



ALTHAMMER
& KILL

**Digitalisierung als
Chance oder Risiko?**

*Aktuelle Entwicklungen zu
Informationssicherheit & KI*

Thomas Althammer, 14.06.2024
Internationale Hochschule

1

Kurz vorgestellt

ALTHAMMER
& KILL



Thomas Althammer

Wirtschaftsinformatiker (Int. MBI)

Externer Datenschutzbeauftragter und
Externer Informationssicherheitsbeauftragter u. a.
im Gesundheits- und Sozialwesen (DSGVO, DSG-EKD, KDG)

Lehrbeauftragter an der Hochschule Hannover
und der Kath. Universität Eichstätt-Ingolstadt

Co-Leiter FINSOZ Fachgruppe IT-Compliance

Seite 2

2

Kurz vorgestellt

ALTHAMMER
& KILL



Althammer & Kill

Unternehmensberatung mit 45 Mitarbeitenden
(Datenschutzbeauftragte, Informationssicherheitsbeauftragte,
Juristinnen/Juristen, Security-Spezialistinnen/Spezialisten)

gegründet 2014, bundesweit im Einsatz mit
Büros in Hannover, Düsseldorf, Mannheim



3

3



Lage der IT-Sicherheit

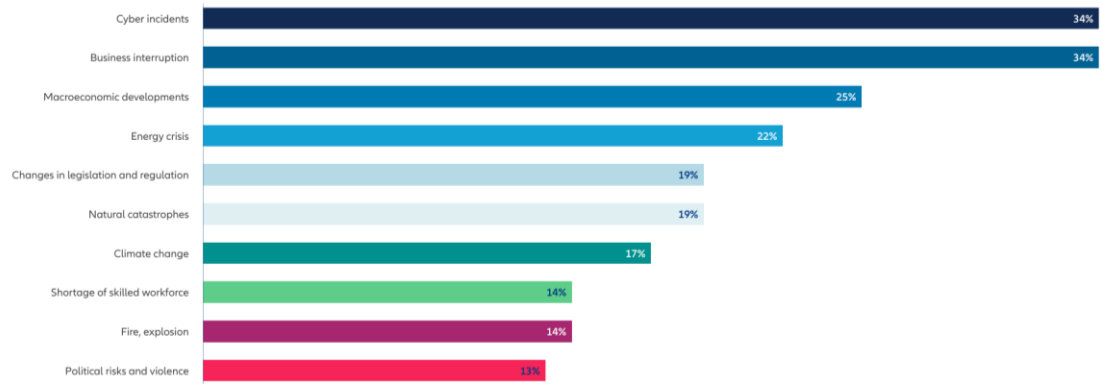
4



The most important business risks in 2023: global

Allianz Risk Barometer 2023

Figures represent how often a risk was selected as a percentage of all survey responses from 2,712 respondents. All respondents could select up to three risks per industry, which is why the figures do not add up to 100%.



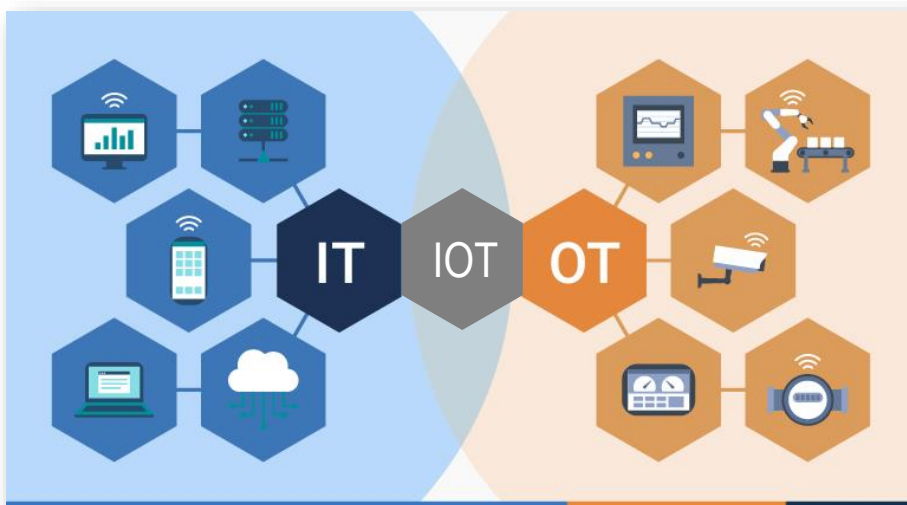
AGCS News & Insights

Source: Allianz Global Corporate & Specialty

5

Digitalisierung als Chance oder Risiko?
Aktuelles zu NIS-2, KI und mehr

ALTHAMMER
& KILL



6

OnLogic

6

Neue Vorgaben durch die EU

Motivation: Schutz der Bevölkerung (nicht des Betreibers)

EU NIS-2
High common level of
cybersecurity across the Union



EU RCE
Resilience of critical entities
in the Union

Mindestniveau für Cyber-Security in der EU.
Regulierung kritischer Dienste und
Infrastrukturen durch die Mitgliedsstaaten

Resilienz-Baseline für Betreiber kritischer
Services. Nationale Regulierung mit
Überwachung durch die EU.

NIS-2-Regulierung

- 10 essenzielle + 6 wichtige Sektoren
- Cyber-Security bei Betreibern
- nationale Governance, EU-Aufsicht
- in Kraft seit 01/23, nationale Umsetzung

RCE-Regulierung

- 10 kritische EU-Sektoren mit „Entitäten“
- Resilienz bei Betreibern
- nationale Governance, EU-Aufsicht
- in Kraft seit 01/23, nationale Umsetzung

