Umständen/Einsatz/Funktion

Gefahr und Risiken für den Mittelstand ?

Gefahr: Der Mittelstand kann durch die KI-VO bei Einsatz von KI in seiner Tätigkeit/Innovationen beeinträchtigt werden.

Die KI-VO enthält viele Vorgaben für KI.

Bei Umsetzung der Vorgaben für bedingtes/hohes Risiko entsteht „viel“ Aufwand, der evtl. Schäden verur-sacht.



Der Mittelstand hat nicht/kaum die organisatorischen, und technischen finanziellen, personellen Mittel

Wo liegen Risiken für den Mittelstand? Ist das eine Gefahr?

Bedrohungen - bleiben

- Komplexe gesetzliche Anforderungen
- Bürokratischer/technischer Mehraufwand
- Bußgeldern

Schwachstellen - kann man angehen

- Unkenntnis der gesetzl. Anforderungen
- Unsicherheiten
  „Darf ich KI überhaupt noch nutzen?“
  „Mache ich etwas falsch?“
- Kosten für Dokumentation & Compliance
- Abhängigkeit von großen KI-Anbietern

Aber:

- Viele Pflichten/ Massnahmen betreffen **Hersteller**
- Kleine Unternehmen **werden eher als Anwender gesehen**
- Kleine Unternehmen werden **nicht wie Konzerne behandelt**

- **Pflichten nur bei Hochrisiko**

➢ **Gefahr entsteht eher durch Nichtwissen und Vorbehalte als durch das KI-Gesetz**

Fazit

Was sollte jetzt konkret getan werden ?

Kein Aktionismus – aber klare Schritte:

- **Überblick gewinnen:** Inventarisierung und Dokumentation, QMS und Risiko einführen.
  Wo nutzen wir KI oder KI-gestützte Software?
  Als Anwender und/oder als Hersteller?
- **Mitarbeitende sensibilisieren** und informieren:
  Was kann KI? Was darf KI und was nicht?
- **Seriöse Anbieter wählen**,
  die EU-konform und transparent sind
  (Anbieterpflichten)
- **KI als Werkzeug**, nicht als Experiment nutzen:
  Unterstützung ja; automatische Entscheidungen nein
  (wenn Hoch-Risiko und/oder kritisch)
- Eigene und die **Risiken** der KI realistisch bewerten

Nicht nötig, aber ggf. im Zugriff

- eigene IT-Abteilung
- Juristen im Betrieb
- Angst vor Strafen

Die meisten KI-Produkte:

- sind erlaubt
- im Risiko begrenzt oder minimal
- kaum zusätzlichen Pflichten


AI
Kaum Gefahr
viel Erfolg
KI im
Mittelstand

Annegrit Seyerlein-Klug

- Dipl.-Ing. (Maschinenbau, Medizintechnik)
- M.Sc. Security Management; M.Sc. Technologie und Innovation
- ISO 27001 und ITIL zertifiziert
- Nixdorf; Siemens Nixdorf/ Siemens Business Services, Siemens/Siemens Enterprise/Unify; Secunet (Security KRITIS); Neurocat (AI Security and Robustness); Intcube (AI Security)
- Technische Hochschule Brandenburg
- Engagiert in
  - **DIN/CEN/ISO Cybersecurity/KI/ Datenschutz u.a. für Energie/KRITIS und Automotive**
  - **Convenor CEN/CENELEC JTC 21 (AI- Act) WG5 „Cybersecurity Specification for AI-systems“**
  - Kompetenzzentrum Kritische Infrastruktur
  - Europäische Akademie für Informationsfreiheit und Datenschutz
  - Bitkom diverse

annegrit.seyerleinklug@th-brandenburg.de