

# Einleitung

Es war ein Montag. Natürlich war es ein Montag.

Ihr Vorstand hatte am Wochenende einen Artikel gelesen. Nicht irgendeinen Artikel — den Artikel. Den, den ein Unternehmensberater für ein Magazin geschrieben hat, das hauptsächlich in Flugzeug-Sitztaschen überlebt, weil es zu glatt ist, um darin einzuschlafen und zu nichtssagend, um es wirklich zu lesen. Der Artikel hieß vermutlich „KI verändert alles — ist Ihr Unternehmen bereit?“ und enthielt mindestens ein Jensen-Huang-Zitat, eine Grafik mit exponentiell ansteigender Kurve ohne Achsenbeschriftung sowie die implizite Drohung, dass Unternehmen, die jetzt nicht handeln, 2027 nicht mehr existieren werden.

Spoiler: Die meisten werden noch existieren. Einige davon sogar mit funktionierendem SharePoint.

Montag, 9:04 Uhr. Ihre Inbox: „Wir müssen unbedingt über KI reden.“

Sie haben geseufzt. Leise, professionell, in einer Weise, die im Open-Space-Büro als Nachdenken durchgeht. Dann haben Sie den Kalender geöffnet und einen Termin geblockt, der „KI-Strategie Kickoff“ heißt und bei dem am Ende niemand genau wissen wird, was als nächstes passiert — außer, dass ein weiterer Termin folgt.

Willkommen. Das ist jetzt Ihr Leben.

Falls Sie hoffen, dass dieses Buch anders ist als der Artikel Ihres Vorstands — Sie haben recht. Es ist anders. Es enthält keine Kurven ohne Achsenbeschriftung, kein Jensen-Huang-Zitat und keine implizite Drohung. Was es enthält, ist die Antwort auf die Frage, die sich hinter „Wir müssen unbedingt über KI reden“ eigentlich verbirgt:

Was zum Teufel sollen wir jetzt konkret tun?

Das ist eine legitime Frage. Und erstaunlich selten wird sie beantwortet, ohne dass dabei jemand etwas verkaufen will.

Lassen Sie mich kurz erklären, was in den letzten drei Jahren passiert ist — für alle, die es verschlafen haben, weil sie mit echter Arbeit beschäftigt waren.

November 2022: OpenAI veröffentlichte ChatGPT. Das Internet explodierte. Studenten freuten sich. Professoren bekamen Augenringe. Vorstände lasen Artikel in Flugzeugmagazinen.

Januar 2023: Microsoft investierte zehn Milliarden Dollar in OpenAI. Das war entweder das klügste Investment seit dem iPhone oder der teuerste Impulskauf der Unternehmensgeschichte — die Jury ist noch unterwegs, aber sie neigt sich.

November 2023: Microsoft 365 Copilot wurde allgemein verfügbar. Preis: 30 US-Dollar pro Nutzer und Monat. Reaktion der IT-Welt: gedämpfte Begeisterung, gefolgt von der Frage, wer das eigentlich genehmigen soll.

Seitdem: Jeden Monat neue Features, neue Produkte, neue Preismodelle, neue Compliance-Anforderungen und neue Artikel in Flugzeugmagazinen. Mittendrin: Sie.

Microsoft Copilot ist kein Chatbot. Das ist die erste wichtige Korrektur.

Es ist ein KI-System, das tief in Ihre Unternehmensinfrastruktur eingreift – in Ihre E-Mails, Ihre Dokumente, Ihre Teams-Chats, Ihre Kalendereinträge. Es weiß, was Ihr Unternehmen weiß. Oder genauer: Es weiß, was Ihre Berechtigungsstruktur ihm erlaubt zu sehen – und wenn Ihre Berechtigungsstruktur so aussieht wie in den meisten Unternehmen, also gewachsen, undokumentiert und seit 2019 nicht mehr angefasst, dann weiß Copilot unter Umständen Dinge, die es besser nicht wissen sollte.

Das ist kein Grund zur Panik. Es ist ein Grund zur Vorbereitung.

Der Unterschied zwischen diesen beiden Reaktionen ist ungefähr der Unterschied zwischen einem IT-Leiter, der seinen Job noch hat, und einem, der erklärt, warum Copilot dem neuen Auszubildenden die Gehaltsstruktur der Führungsebene zusammengefasst hat.

Dieses Buch ist nicht für Menschen geschrieben, die KI lieben.

Es ist für Menschen geschrieben, die Verantwortung tragen – und dafür haften, wenn etwas schiefgeht. Für CISOs, die nachts wach liegen und an Prompt Injection denken, ohne genau zu wissen, was das ist, aber ein ungutes Gefühl haben. Für Datenschutzbeauftragte, die ahnen, dass „wir haben einen Auftragsverarbeitungsvertrag mit Microsoft“ nicht die vollständige Antwort auf die DSGVO-Frage ist, aber noch nicht genau wissen, was die vollständige Antwort wäre. Für IT-Leiter, die erklären müssen, was der Unterschied zwischen Copilot, Azure OpenAI und Copilot Studio ist – am besten in einem Satz, weil der Vorstand gleich noch drei andere Termine hat.

Für all diese Menschen ist dieses Buch geschrieben.

Und für alle, die im Meeting sitzen, nicken, und danach jemanden anrufen, der das eigentlich weiß.

Was Sie hier nicht finden werden: Begeisterung um der Begeisterung willen. Die Behauptung, KI löse alle Ihre Probleme. Das Versprechen, nach der Lektüre sei alles klar. Und Jensen Huang.

Was Sie finden werden: Die ehrliche Antwort auf die Frage, was Microsoft Copilot mit Ihren Daten tut – technisch präzise, aber ohne, dass Sie Informatik studiert

haben müssen. Eine Einschätzung des EU AI Acts, die über „wir beobachten das“ hinausgeht. Ein Governance-Framework, das nicht im ersten Quartal in der Schublade verschwindet. Und eine Kostenrechnung, die auch die Positionen enthält, die in keinem Microsoft-Angebot stehen.

Die Fallstudien in diesem Buch sind fiktiv. Die Fehler, die darin gemacht werden, sind es nicht — ich habe sie in verschiedenen Variationen in echten Unternehmen beobachtet, mit echten Konsequenzen und echten Gesichtern, die ich aus Gründen des Datenschutzes durch Musterwerk GmbH, Sparfuchs & Partner und Trendforge Digital GmbH ersetzt habe.