7

Stand 05/2024

7

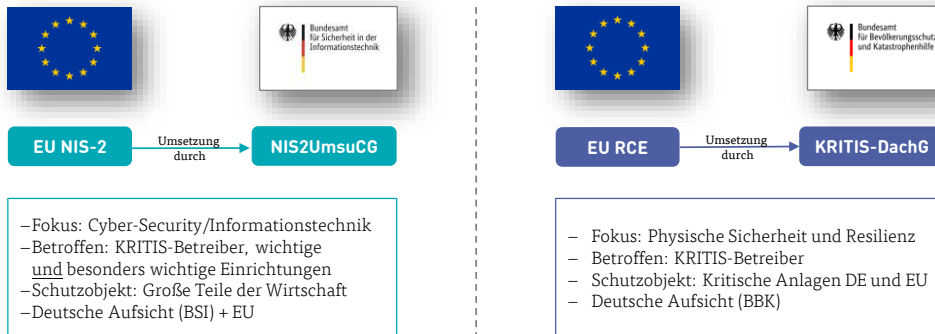


8

<https://www.dke.de/de/arbeitsfelder/cybersecurity/cybersecurity-navigator>

8

Nationale Umsetzung NIS-2 und RCE

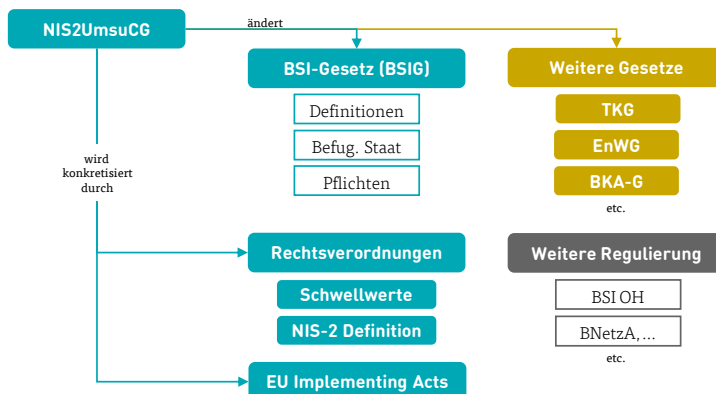


9

Stand 05/2024

9

Nationale Umsetzung und Regulierung

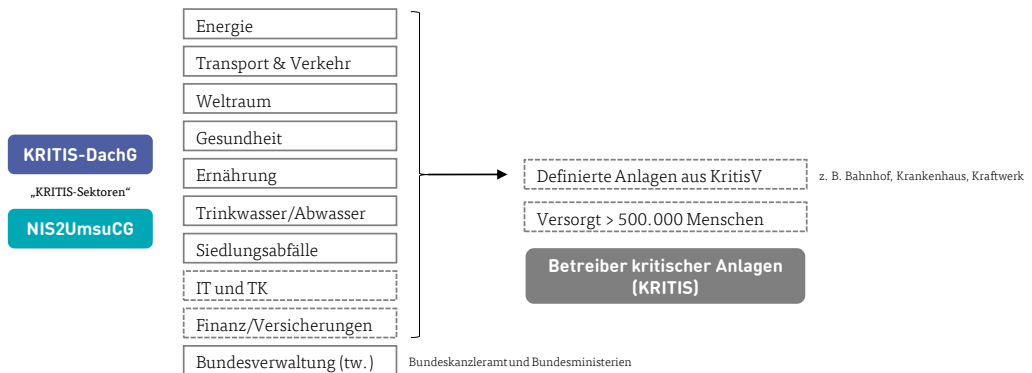


10

Stand 05/2024

10

Sektoren KRITIS-Dachgesetz



11

Stand 05/2024

11

KRITIS-DachG – Physische Sicherheit

- Registrierung (Frist: 3 Monate)
- Resilienz-Maßnahmen (Frist: 10 Monate)
- Risikoanalyse (Frist: alle 4 Jahre)
- Meldepflicht (Frist: 10 Monate – nach Vorfall 24 h)
- Nachweise/Audits
- Sanktionen

12

Stand 05/2024

12

Schwellwerte NIS2UmsuCG

Organisationen	Sektoren	Mitarbeitende	Umsatz	Bilanz
Besonders wichtige Einrichtungen	NIS-2 Anlage 1	a) ≥ 250 b)	≥ 50 Mio. EUR und	≥ 43 Mio. EUR
Wichtige Einrichtungen	NIS-2 Anlage 1 NIS-2 Anlage 2	a) ≥ 50 b)	≥ 10 Mio. EUR und	≥ 10 Mio. EUR
Kritische Anlagen	KRITIS-Sektoren	Schwellwerte werden pro Anlage definiert		

Pflichten im NIS2UmsuCG

- Registrierung (Frist: 3 Monate)
- Risikomanagement (Risikoanalysen, ISMS, Incident Management, BCM, etc.)
- Meldepflichten (nach Vorfall 24 h, SOC/SIEM)
- Nachweise/Audits
- Informationspflichten
- Governance (persönliche Haftung Geschäftsleitung)
- Sanktionen (bis 10 Mio. EUR/2 % vom weltweiten Umsatz)

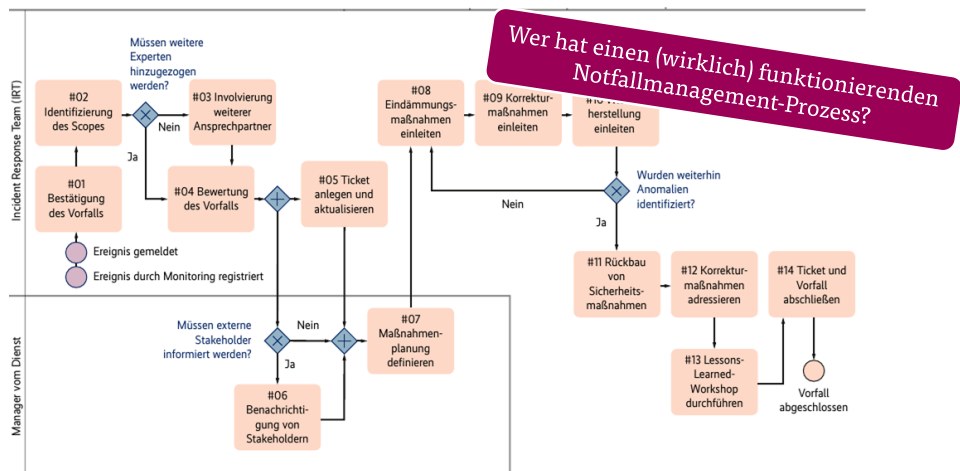
Ganz konkret gefragt...:

- Haben wir ein aktuelles Backup?
- Wo liegt das Backup? Ist das Backup offline?
- Haben wir die Wiederherstellung getestet?
- Also haben wir getestet, ob System <xx> wirklich wiederherstellbar ist?
- Wie lange braucht das Wiedereinspielen?
- ... das gleiche für Firewall, Patch-Management, Benutzerverwaltung, uvm.

15

15

Notfallprozess & Notfallhandbuch



16

16



Was gilt denn nun?

17

..... Digitalisierung als Chance oder Risiko?
..... Aktuelles zu NIS-2, KI und mehr

ALTHAMMER
& KILL

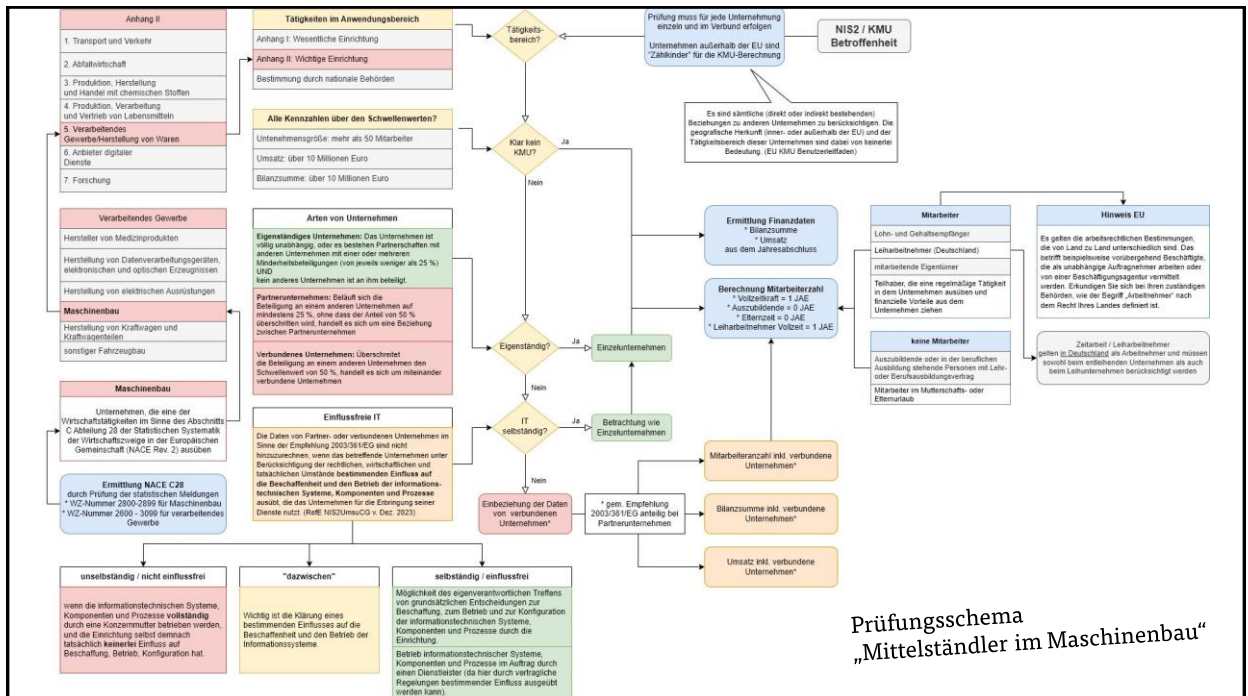
Wer ist betroffen von NIS-2?