Eine Anmerkung noch.

Ich sieze Sie. Das ist in einem Buch dieser Art eigentlich selbstverständlich, aber ich erwähne es, weil ich gleichzeitig vorhabe, Ihnen die Wahrheit zu sagen — auch wenn sie unbequem ist, auch wenn sie bedeutet, dass ich Ihnen erkläre, dass Ihr Berechtigungskonzept vermutlich in einem bedenklichen Zustand ist, bevor ich Sie persönlich kenne. Das ist kein Angriff. Das ist Statistik.

Betrachten Sie dieses Buch als das Gespräch, das Sie mit einem guten IT-Consultant hätten — einem, der Ihnen nicht nach dem Mund redet, weil er das nächste Projekt verkaufen will, sondern einem, der Ihnen sagt, was Sache ist, damit Sie eine fundierte Entscheidung treffen können.

Das schulde ich Ihnen. Dafür haben Sie bezahlt.

**Ulrich Boddenberg**

Dortmund, 2026

P.S. Wenn Ihr Vorstand fragt, wie das Meeting war: gut. Es war sehr produktiv. Sie haben konkrete nächste Schritte vereinbart.

# Inhaltsverzeichnis

Einleitung.....	2
Was Microsoft aus KI gemacht hat – und warum Sie das jetzt betrifft.....	17
1.1 Wie Microsoft zur KI-Firma wurde.....	18
Der ChatGPT-Schock – und Microsofts Reaktion.....	19
Satya Nadella und die strategische Neuausrichtung.....	19
Das Branding-Problem: Fünf Produkte, ein Name.....	19
November 2023: Copilot für alle – 30 Dollar pro Kopf und Monat.....	20
1.2 Das Portfolio: Was Microsoft mit 'KI' alles meint.....	21
Microsoft 365 Copilot – der Einstieg für Wissensarbeiter.....	22
Azure OpenAI Service – für Entwickler, nicht für Endanwender.....	22
Copilot Studio – eigene KI-Agenten ohne Programmierkenntnisse.....	22
GitHub Copilot – KI für Entwickler.....	22
Copilot for Security – KI für das SOC.....	23
Azure AI Studio und Azure Machine Learning – die Entwicklerplattform.....	23
Power Platform KI – Automatisierung für alle.....	23
Wo beginnt KI und wo endet Marketing?.....	23
1.3 Warum 'wir schauen erst mal' keine Strategie ist.....	28
Shadow AI: Die Entscheidung haben Ihre Mitarbeiter schon getroffen.....	28
Was in der Zwischenzeit bei der Konkurrenz passiert.....	29
Die Halbwertszeit des Beobachtens.....	30
Die echten Kosten des Abwartens.....	30
Was 'wir beobachten das' wirklich bedeutet.....	31
1.4 Wie dieses Buch aufgebaut ist.....	33
Die Kapitelstruktur im Überblick.....	33
1.5 Leseanleitung: Wie Sie dieses Buch am effektivsten nutzen.....	34
Management Summary Kästen – Das Wichtigste in fünf Minuten.....	34
Fallstudien – Was Sie lernen können, und was nicht.....	34
Tabellen – Entscheidungshilfen, keine Dekoration.....	34
Risiko- und Tipp-Kästen – Kontext zu den Hauptaussagen.....	35
Was dieses Buch nicht ist.....	35
Wo stehen Sie wirklich? Eine ehrliche Standortbestimmung.....	37
2.1 Die drei Typen: Wer sind Sie eigentlich?.....	37
Typ 1: Der ehrliche Abwarter.....	38

Typ 2: Der vorsichtige Tester .....	39
Typ 3: Der aktive Pilot .....	39
2.2 Wo Ihre Mitbewerber stehen – und was das für Sie bedeutet .....	41
Die 3%-Zahl: Was sie bedeutet und was nicht .....	41
Google, SAP, Salesforce: Was Ihre Systeme bereits können .....	42
Das wirkliche Wettbewerbsrisiko: Produktivitätslücke und Talente .....	43
2.3 Der ehrliche Selbstcheck: Sind Sie bereit?.....	44
2.4 Was es wirklich kostet – die ehrliche Rechnung.....	48
Die vollständige Kostenrechnung: 100 Nutzer, Mittelstand, Jahr 1 .....	48
ROI-Mythen und was realistisch ist .....	49
2.5 Warum KI-Projekte scheitern – und wie Sie das vermeiden .....	50
Das Governance-First-Prinzip.....	51
Das Pilotprojekt als Lernlabor .....	52
2.6 Die Adoptionsrealität: Was die Zahlen wirklich sagen .....	53
Was 3% wirklich bedeuten .....	54
Aktivierungsrate vs. echte Nutzung.....	54
Prognose 2025–2026: Wo die Kurve hingehet.....	55
Was das für Ihre Entscheidung bedeutet: Jetzt oder nach der Kurve?.....	56
Marktdaten zur Copilot-Adoption: Was die Zahlen konkret bedeuten.....	57
Das Henne-Ei-Problem: Warum Adoption und Vorbereitung sich blockieren .	58
Drei Adoptions-Typen in der Praxis: Schnell, Gründlich, Hängengeblieben....	58
Wie Copilot auf Ihre Daten zugreift – und warum das Ihre Berechtigungsstruktur betrifft .....	61
3.1 Microsoft Graph – das Nervensystem Ihres Tenants .....	61
Der Semantic Index: mehr als eine Suche .....	62
Der Copilot-Verarbeitungsprozess Schritt für Schritt.....	64
3.2 Was Copilot tatsächlich sieht – und was nicht.....	66
Das Effective-Permissions-Prinzip: Ein Praxisbeispiel.....	66
Sensitivity Labels: der zweite Kontrollmechanismus.....	67
3.3 Das Oversharing-Problem – wenn Copilot zu viel weiß .....	68
Warum Oversharing so verbreitet ist .....	70
Oversharing in der Praxis: Drei Szenarien .....	70
3.4 Was Microsoft mit Ihren Daten macht – Fakten statt Gerüchte .....	72
Trainiert Microsoft KI-Modelle mit Ihren Unternehmensdaten? .....	72
Was wird protokolliert? .....	73
3.5 Die EU Data Boundary – was das konkret bedeutet .....	74