1. Unmittelbar betroffen in definierten Sektoren sind
 - „Wichtige“ Einrichtungen
 - „Besonders wichtige“ Einrichtungen
 - Betreiber kritischer Anlagen
2. Mittelbar betroffen sind
 - Dienstleister, Zulieferer
 - Nebenprozesse, die schnell mal übersehen werden

..... 18

Vorbehaltlich Änderungen, Stand 05/2024

18



1) Sektoren nach Anlage 1 und 2

- 70 -

Bearbeitungsstand: 07.05.2024 10:19

Anlage 1

Sektoren besonders wichtiger und wichtiger Einrichtungen

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Sektor	Branche	Einrichtungsart
1	Energie		
1.1		Stromversorger	Stromlieferanten gemäß § 3 Nr. 31a EnWG
4	Gesundheit		
4.1			Erbringer von Gesundheitsdienstleistungen im Sinne der Richtlinie (EU) 2011/24 des Europäischen Parlaments und des Rates
4.1.2			EU-Referenzlaboratorien nach Artikel 15 der Verordnung (EU) 2022/2371 des Europäischen Parlaments und des Rates

Referentenentwurf
Stand 07.05.2024

2) Definition Gesundheitsdienstleister

27.12.2022 DE Amtsblatt der Europäischen Union L 333/80

RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES
vom 14. Dezember 2022
über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1872 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie)

(Text von Bedeutung für den EWR)

5. Gesundheitswesen	<p>„Gesundheitsdienstleister“ im Sinne des Artikels 3 Buchstabe g der Richtlinie 2011/24/EU des Europäischen Parlaments und des Rates ⁽¹⁵⁾</p> <p>EU-Referenzlaboratorien im Sinne des Artikels 15 der Verordnung (EU) 2022/2371 des Europäischen Parlaments und des Rates ⁽¹⁶⁾</p> <p>Einrichtungen, die Forschungs- und Entwicklungstätigkeiten in Bezug auf Arzneimittel im Sinne des Artikels 1 Nummer 2 der Richtlinie 2001/83/EG des Europäischen Parlaments und des Rates ⁽¹⁷⁾ ausüben</p> <p>Einrichtungen, die pharmazeutische Erzeugnisse im Sinne des Abschnitts C Abteilung 21 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) herstellen</p> <p>Einrichtungen, die Medizinprodukte herstellen, die während einer Notlage im Bereich der öffentlichen Gesundheit als kritisch im Sinne des Artikels 22 der Verordnung (EU) 2022/123 des Europäischen Parlaments und des Rates ⁽¹⁸⁾ („Liste kritischer Medizinprodukte für Notlagen im Bereich der öffentlichen Gesundheit“) eingestuft werden</p> <p>Lieferanten von und Umsendern der Versorgung mit „Wasser für den menschlichen Gebrauch“ im Sinne des Artikels 2 Nummer 1 Buchstabe a der Richtlinie (EU) 2020/2184 des Europäischen Parlaments und des Rates ⁽¹⁹⁾, jedoch unter Ausschluss der Lieferanten, für die die Lieferung von Wasser für den menschlichen Gebrauch ein nicht wesentlicher Teil ihrer allgemeinen Tätigkeit der Lieferung anderer Rohstoffe und Güter ist</p>
6. Trinkwasser	

https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555&qid=1701426623240#nr18-L_2022333DE.01014301-E0018

21

3) Gesundheitsdienstleister im Detail

4.4.2011 DE Amtsblatt der Europäischen Union L 88/55

Artikel 3
Begriffsbestimmungen

Im Sinne dieser Richtlinie bezeichnet der Ausdruck

a) „Gesundheitsversorgung“ Gesundheitsdienstleistungen, die von Angehörigen der Gesundheitsberufe gegenüber Patienten erbracht werden, um deren Gesundheitszustand zu beurteilen, zu erhalten oder wiederherzustellen, einschließlich der Verschreibung, Abgabe und Bereitstellung von Arzneimitteln und Medizinprodukten;

b) „Versicherter“

i) Personen einschließlich ihrer Familienangehörigen und Hinterbliebenen, die unter Artikel 2 der Verordnung (EG) Nr. 883/2004 fallen und die Versicherte im Sinne des Artikels 1 Buchstabe c jener Verordnung sind, und

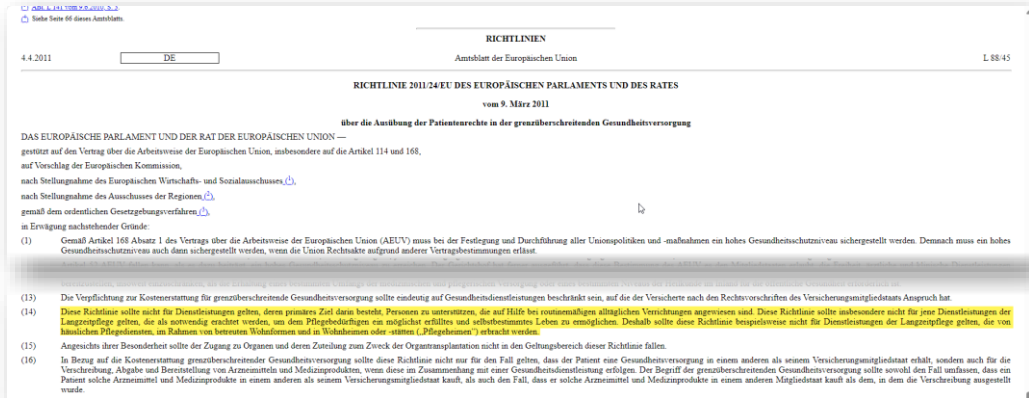
f) „Angehöriger der Gesundheitsberufe“ einen Arzt, eine Krankenschwester oder einen Krankenpfleger für allgemeine Pflege, einen Zahnarzt, eine Hebamme oder einen Apotheker im Sinne der Richtlinie 2005/36/EG oder eine andere Fachkraft, die im Gesundheitsbereich Tätigkeiten ausübt, die einem reglementierten Beruf im Sinne von Artikel 3 Absatz 1 Buchstabe a der Richtlinie 2005/36/EG vorbehalten sind, oder eine Person, die nach den Rechtsvorschriften des Behandlungsmitgliedstaats als Angehöriger der Gesundheitsberufe gilt;

g) „Gesundheitsdienstleister“ jede natürliche oder juristische Person oder sonstige Einrichtung, die im Hoheitsgebiet eines Mitgliedstaats rechtmäßig Gesundheitsdienstleistungen erbringt;

<https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:088:0045:0065:de:PDF>

22

4) Bedeutung für die Pflege

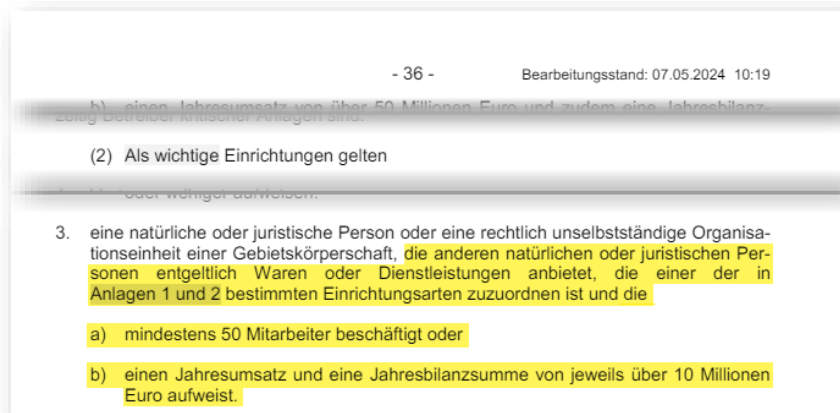


23

<https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L:2011:088:FULL>

23

Geltungsbereich Lieferketten

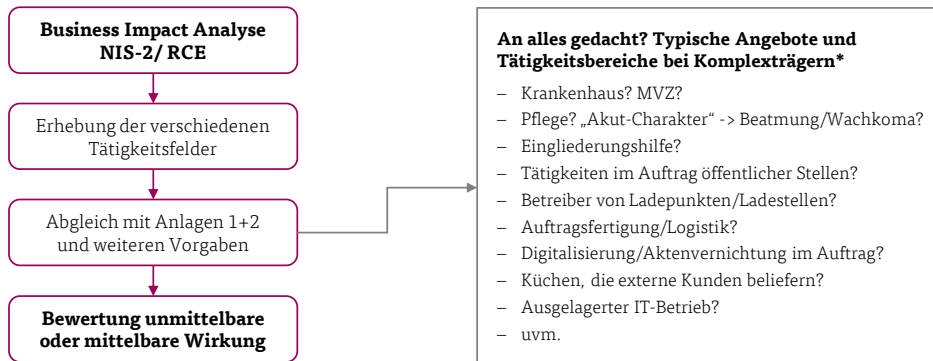


24

Referentenentwurf
Stand 07.05.2024

24

(Un-)Mittelbare Wirkung prüfen



25

*) Hinweis: Die NIS-2-Richtlinie unterscheidet nicht zwischen Haupt- und Nebentätigkeit.