Praktischer Check: Ist Ihr Tenant korrekt konfiguriert? .....	75
3.6 Die fünf Fragen, die Sie sich jetzt stellen müssen.....	75
Was Sie mit den Antworten tun .....	78
Fazit: Copilot ist so sicher wie Ihre Berechtigungsstruktur .....	79
Praktische Umsetzung: Die Berechtigungsvereinigung in Phasen.....	80
Copilot und Gast-Nutzer: ein unterschätztes Risiko.....	81
Copilot-Governance: Wer darf Copilot wie nutzen? .....	81
Wie Sie ein Governance-Framework aufbauen, das funktioniert.....	83
4.1 Was „Governance“ bedeutet – und was es nicht ist.....	83
Das Governance-Paradox: Zu wenig kostet mehr als zu viel.....	84
Was Governance konkret leistet – und was nicht .....	85
Shadow AI: Das kostspieligste Governance-Versagen .....	87
4.2 Wer entscheidet – Rollen und Verantwortlichkeiten.....	87
Der KI-Lenkungsausschuss .....	88
Der KI-Koordinator: Dreh- und Angelpunkt im Alltag.....	88
Was passiert, wenn niemand verantwortlich ist.....	89
Thomas Berger bekommt eine neue Aufgabe .....	90
CISO und DSB: Keine Erweiterungen, sondern Kernrollen.....	90
4.3 Die KI-Richtlinie: Was rein muss – und was nicht.....	91
10 Pflichtinhalte jeder KI-Richtlinie .....	93
4.4 Abteilungen einbinden – ohne dass alle gleichzeitig klagen .....	95
Die fünf schwierigen Abteilungen und wie man sie einbindet .....	95
Das Schulungskonzept: Wer braucht was wann .....	97
Change Management: Was funktioniert und was nicht .....	98
Die Pilot-Begleitung: Monitoring ohne Überwachung.....	98
Die „Das-haben-wir-doch-schon“-Falle .....	99
Welche Abteilungen zuerst?.....	99
Abteilungsspezifische Herausforderungen.....	100
Die drei häufigsten Abteilungs-Rollout-Fehler .....	101
4.5 Das Pilotprojekt: Wie man es richtig macht.....	101
Pilotgröße und Gruppenauswahl .....	102
Technische Vorbereitung vor dem Pilot .....	103
Abbruchkriterien: Wann man aufhören muss.....	104
Die Abschlussevaluation: Was eine valide Entscheidungsgrundlage ist .....	105
Abbruchkriterien – wann Sie den Pilot stoppen .....	106
Erfolgsmessung – was Sie tatsächlich messen.....	107

Was nach dem Pilot passiert .....	108
4.6 Fallstudie Musterwerk GmbH: Vom Chaos zur Governance.....	108
Monat 1: Die Entscheidung und ihre Nebenwirkungen .....	109
Monat 2: Der Governance-Aufbau .....	109
Monat 3: Die KI-Richtlinie und der Betriebsrat .....	109
Monat 4: Der Pilot beginnt .....	110
Monat 5: Der Überraschungsmoment.....	110
Monat 6: Abschlussevaluation und Entscheidung.....	110
Was andere Unternehmen aus Musterwerk lernen können.....	111
Das Rückkehr-Investment: Wann lohnt sich Governance?.....	115
Wie Sie Betriebsrat, Belegschaft – und sich selbst – vor Shadow AI schützen.....	117
5.1 Was Shadow AI ist – und warum Verbote nicht funktionieren.....	118
Shadow AI – die Definition .....	118
Warum Verbote nicht funktionieren – Psychologie und Praxis.....	119
Der Governance-Ansatz: Kontrollierter Wildwuchs statt Wildwuchs .....	121
5.2 Wie Sie Shadow AI in Ihrem Unternehmen erkennen.....	121
Methode 1: Netzwerk-Monitoring und DLP .....	121
Methode 2: Anonyme Mitarbeiterbefragung .....	122
Methode 3: App-Nutzungsanalyse und Browser-Extension-Audit.....	122
5.3 Wie Sie den Betriebsrat einbinden – rechtlich korrekt, ohne Drama .....	124
Die rechtliche Grundlage: §87 Abs. 1 Nr. 6 BetrVG .....	124
Die Betriebsvereinbarung: Pflichtbestandteile und Verhandlungsstrategie ...	125
5.4 Wie eine wirksame KI-Nutzungsrichtlinie aussieht.....	127
Aufbau und Pflichtinhalte .....	127
5.5 Change Management: Wie Sie die Belegschaft mitnehmen .....	129
Das Champions-Programm: Peer-Learning statt Top-Down-Schulung .....	130
5.6 Fallstudie Trendforge Digital: Wenn alle eine Meinung haben.....	132
Was die DSGVO von Ihnen verlangt – bevor Copilot live geht.....	136
6.1 Der Auftragsverarbeitungsvertrag – was Microsoft zusagt (und was nicht) 137	
6.2 Die Datenschutz-Folgenabschätzung – wann sie Pflicht ist und was sie enthalten muss.....	141
Was die DSFA enthalten muss – vier Pflichtbestandteile.....	143
Wie lange dauert eine DSFA? Realistische Zeitplanung.....	144
6.3 Besondere Kategorien personenbezogener Daten – die unsichtbare Grenze145	
Wo besondere Kategorien in Microsoft 365 auftauchen .....	146
Drei konkrete Szenarien – und was sie kosten können .....	147

Was Sie jetzt prüfen müssen .....	148
Technische Maßnahmen gegen Art.-9-Verarbeitung durch Copilot.....	149
6.4 Dokumentationspflichten – was Sie nachweisen müssen, bevor der Prüfer klingelt.....	150
Die Mindest-Dokumentation vor dem Go-live .....	151
Was „dokumentiert“ konkret bedeutet.....	152
Das Verarbeitungsverzeichnis: Was der VVT-Eintrag für Copilot enthalten muss .....	153
Informationspflichten gegenüber Beschäftigten .....	153
Löschkonzept: Was passiert mit Copilot-Daten?.....	154
Rechenschaftspflicht in der Praxis: Was „nachweisen“ bedeutet.....	155
Betroffenenrechte bei Copilot: Auskunft, Löschung, Widerspruch.....	155
6.5 Aufsichtsbehörden und Meldepflichten – was passiert, wenn es schiefgeht.....	156
Was ist eine Datenpanne bei Copilot?.....	156
Bußgelder: Was Art. 83 DSGVO für Copilot-Verstöße bedeutet .....	158
6.6 Fallstudie: Sparfuchs & Partner – der DSB, der zu spät informiert wurde.....	160
Das Problem: DSGVO trifft § 203 StGB .....	161
Die Maßnahmen: Was Sparfuchs in drei Monaten aufgebaut hat.....	162
Die Lehren aus Sparfuchs: Drei Essentials.....	163
Was der EU AI Act von Ihnen erwartet – konkret und ohne Juristendeutsch.....	165
7.1 Der EU AI Act als Nutzer – warum er auch für Unternehmen gilt, die keine KI entwickeln.....	166
7.2 Risikoklassen – welche Einstufung Ihre Microsoft-KI-Tools trifft.....	168
Verbotene KI-Praktiken nach Art. 5 EU AI Act .....	170
7.3 Verbote und Hochrisiko – was Sie nicht tun dürfen .....	171
Hochrisiko-Szenarien mit Microsoft-KI.....	173
7.4 Nutzerpflichten – was Sie als Deployer konkret leisten müssen .....	174
7.5 Zeitplan – alle Stichtage mit konkreten Handlungspflichten.....	178
August 2024: In Kraft getreten .....	178
Februar 2025: Verbote gelten – und Governance-Strukturen .....	178
August 2025: GPAI-Modell-Pflichten .....	179
August 2026: Hochrisiko-Systeme.....	180
August 2027: Volle Geltung .....	180
Was konkret bis wann umgesetzt sein muss .....	180
Bis August 2025: GPAI-Modell-Transparenz intern sicherstellen .....	180
Bis August 2026: Hochrisiko-Pflichten für Annex-III-Systeme.....	181
Bis August 2027: Vollständiges KI-Inventar und Abschluss-Audit.....	181

7.6 Dokumentation und AI Literacy – was nachweisbar vorliegen muss .....	182
AI Literacy: Art. 4 und was er bedeutet .....	182
Was „AI Literacy“ in der Praxis bedeutet.....	184
KI-Inventar und Systemdokumentation.....	184
Was dokumentiert sein muss – eine Checkliste .....	186
Was ein CISO über KI-Sicherheitsrisiken wissen muss .....	189
8.1 Angriffsvektoren – wie KI neue Angriffsflächen schafft.....	190
8.2 Prompt Injection – die wichtigste neue Angriffsmethode.....	192
8.3 KI als Waffe – wie Angreifer KI einsetzen .....	195
8.4 Copilot for Security – was es leistet und was nicht .....	198
8.5 Sofortmaßnahmen – was jeder CISO heute umsetzen kann .....	201
8.6 MCP-Sicherheit – Model Context Protocol und seine Risiken .....	203
Was Entscheider jetzt entscheiden müssen .....	206
Konkrete Governance-Empfehlungen .....	207
Was der Standard noch nicht löst .....	208
Was Sie wirklich bezahlen – und was die Lizenz verschweigt .....	211
9.1 Das Lizenzmodell – was Microsoft verkauft und wie es aufgebaut ist .....	211
Microsoft 365 Copilot: Die Hauptlizenz .....	212
Die Voraussetzung: M365 E3 oder E5.....	212
Abb. 9.1 – Lizenzmodell-Vergleichsmatrix aller Copilot-Varianten .....	213
Copilot Chat: Die kostenlose Alternative .....	213
Copilot Studio: Wenn Sie eigene KI-Agenten bauen wollen.....	214
GitHub Copilot und Security Copilot: Andere Produktfamilien.....	214
9.2 Die versteckten Kosten – was im Angebot nicht steht .....	215
Die zehn Kostenkategorien, die kein Angebot nennt .....	215
Abb. 9.2 – Architektur der versteckten Kosten .....	215
Abb. 9.3 – Was das Angebot zeigt vs. tatsächliche Gesamtkosten .....	217
Der Multiplikator-Faktor .....	217
9.3 ROI-Mythen – warum die Produktivitätsstudien vorsichtig zu lesen sind ..	218
Was unabhängige Studien sagen .....	219
Was messbar ist – und was nicht.....	219
Die drei ehrlichsten Fragen vor der ROI-Entscheidung.....	219
Abb. 9.4 – ROI-Analyse: Microsoft-Versprechen vs. Praxismessungen .....	219
Das Problem mit der 40-Prozent-Produktivitätsbehauptung .....	220
9.4 Wann lohnt es sich – eine ehrliche Rechnung .....	221
Drei Szenarien im Vergleich.....	221

Abb. 9.5 – Break-Even-Analyse: Wann rechnet sich Copilot?.....	222
Wie viele Nutzer wirklich Copilot brauchen .....	222
Was viele Entscheider beim Piloten falsch machen .....	223
Die hidden ROI-Faktoren: Was oft vergessen wird .....	223
Abb. 9.6 – Lizenzoptimierung: Wer braucht welche Lizenz? .....	223
9.5 Fallstudie Trendforge Digital – ein vollständiges Kostenmodell.....	225
Abb. 9.7 – Trendforge: Geplante vs. tatsächliche Kosten nach 12 Monaten ...	226
Die vollständige Kostenrechnung .....	226
Der ROI – was gemessen werden konnte .....	227
Lessons learned – was Trendforge beim nächsten Mal anders machen würde	227
Was Trendforge beim zweiten Versuch besser gemacht hat .....	227
9.6 Preiserhöhung Juli 2026 – was sich ändert und was das für Sie bedeutet...	228
Was sich ab Juli 2026 konkret ändert.....	228
Abb. 9.8 – Preiserhöhung Juli 2026: Welche SKUs steigen wie stark.....	228
Was für laufende Verträge gilt .....	229
Abb. 9.9 – Gesamtkosten-Zeitstrahl: 100 Nutzer, 12 Monate inkl. Preiserhöhung .....	229
Die strategische Abwägung: Jetzt abschließen oder warten? .....	230
Abb. 9.10 – Kostenmodell-Vergleich: Copilot vs. selbst gebaut vs. Drittanbieter .....	231
Was die Preiserhöhung für Ihre mehrjährige Kalkulation bedeutet.....	231
Welche SKUs betroffen sind – konkret .....	233
Was mit laufenden Verträgen passiert .....	234
Was die Preiserhöhung über Microsofts Strategie sagt.....	234
Die ehrliche Zusammenfassung: Was Copilot ist und was nicht.....	235
Wie Sie die richtige Entscheidung treffen – strukturiert, nicht aus dem Bauch....	237
10.1 Der Entscheidungsrahmen – wie man strategische KI-Entscheidungen strukturiert .....	237
Die häufigsten Entscheidungsfehler .....	238
Der strukturierte Dreischritt.....	239
Was vor der Entscheidung feststehen muss .....	241
10.2 Build vs. Buy – wann Azure OpenAI-Eigenentwicklung, wann Copilot.....	242
Wann Copilot M365 die richtige Wahl ist .....	243
Wann Azure OpenAI sinnvoll ist.....	243
10.3 Selbst bauen – was das wirklich bedeutet .....	245
Minimum-Ressourcen für Eigenentwicklung.....	245
Warum Eigenentwicklungen scheitern .....	246