25

Zusammenfassung

1. Für viele Unternehmen besteht Unklarheit
 - Einerseits werden nur manche direkt unter das NIS2UmsuCG fallen
 - Andererseits bestehen mittelbare Verpflichtungen, je nach Größe, Struktur und Leistungsangebot der Organisation
2. These: NIS-2 wird zum branchenübergreifenden Orientierungsrahmen, nach dem „Reifegrad“ und „Stand der Technik“ zukünftig bewertet werden.
3. Die aktuelle Cyber-Bedrohungslage, allgemeine gesetzliche Vorgaben und Fürsorgepflichten erfordern eine aktivere Auseinandersetzung mit Informationssicherheit und BCM-Konzepten.

26

26

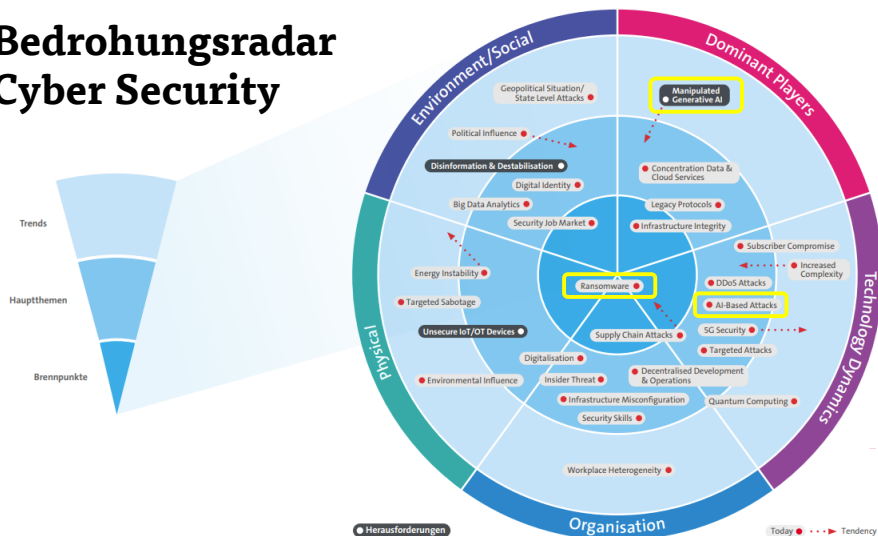
Nächste Schritte

1. NIS-2-Assessment für die eigene Organisation durchführen (lassen):
 - Fallen wir unmittelbar unter die neuen Vorgaben?
 - Welche Folgen ergeben sich mittelbar aufgrund unseres Leistungsspektrums?
 - Was kommt auf uns zu und wie bereiten wir uns darauf vor?
2. Resilienz und Krisenfestigkeit der eigenen Organisation verbessern:
 - GAP-Analyse Informationssicherheit, Aufgaben umsetzen und laufend verbessern (Fürsorgepflichten, ganz unabhängig von gesetzlichen Auflagen)
 - Notfallmanagement aufbauen, prüfen und laufend optimieren

27

27

Bedrohungsradar Cyber Security



28

Quelle: Swisscom Cyber Security Threat Radar

28

Kurz vorgestellt

ALTHAMMER
& KILL

Aktuelle Projekte im Umfeld KI

- KI-Richtlinien
- Beratung zu Produktentwicklung mit KI-Anteilen
- Begleitung von KI-Projekten und Einführung von KI in Organisationen
- Risikobewertung und Datenschutz-Folgenabschätzungen für KI-Lösungen

29

29



**„Künstliche Intelligenz“
zwischen Hype und Realität**

30

Wie funktioniert Machine Learning/KI?

ALTHAMMER
& KILL

Natural Language Processing (NLP)



NLP erlaubt Maschinen, menschliche Sprache zu verstehen und zu generieren. Es wird in sprachgesteuerten Assistenten, Chatbots und zur Vervollständigung von Google-Suchanfragen verwendet.

Maschinelles Lernen (ML)



ML nutzt Algorithmen zur Mustererkennung in großen Datenmengen und bildet die Grundlage für Dienste wie Netflix-Empfehlungen, Google-Suchmaschinen oder Prioritäten in Social-Media-Feeds.

Generative KI



Generative KI kann neue Inhalte wie Texte, Bilder oder Musik erstellen. Sie ist besonders im Online-Marketing wichtig, da sie automatisiert hochwertigen Content generiert.

Deep Learning



Deep Learning, eine Unterdisziplin des maschinellen Lernens, konzentriert sich auf neuronale Netzwerke zur Verarbeitung großer Datenmengen und verbessert die Genauigkeit und Leistung.

31

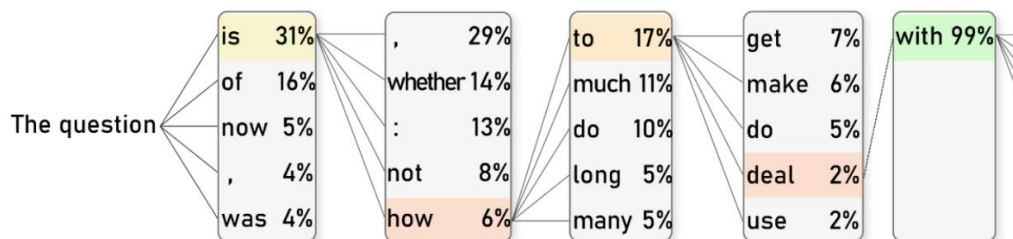
Grafik: Löwenstark

31

Wie funktioniert Machine Learning/KI?

ALTHAMMER
& KILL

The question is how to deal with the issue



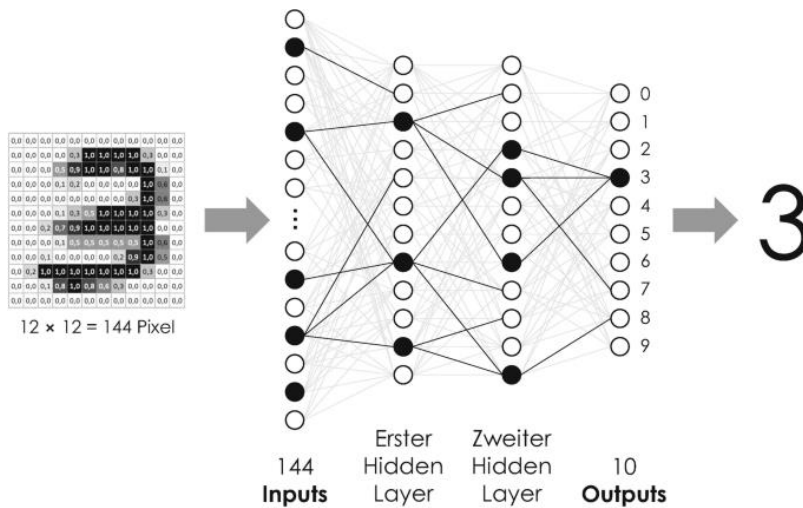
32

(Sobieszek/Price 2022)

32

Wie funktioniert Machine Learning/KI?