RAG: Wie eigene Unternehmensdaten sicher eingebunden werden .....	246
10.4 Der Stufenplan – Pilot, Rollout, Vollbetrieb .....	247
Phase 0: Vorbereitung (4–6 Wochen) .....	248
Phase 1: Pilot (8–12 Wochen) .....	248
Erfolgskriterien für den Pilot .....	249
Phasen 2–4: Rollout und Vollbetrieb .....	250
Was einen misslungenen Pilot von einem erfolgreichen unterscheidet.....	252
Die Kostenfrage im Vollbetrieb .....	253
Wann ist die Entscheidung für Copilot die falsche?.....	254
Worauf Sie sich vorbereiten sollten – auch wenn Sie heute noch keinen Copilot haben.....	256
11.1 Agentic AI – was sich grundlegend ändert .....	256
11.2 Wave 3 und Agent 365 – was Microsoft ankündigt und was davon realistisch ist.....	259
11.3 Haftung – wer haftet wenn ein Agent einen Fehler macht .....	262
11.4 Das Tempo-Problem – warum schnelle Features zu langsamer Entscheidungskultur passen müssen.....	264
11.5 Was stabil bleibt – worauf Sie jetzt investieren können .....	266
11.6 Jetzt handeln – konkrete Maßnahmen unabhängig vom KI-Reifegrad ...	269
Maßnahme 1: Berechtigungsaudit.....	270
Maßnahme 2: DSB einbinden .....	271
Maßnahme 3: Betriebsrat informieren .....	271
Maßnahme 4: KI-Richtlinie skizzieren .....	271
Maßnahme 5: IT-Team schulen .....	272
Schlusswort – Die Entscheidung ist bereits gefallen .....	274
Anhang A – Checkliste: Tenant-Readiness vor dem Copilot-Rollout .....	277
Anhang B – Checkliste: DSGVO und Datenschutz vor dem Go-live .....	279
Anhang C – Checkliste: EU AI Act – Wo stehen Sie heute?.....	281
Anhang D – Checkliste: Security-Review vor dem Copilot-Einsatz .....	283
Anhang E – Checkliste: Betriebsvereinbarung und Mitbestimmung.....	285
Anhang F – Checkliste: Shadow-AI-Governance .....	287
Anhang G – Checkliste: Pilotprojekt-Steuerung .....	289
Anhang H – Checkliste: Kostenplanung und Budget .....	291
Anhang I – Checkliste: Governance-Framework-Einführung.....	294
Anhang J – Checkliste: Change Management und Kommunikation .....	296
Anhang K – Entscheidungsmatrix: Copilot, Azure OpenAI oder Drittanbieter?...	298
Anhang L – Über den Autor und sein Angebot .....	300

Ulrich Boddenberg – Drei Jahrzehnte. Kein Lehrstuhl. Dafür Praxis.....	300
Beratungsangebot – Wenn das Buch nicht reicht .....	300
KI-Readiness-Analyse zum Festpreis.....	300
Governance-Konzeption und Rollout-Begleitung.....	301
Projektberatung und Troubleshooting.....	301
Kontakt.....	301

# Was Microsoft aus KI gemacht hat — und warum Sie das jetzt betrifft

## MANAGEMENT SUMMARY — Was Sie in Kapitel 1 in 5 Minuten wissen müssen

Microsoft hat zwischen 2019 und 2024 über 13 Milliarden US-Dollar in OpenAI investiert und damit das gesamte KI-Portfolio neu ausgerichtet. Das ist keine Produktstrategie mehr — das ist eine Neupositionierung des Unternehmens.

Was das für Sie bedeutet:

- Microsoft 365 Copilot ist kein Chatbot — er greift tief in Ihre E-Mails, Dokumente und Chats ein.
- Der Begriff 'Copilot' bezeichnet bei Microsoft mindestens fünf verschiedene Produkte. Welches welche Lizenz braucht und was es darf, ist nicht trivial.
- 'Wir beobachten das erstmal' ist eine Entscheidung — und hat Konsequenzen. Mitarbeiter nutzen KI bereits, ob Sie es wollen oder nicht.
- Google, Salesforce und SAP schlafen nicht. Der Abstand zu Konkurrenten, die jetzt handeln, wächst jeden Monat.
- Dieses Buch hilft Ihnen, eine fundierte Entscheidung zu treffen — nicht aus dem Bauch, sondern auf Basis von Fakten und konkreten Werkzeugen.

Zeitaufwand für Erstentscheidung nach Lektüre dieses Kapitels: ca. 45 Minuten — deutlich kürzer als das nächste Meeting über KI-Strategie, bei dem am Ende wieder niemand weiß, was als nächstes passiert.

## Microsoft KI-Portfolio — Architektur-Übersicht 2024

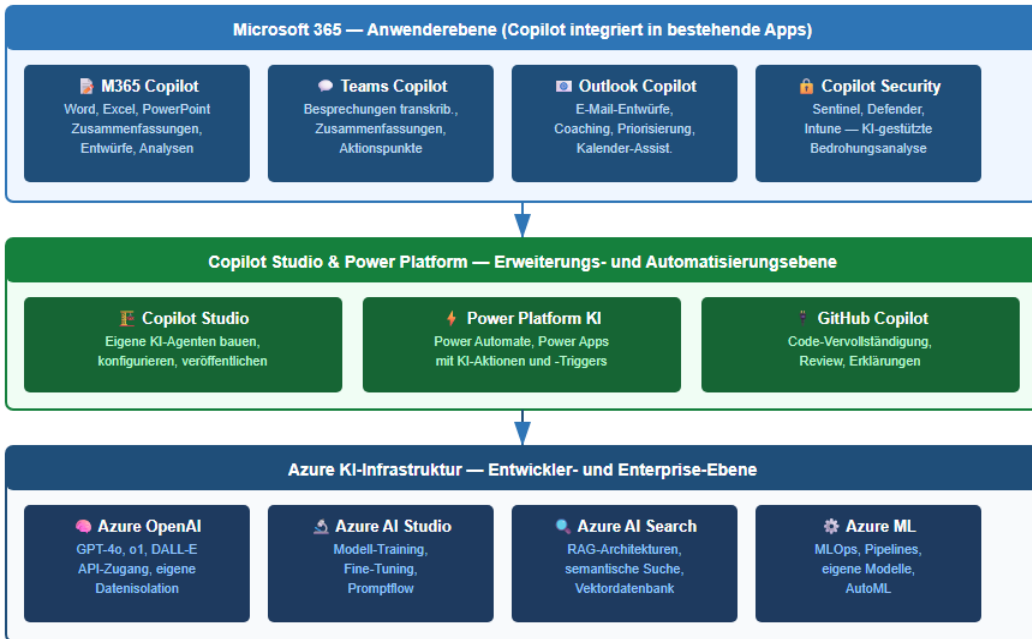


Abb. 1.1 — Microsoft KI-Portfolio — Alle Ebenen und Produkte im Überblick (Stand: 2024)

Abb. 1.1 — Microsoft KI-Portfolio — Alle drei Ebenen: M365-Anwenderebene, Copilot Studio und Azure KI-Infrastruktur

### 1.1 Wie Microsoft zur KI-Firma wurde

Es gibt eine Lesart der Geschichte, in der Microsoft schlicht das Glück hatte, zum richtigen Zeitpunkt am richtigen Tisch zu sitzen. Eine andere Lesart sagt, dass Satya Nadella eines der risikoreichsten Wetten der Unternehmensgeschichte eingegangen ist — und damit recht behalten hat. Wahrscheinlich sind beide Lesarten korrekt.

Der Anfang liegt im Jahr **2019**. Microsoft investierte eine Milliarde US-Dollar in OpenAI, ein damals noch weitgehend unbekanntes KI-Forschungslabor in San Francisco. Die Berichterstattung war freundlich, aber unaufgeregt. Wer sich die Reaktion der Finanzpresse aus jener Zeit ansieht, findet Sätze wie 'strategisches Investment' und 'spannender Schritt im Bereich KI-Forschung'. Niemand ahnte, was daraus werden würde.

2020 sicherte sich Microsoft die Exklusivlizenz für GPT-3 — zu einem Zeitpunkt, als die meisten Unternehmenslenker noch nicht wussten, was ein Large Language Model ist. Diese Lizenz bedeutete: Wenn GPT-3 irgendwann kommerziell relevant werden sollte, hatte Microsoft eine Startposition, die kein Wettbewerber in dieser Form einholen konnte. Google hatte eigene Sprachmodelle, Amazon hatte AWS, aber die direkte Partnerschaft mit dem führenden KI-Labor blieb Microsofts Alleinstellungsmerkmal.

2021 folgte der **Azure OpenAI Service** — zunächst als eingeschränkte Vorschau für ausgewählte Unternehmenskunden. Microsoft begann, die OpenAI-Technologie in seine Cloud-Infrastruktur zu integrieren. Das war kein Meilenstein für Endanwender, aber ein kritischer Schritt: Azure wurde zur Plattform, auf der

OpenAI-Modelle für Unternehmen verfügbar gemacht werden sollten — mit allen Compliance- und Sicherheitsversprechen, die Enterprise-Kunden erwarten.

## Der ChatGPT-Schock — und Microsofts Reaktion

Im November 2022 veröffentlichte OpenAI ChatGPT. Was danach passierte, lässt sich kaum übertreiben. In fünf Tagen hatte ChatGPT eine Million Nutzer. In zwei Monaten waren es 100 Millionen. Kein Dienst in der Geschichte des Internets hatte dieses Wachstumstempo erreicht.

Für Microsoft war das eine zweiseitige Situation. Einerseits: Man hatte investiert, man hatte die Lizenz, man war bereit. Andererseits: ChatGPT war ein Consumer-Produkt und lief direkt auf der OpenAI-Infrastruktur — nicht auf Azure. Microsoft musste schnell zeigen, dass es die Technologie in eigene Produkte übersetzen kann.

Im Januar 2023 folgte die nächste Investitionsrunde — diesmal **10 Milliarden US-Dollar**. Das war kein Investmententscheid mehr, das war ein öffentliches Bekenntnis: Microsoft positionierte sich als KI-Unternehmen. Satya Nadellas früheres Motto 'Mobile First, Cloud First' wurde still durch 'AI First' ersetzt — nicht durch einen offiziellen Slogan, sondern durch die Produktentscheidungen der folgenden 18 Monate.

Im Februar 2023 startete Microsoft **Bing mit GPT-4-Integration**. Die Reaktion der Presse war begeistert. Die tatsächliche Marktdurchdringung blieb bescheiden — Google hält noch immer über 90 Prozent des Suchmarkts. Aber Bing war nicht das Ziel. Bing war die Demonstration, dass Microsoft KI in Produkte integrieren kann. Der eigentliche Schachzug folgte später.

## Satya Nadella und die strategische Neuausrichtung

Satya Nadella, seit 2014 CEO von Microsoft, hat in seiner Amtszeit bereits eine erfolgreiche Transformation vollzogen: von einem Unternehmen, das hauptsächlich Windows und Office verkaufte, zu einem Cloud-Konzern, dessen wichtigstes Produkt Azure ist. KI ist die zweite Transformation — und diesmal geht es schneller. Nadellas öffentliche Aussagen zu KI sind bemerkenswert konkret: Er beschreibt KI nicht als Produktfeature, sondern als neue Rechenebene — vergleichbar mit der Einführung von Client-Server-Architektur in den 1990er Jahren oder dem Übergang zu Cloud in den 2010er Jahren.

Was Nadella richtig eingeschätzt hat und was viele Beobachter unterschätzten: Generative KI ist keine neue Produktkategorie, die neben bestehende Produkte gestellt wird. Sie ist eine Eigenschaft, die bestehende Produkte verändert — so wie das Hinzufügen von Internetfähigkeit in den 1990er Jahren jedes Softwareprodukt verändert hat. Wer das früh versteht, hat einen strukturellen Vorteil, der sich nicht durch ein einzelnes Investment einholen lässt. GitHub Copilot war das am schnellsten wachsende Produkt in der Geschichte von GitHub — und GitHub selbst gehörte Microsoft erst seit 2018.