ALTHAMMER
& KILL



33

(Lang 2023)

33

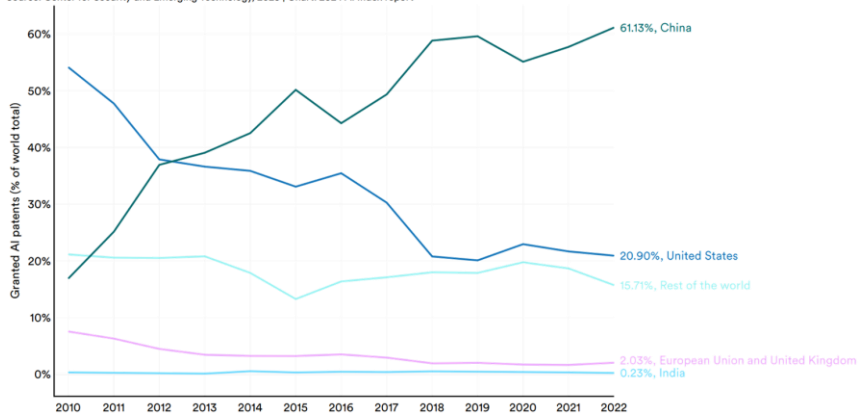
Wie funktioniert Machine Learning/KI?

ALTHAMMER
& KILL

Wo findet KI-Entwicklung statt?

Granted AI patents (% of world total) by geographic area, 2010–22

Source: Center for Security and Emerging Technology, 2023 | Chart: 2024 AI Index report



34

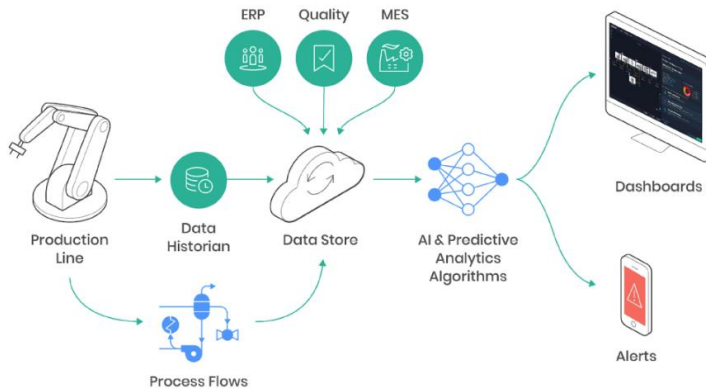
Quelle: Artificial Intelligence Index Report 2024 (Stanford)

34

Wie funktioniert
Machine Learning/KI?

ALTHAMMER
& KILL

Use Case: Predictive Maintenance



35

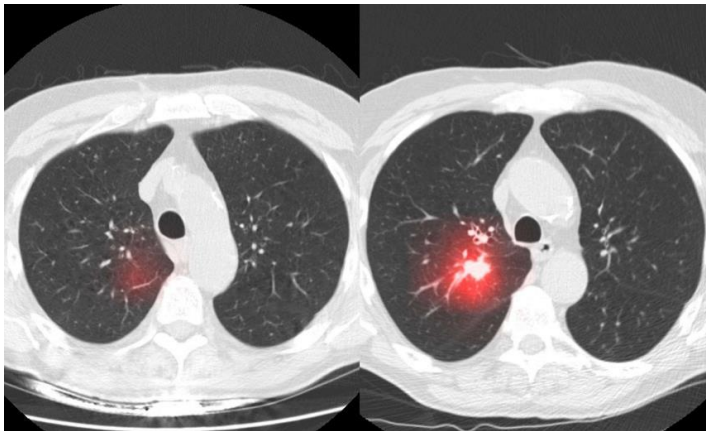
Bildnachweis: Aegasis Labs

35

Wie funktioniert
Machine Learning/KI?

ALTHAMMER
& KILL

Use Case: Krebserkennung



36

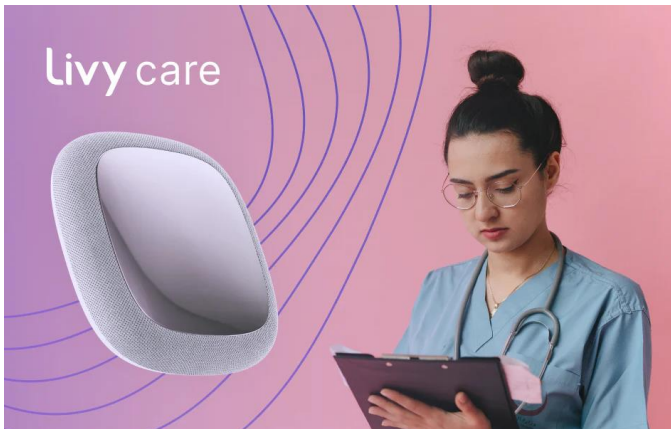
Quelle: Mass Gen Cancer Center

36

Wie funktioniert
Machine Learning/KI?

ALTHAMMER
& KILL

Use Case: Intelligente Raumüberwachung



37

Quelle: Livy Care

37

Wie funktioniert
Machine Learning/KI?

ALTHAMMER
& KILL

Use Case: Social Robots



38

Quelle: Navel Robotics

38

Use Case: Spracherkennung in der Pflege





39

Quelle: Voize

39

Datenschutz und KI

Phase	Fragestellung
 Entwicklung & Training	Einsatzfeld und Rechtmäßigkeit von KI-Systemen
	Erhebung von Trainingsdaten für KI-Systeme
	Verarbeitung von Daten für das Training von KI-Systemen
 Betrieb & Nutzung	Bereitstellung von KI-Systemen
	Nutzung von KI-Systemen
	Umgang mit Ergebnissen von KI-Systemen

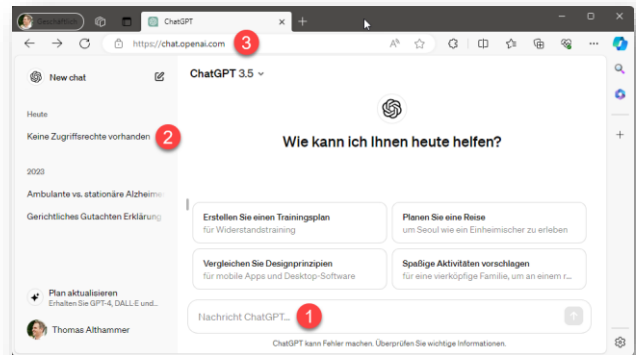
40

40

ChatBots & Datenschutz

Abgesehen von den
„Datenschutz-Basics“:

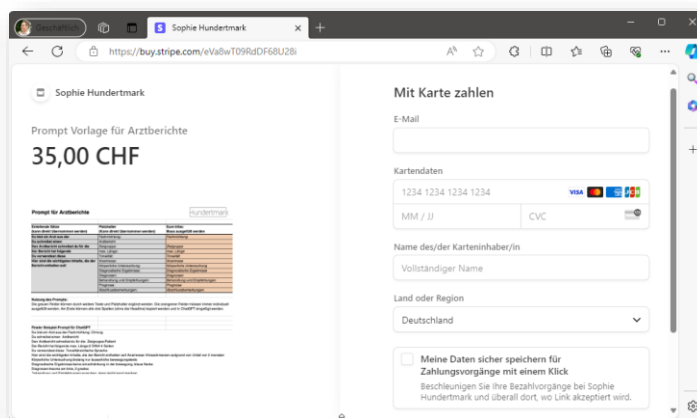
1. Vertrauliches oder personenbezogene Daten im Prompt?
2. Nutzung des Outputs? Lernendes LLM?
3. Wie sind die Datenströme?