Für Sie als Entscheider bedeutet das: Microsoft wird nicht damit aufhören, KI in alle seine Produkte zu integrieren. Das ist keine Option mehr, die evaluiert wird — es ist die Richtung des Unternehmens. Die Frage ist nicht, ob Microsoft KI in Ihre Infrastruktur bringt, sondern wie Sie damit umgehen, wenn es passiert. Und es passiert bereits.

## Das Branding-Problem: Fünf Produkte, ein Name

Microsoft hat im Jahr 2023 eine Entscheidung getroffen, die aus Marketingperspektive nachvollziehbar, aus Kundenperspektive aber eine Quelle dauerhafter Verwirrung ist: Alles, was KI enthält, heißt 'Copilot'. Das ist die Marke. Der Inhalt dahinter ist radikal unterschiedlich.

GitHub Copilot für Entwickler gibt es seit 2022 und hat mit Microsoft 365 Copilot für Wissensarbeiter nichts gemein außer dem Namen – und dem Umstand, dass beide auf OpenAI-Modellen basieren. Copilot Studio ist wieder etwas anderes: ein Low-Code-Tool, mit dem eigene KI-Agenten gebaut werden können. Copilot for Security richtet sich an SOC-Analysten und ist in Microsoft Sentinel integriert. Copilot+ schließlich bezeichnet KI-fähige Windows-Geräte mit Neural Processing Unit. Fünf Produkte, ein Name – das ist Branding-Strategie, keine Produktarchitektur.

Das Ergebnis in der Praxis: Wenn in einer Führungsrunde jemand sagt 'wir sollten Copilot einsetzen', weiß niemand genau, worüber gesprochen wird. IT-Budgets werden für das falsche Produkt geplant, Pilotprojekte starten mit falschen Erwartungen, und Governance-Überlegungen setzen am falschen Punkt an. Die Faustregel für jedes Meeting: Klären Sie zuerst, über welches Copilot-Produkt gesprochen wird. Das allein verhindert mehr Fehler als die meisten KI-Schulungen.

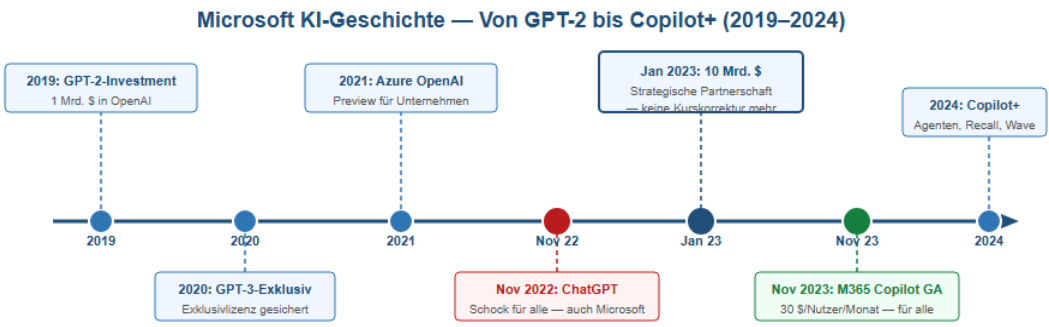


Abb. 1.2 — Microsoft KI-Zeitstrahl 2019–2024 — Von der ersten OpenAI-Beteiligung bis Copilot+

Abb. 1.2 — Microsoft KI-Zeitstrahl 2019–2024: Von der ersten OpenAI-Beteiligung bis Copilot+

### November 2023: Copilot für alle — 30 Dollar pro Kopf und Monat

Im November 2023 wurde Microsoft 365 Copilot allgemein verfügbar. Preis: 30 US-Dollar pro Nutzer und Monat, on top zu bestehenden M365-Lizenzen. Das war der Moment, an dem KI zu einer Beschaffungsentscheidung wurde – und nicht mehr nur zu einem Strategiethema.

Seitdem hat Microsoft das Portfolio konsequent erweitert. GitHub Copilot für Entwickler, Copilot for Security für IT-Sicherheitsteams, Copilot Studio für die Erstellung eigener KI-Agenten, Copilot+ als Bezeichnung für KI-integrierte Hardware. Und wer jetzt den Überblick verloren hat: Das ist normal. Microsoft hat in weniger als zwei Jahren mehr KI-Produkte unter dem Namen 'Copilot' gestartet als die meisten Unternehmen in einem Jahrzehnt an IT-Projekten.

Der Name 'Copilot' ist dabei keine Produktbezeichnung mehr – er ist eine Marke, die auf alles angewendet wird, was bei Microsoft KI enthält. Das ist für Endanwender verwirrend, für IT-Abteilungen eine Quelle dauerhafter Verwirrung und für

Lizenzentscheidungen ein eigenes Kapitel. Spoiler: Sie bekommen dieses Kapitel. Es ist Kapitel 9.

**Tabelle 1.1 – Microsoft KI-Meilensteine 2019–2024**

Jahr	Ereignis	Bedeutung für Unternehmen
2019	1 Mrd. \$ Investment in OpenAI	Strategische Partnerschaft – noch kein Produkt
2020	GPT-3-Exklusivlizenz	Microsoft sichert sich Technologievorsprung
2021	Azure OpenAI Service Preview	Enterprise-Zugang zu GPT – für Entwickler
Nov 2022	ChatGPT Launch (OpenAI)	Massenwirkung KI – Vorstand beginnt zu fragen
Jan 2023	10 Mrd. \$ Folgeinvestition	Kein Zurück mehr – Microsoft ist KI-Unternehmen
Feb 2023	Bing mit GPT-4	Demo-Effekt – aber kein Marktanteilsgewinn
Mar 2023	Microsoft 365 Copilot angekündigt	KI in Ihrem Posteingang – bald
Nov 2023	M365 Copilot GA: 30 \$/Nutzer/Monat	Jetzt ist es eine Beschaffungsentscheidung
2024	Copilot+, Agenten, Wave-Releases	Monatliche Feature-Updates – Tempo steigt

Tabelle 1.1 – Microsoft KI-Meilensteine: Von der ersten Investition bis zum aktuellen Produktportfolio