41

41

Prompt-Vorlage: Arztbrief mit ChatGPT



42

Quelle: <https://www.sophiehundertmark.com/chatgpt-und-generative-ai-fuer-arztberichte/>

42

Herausforderung Zugriffsrechte

Unternehmensinterne ChatBots:

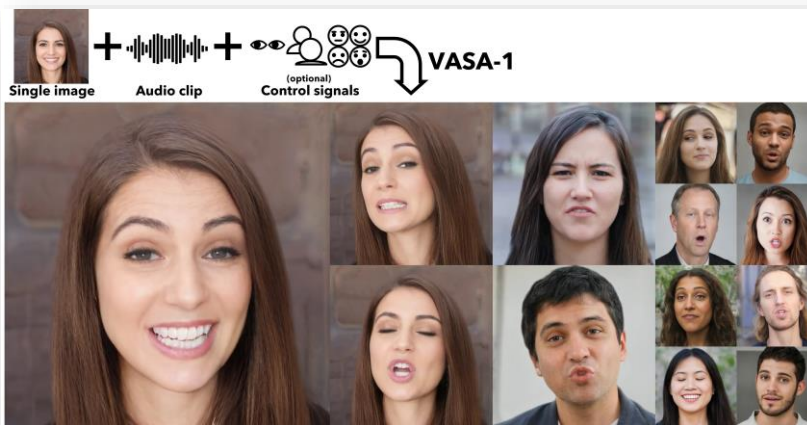
- Qualität der Trainingsdaten (Bias, Diskriminierung, Datenschutz, Schutzrechte Dritter)
- Überprüfung von Prompts – wie Zugriffsrechte handhaben?
- Bewertung und Überprüfung der Ausgabe in Hinblick auf Berechtigung, Korrektheit, etc.



43

43

VASA-1: Lifelike Audio-Driven Talking Faces

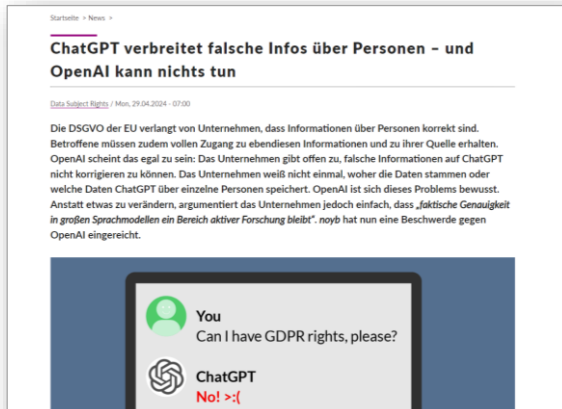


44

Quelle: <https://www.microsoft.com/en-us/research/project/vasa-1/>

44

Problem KI-Halluzination



Halluzination

ist das überzeugend formulierte Ergebnis generativer KI, das nicht durch Trainingsdaten gerechtfertigt zu sein scheint und objektiv falsch sein kann.

Pressemitteilung: <https://noyb.eu/>

45

45

Auswirkung von KI-Halluzination

Risiken
im Umgang mit
Halluzinationen bei
Einsatz von KI im
Gesundheits- und
Sozialwesen



46

46



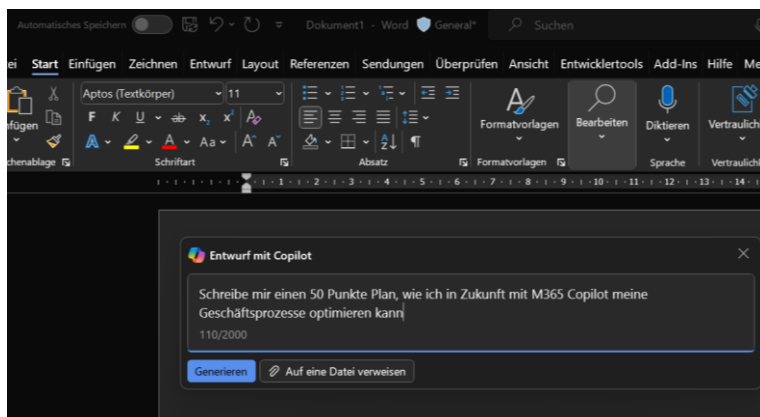
Microsoft Copilot im Kontext Datenschutz und IT-Sicherheit

47

Microsoft Copilot im Kontext
Datenschutz und IT-Sicherheit

ALTHAMMER
& KILL

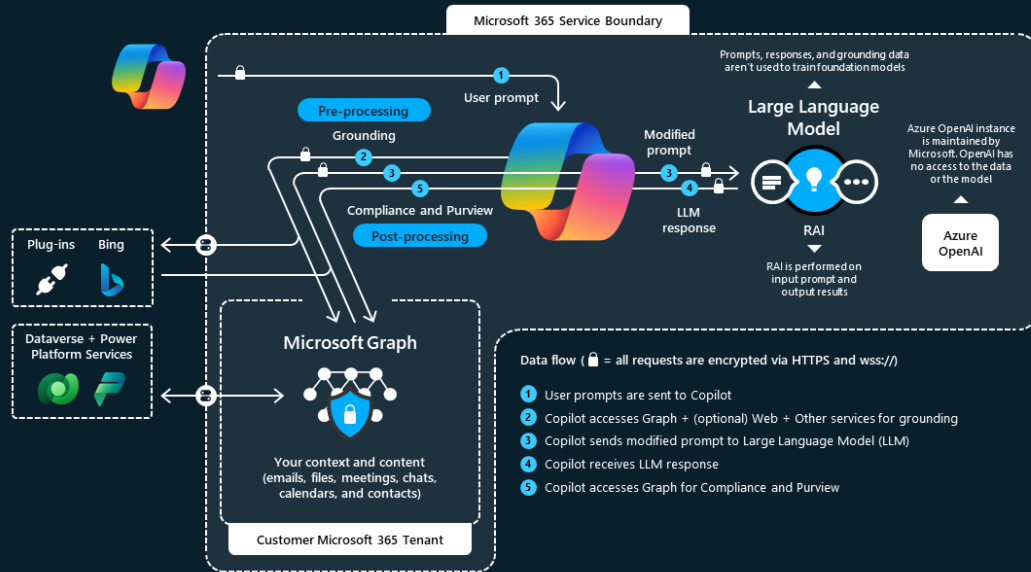
Microsoft Copilot für Microsoft 365



48

48

Microsoft Copilot for Microsoft 365 architecture



49

Microsoft Copilot im Kontext
Datenschutz und IT-Sicherheit

ALTHAMMER
& KILL

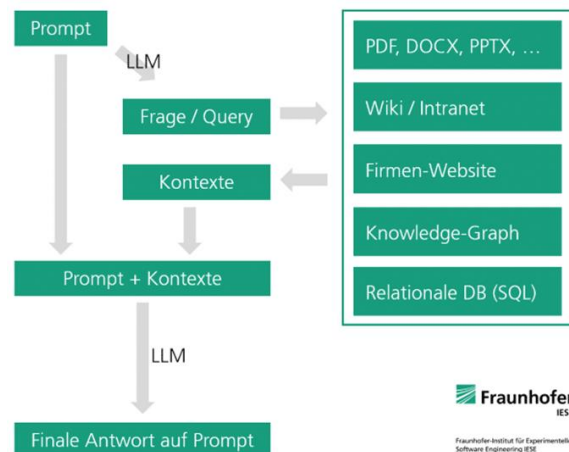
Lücken füllen

Grounding

Prompt wird Kontext gegeben,
Zugriff auf Daten und Quellen,
Callbacks für Rückfragen

Retrieval-Augmented Generation

Einfügen relevanter Fakten aus
externen Datenquellen/Dokumenten



Fraunhofer
IESE
Fraunhofer-Institut für Experimentelles
Software Engineering IES

Quelle: <https://www.iese.fraunhofer.de/blog/retrieval-augmented-generation-rag>

50

50

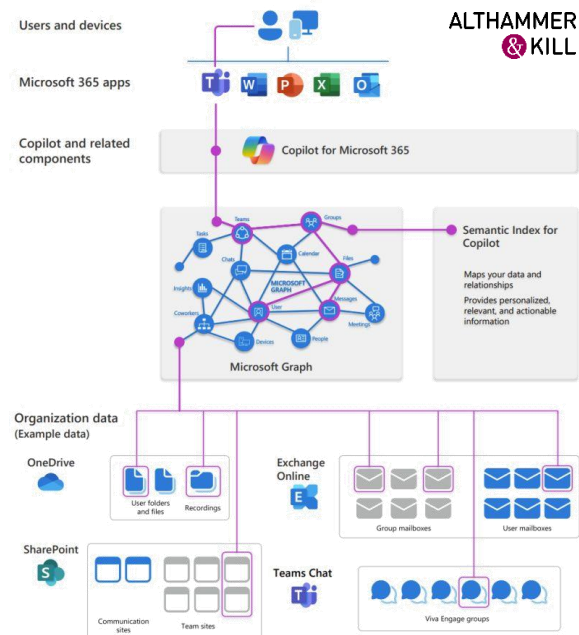
Lücken füllen

Grounding

Prompt wird Kontext gegeben,
Zugriff auf Daten und Quellen,
Callbacks für Rückfragen

Retrieval-Augmented Generation

Einfügen relevanter Fakten aus
externen Datenquellen/Dokumenten



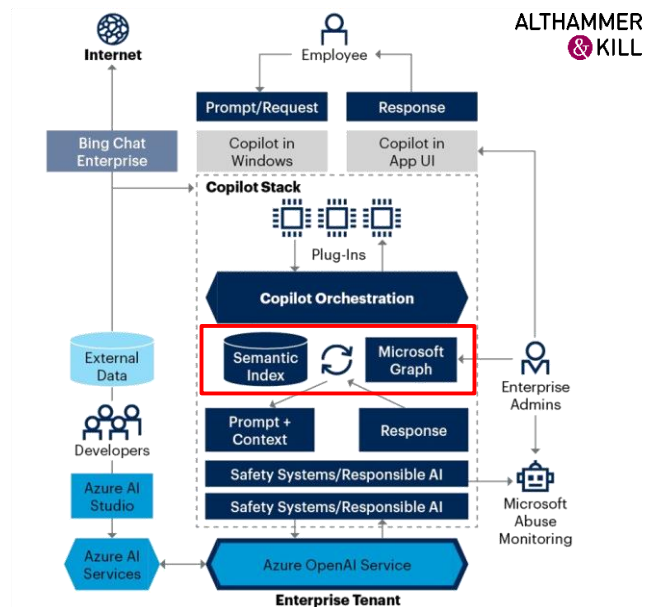
51

Bildnachweis: Microsoft

51

Ihre Daten als Chance & Risiko

- Für eine sinnvolle Nutzung von Microsoft Copilot müssen Ihre Datenbestände strukturiert, klassifiziert und analysierbar sein.
- Wie gut ist heute Ihre Dateiablage strukturiert?



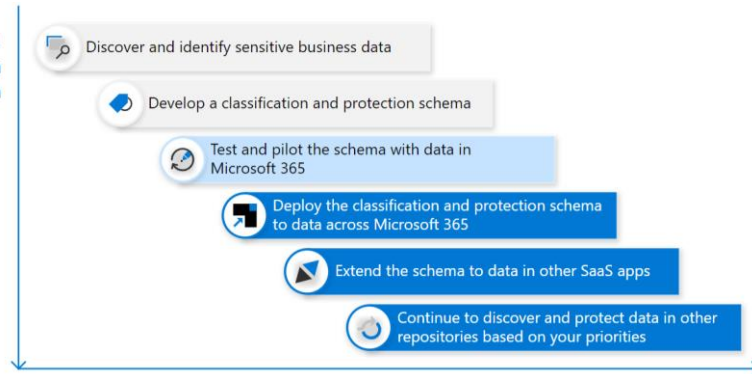
53

Quelle Gartner, <https://twitter.com/mobilegourmet/>

53

Rollout für Copilot vorbereiten

Technical adoption
of information
protection

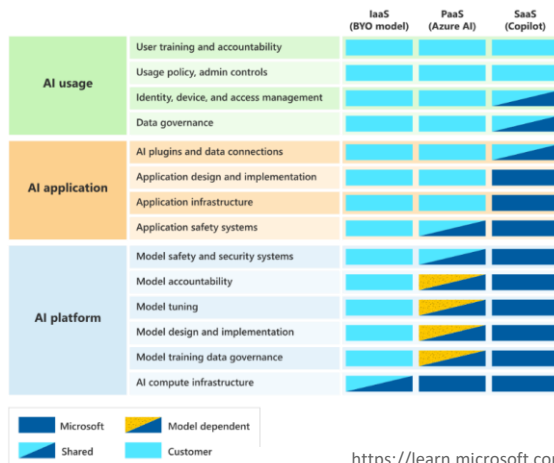


54

Quelle: <https://learn.microsoft.com/en-us/security/zero-trust/copilots/zero-trust-microsoft-365-copilot>

54

Microsoft AI Shared Responsibility Model



Verantwortung bei Einsatz:

1. Sie sind Verantwortliche Stelle nach DSGVO, DSG-EKD & KDG
2. Rechtsgrundlagen, Vertrag, Betroffenenrechte, etc. klären
3. Mitarbeitende anweisen/schulen, KI-Richtlinie veröffentlichen
4. Zugriffsrechte organisieren und deren Umsetzung sicherstellen
5. Datenklassifizierung, d.h. Lebenszyklus Daten/Dokumente
6. Datenquellen orchestrieren

55

<https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility-ai>

55



Hürde Datenschutz? KI & Copilot im Einsatz

56

Hürde Datenschutz?
KI & Copilot im Einsatz

ALTHAMMER
& KILL

Datenschutz bei ChatGPT und Gemini

	ChatGPT Free/Plus EU-TermsOfUse	ChatGPT Team/ Enterprise/API Business-Terms	Google Gemini Privacy-Notice	Google Vertex AI Cloud-Platform-Terms
Auftragsverarbeitung (Abschluss DPA möglich)	🚫 nicht verfügbar	✅ DPA vorhanden	🚫 nicht verfügbar	✅ DPA vorhanden
Nutzung mit personenbezogenen Daten	🚫 nein	✅ möglich	🚫 nein	✅ möglich
Nutzung mit vertraulichen Daten	🚫 nein	⚠ teilweise	🚫 nein	✅ über Vereinbarung
Ausschluss Eigeninteressen Anbieter (Training, Optimierung)	❗ nein/teilweise	✅	🚫 nein	✅
Einsatz im Unternehmen	🚫 nicht empfohlen	✅ möglich	🚫 nicht empfohlen	✅ möglich

57

Stand 04/2024; Quellen u. a. VISCHER, Hunger/Rosenthal

57

Datenschutz bei Copilot und Azure

	Copilot Copilot Pro TermsOfUse	... mit kommerz. Datenschutz BCETermsOfUse	Copilot für Microsoft 365 MS-DPA	Azure OpenAI Services MS-DPA
Auftragsverarbeitung (Abschluss DPA möglich?)	❌ nicht verfügbar	❓ DPA unklar	✅ vorhanden	✅ vorhanden
Nutzung mit personenbezogenen Daten	❌ nein	❓ DPA unklar	✅ möglich	✅ möglich
Nutzung mit vertraulichen Daten	❌ nein	❓ DPA unklar	✅ über Vereinbarung	✅ über Vereinbarung
Ausschluss Eigeninteressen Anbieter (Training, Optimierung)	❌ nein/unklar	❓	✅	✅
Einsatz im Unternehmen	❌ nicht empfohlen	❓ unklar	✅ möglich	✅ möglich

58

Stand 04/2024; Quellen u. a. VISCHER, Hunger/Rosenthal

58

Beispiel Datenschutz „Bing Chat Enterprise“

In Sachen KI-Dienste ist immer eine Analyse der vertraglichen Grundlagen erforderlich!

Online Services excluded from the DPA

Except as provided in the **Product-Specific Terms**, the terms of the DPA do not apply to: Bing Maps Mobile Asset Management Platform, Bing Maps Transactions and Users, Bing Search Services, Azure AI Services in containers installed on Customer's dedicated hardware, **Microsoft Copilot with commercial data protection (formerly known as Bing Chat Enterprise)**, GitHub Offerings, LinkedIn Sales Navigator, Microsoft Defender for IoT (excluding any cloud-connected features), Azure SQL Edge, Azure Stack HCI, Azure Stack Hub, Microsoft Graph data connect for ISVs, Microsoft Genomics, and Visual Studio App Center Test. Each of these Online Services are governed by the privacy and security terms in the applicable **Product-Specific Terms**.

59

Quelle: <https://www.microsoft.com/licensing/terms/product/PrivacyandSecurityTerms/all> (lt. Abruf Mai 2024)

59

Aufgaben Datenschutz bei Einsatz von KI

Voraussetzungen

- Zweck?
- Nutzung Lokal, Hosting, Cloud
- Rechtsgrundlage
- Richtlinien
- Sensibilisierung und Schulung

Anbieter & Lösung

- Eignung
- Sitz/Rechtsrahmen, Datenströme
- Nutzungsbedingungen
- Auftragsverarbeitung bzw. Joint Controllership
- Erlaubter Nutzungsumfang (privat/beruflich/vertraulich)
- Qualität des KI-Modells (Herkunft der Trainingsdaten)
- Eigene Zwecke des Anbieters (Training, Verbesserung?)

Betrieb & Einsatz

- Dokumentation (Verarbeitung und KI-Verfahren)
- Betroffenenrechte (z. B. Auskunft, Widerspruch)
- Datenschutz-Folgenabschätzung
- Risiko-Bewertung AI-Act
- Prozesse, Umgang mit Vorfällen
- Richtigkeit Output

60

60

Priorisierung von KI-Projekten

Risiko

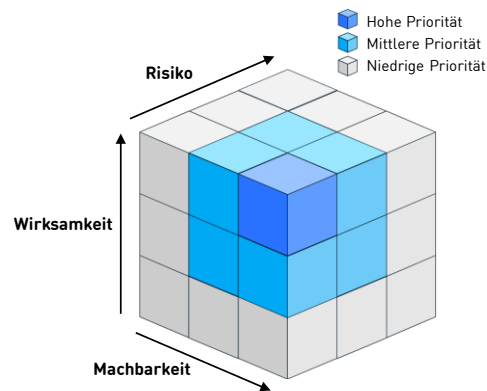
- Datenquellen/Datenqualität und Nutzung
- (IT-)Sicherheitsfragen
- Transparenz und Regularien
- Strategische Fragen
- Lieferkette/Auftragnehmer

Wirksamkeit

- Lösung von Problemen/Arbeitserleichterung
- Qualitätsverbesserung
- Strategische Bedeutung
- Skalierbarkeit
- Kosteneinsparung, Umsatz/Ergebnis

Machbarkeit

- Datenqualität und Architektur
- Reifegrad von Technologie/System
- Personelle Ausstattung
- Veränderungsbereitschaft der Organisation



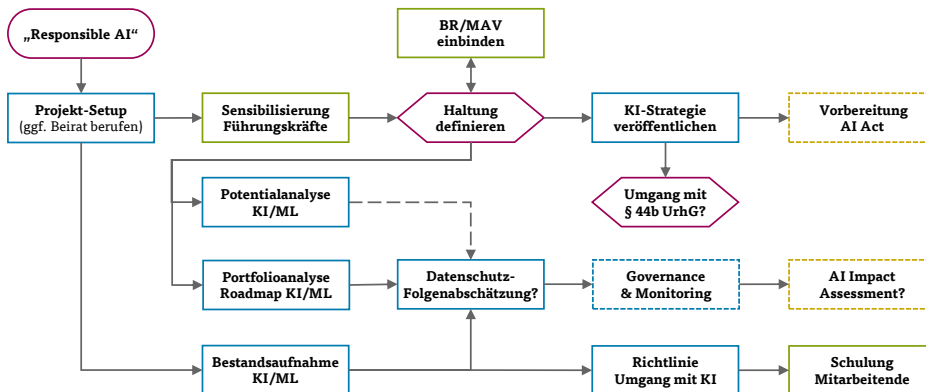
in Anlehnung an McKinsey

61

61



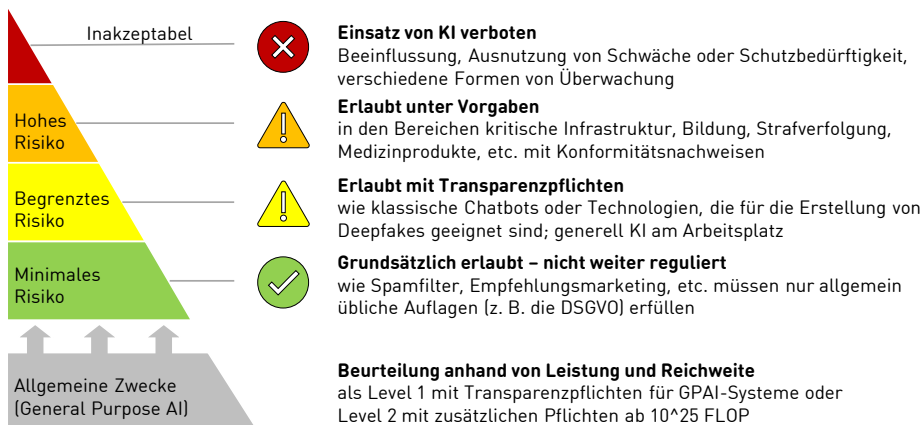
Projektskizze KI im Sozialwesen



62

62

Risikostufen AI Act



63

Stand Gesetzgebungsverfahren 04/2024

63

Global AI Law and Policy Tracker



64

Quelle: Global AI Law and Policy Tracker, IAPP

64

Studie KI in der Sozialwirtschaft



65

65

Praxistage Datenschutz & Informationssicherheit

Aktuelle Entwicklungen und relevante Fakten
zu NIS-2, KI und IT-Recht im Kontext von
Gesundheits- und Sozialwesen, Kirche & Non-Profits



ALTHAMMER
& KILL

04.-06.09.2024

📍 Paderborn

Speaker u. a.:

Prof. Dr. Sabina Jeschke
CEO KI Park e.V.

Felix Neumann
Artikel91.eu

Michael Jacob
Datenschutz-
beauftragter
EKD

Manuel Atug
Gründer unabhängige
AG KRITIS

**Prof. Helmut
Kreidenweis**
Katholische Universität
Eichstätt-Ingolstadt



66

ALTHAMMER
& KILL

Vielen Dank!
*Bleiben Sie mit uns
in Verbindung...*

Tel. +49 511 330603-0
info@althammer-kill.de
www.althammer-kill.de

67



Hinweis und Nutzungsrechte

© Althammer & Kill GmbH & Co. KG – Alle Rechte vorbehalten.

Diese Präsentation wurde nach bestem Wissen anhand des zum Zeitpunkt der Erstellung geltenden Rechtsstandes erstellt. Es wird kein Anspruch auf Vollständigkeit und Richtigkeit erhoben. Die Überlassung der Präsentation erfolgt nur für den internen Gebrauch des Empfängers. Weitergabe oder Veröffentlichung sind nur mit ausdrücklicher vorheriger Zustimmung von Althammer & Kill erlaubt.

Wir verwenden Bilder und Grafiken von:
www.miniansichten.de, www.pixabay.de und www.unsplash.com