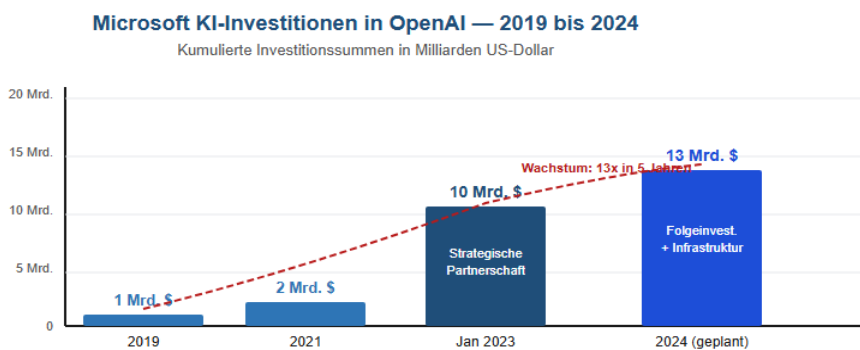


Abb. 1.6 – Microsoft KI-Investitionen in OpenAI 2019–2024 — Keine Kurskorrektur mehr möglich

Abb. 1.6 – Microsoft KI-Investitionen 2019–2024: 13-faches Wachstum in fünf Jahren

## 1.2 Das Portfolio: Was Microsoft mit 'KI' alles meint

Wenn Ihr Vorstand fragt, ob Sie 'Microsoft KI' einsetzen, und Sie mit 'Ja' antworten, haben Sie damit noch nichts Konkretes gesagt. Microsoft betreibt heute mindestens fünf verschiedene Produktlinien unter dem Begriff KI — und jede davon hat andere Zielgruppen, andere Lizenzmodelle und andere Compliance-Anforderungen.

### Microsoft 365 Copilot — der Einstieg für Wissensarbeiter

Microsoft 365 Copilot ist das Produkt, das die meisten Entscheider meinen, wenn sie über 'Copilot' sprechen. Es ist in Word, Excel, PowerPoint, Outlook und Teams integriert und kann auf Ihre Unternehmensdaten zugreifen — über die Microsoft Graph API. Das bedeutet: Copilot sieht alles, auf das Sie Zugriffsrechte haben.

Preis: 30 US-Dollar pro Nutzer und Monat, zusätzlich zu einer bestehenden Microsoft 365 E3- oder E5-Lizenz. Minimum ist seit Januar 2024 aufgehoben — früher waren 300 Lizenzen Pflicht, jetzt kann auch ein Einzelplatz lizenziert werden. Das macht die Entscheidung zwar einfacher, aber nicht unbedingt günstiger.

### Azure OpenAI Service — für Entwickler, nicht für Endanwender

Der Azure OpenAI Service ist das Gegenteil von M365 Copilot: kein fertiges Produkt, sondern eine API. Unternehmen greifen per Programmcode auf GPT-4o, DALL-E, Whisper und andere Modelle zu und integrieren diese in eigene Anwendungen. Das Besondere gegenüber der direkten OpenAI-API: Die Daten verlassen nicht die Azure-Umgebung des Kunden, Microsoft verpflichtet sich in seinen Vertragsklauseln auf strikten Datenschutz, und die Modelle werden nicht mit Kundendaten nachtrainiert.

Für wen ist das relevant? Für IT-Abteilungen, die eigene KI-gestützte Anwendungen entwickeln wollen — etwa einen internen Wissens-Chatbot, ein automatisiertes Dokumenten-Klassifizierungssystem oder eine KI-gestützte Suchfunktion für das Intranet. Azure OpenAI ist kein Einsteigerprodukt: Es erfordert Entwicklungskompetenz und eine klare Architekturentscheidung.

### Copilot Studio — eigene KI-Agenten ohne Programmierkenntnisse

Copilot Studio (früher: Power Virtual Agents) erlaubt es, eigene KI-Agenten zu bauen — ohne tiefe Programmierkenntnisse. Ein Unternehmen kann hier beispielsweise einen HR-Assistenten erstellen, der Mitarbeitern häufige Fragen zu Urlaubsregelungen beantwortet, oder einen internen IT-Helpdesk-Bot, der auf die eigene Wissensdatenbank zugreift.

Copilot Studio-Agenten können in Teams, auf Websites oder in anderen Kanälen veröffentlicht werden. Die Kosten sind komplex: Es gibt ein Tenant-Modell und ein Nachrichten-basiertes Abrechnungsmodell. Wer hier ohne Planung startet, erlebt Überraschungen auf der Rechnung — mehr dazu in Kapitel 9.

### GitHub Copilot — KI für Entwickler

GitHub Copilot ist für Softwareentwickler das, was M365 Copilot für Wissensarbeiter ist: ein KI-Assistent, der direkt in der Entwicklungsumgebung arbeitet. GitHub Copilot ergänzt Code, schlägt Funktionen vor, erklärt fremden Code und hilft bei der Fehlersuche. Studien zeigen Produktivitätssteigerungen von 30 bis 50 Prozent bei bestimmten Aufgabentypen.

Für IT-Leiter, die Softwareentwicklung verantworten, ist GitHub Copilot oft der einfachste Einstieg in generative KI — weil die Zielgruppe klar ist, die Nutzung gut messbar ist und das Datenschutzrisiko überschaubar bleibt (es werden nur Codedateien verarbeitet, keine Business-Daten).

## Copilot for Security – KI für das SOC

Copilot for Security ist ein eigenständiges Produkt für IT-Sicherheitsteams. Es ist in Microsoft Sentinel, Defender und Intune integriert und kann Sicherheitsereignisse analysieren, Angriffsmuster erkennen und Gegenmaßnahmen vorschlagen. Das Produkt ist teuer – es wird per Security Compute Unit abgerechnet – und setzt eine gewisse Reife der Security-Infrastruktur voraus.

Für CISOs, die ohnehin auf Microsoft Security setzen, ist es ein Werkzeug, das die Analyse-Kapazität des Teams erweitern kann, ohne neue Mitarbeiter einstellen zu müssen. Realistisches Einsatzszenario: Ein Sicherheitsanalyst bekommt KI-generierte Zusammenfassungen von Incidents, muss aber die endgültige Entscheidung weiterhin selbst treffen. Mehr dazu in Kapitel 8.

## Azure AI Studio und Azure Machine Learning – die Entwicklerplattform

Jenseits von Azure OpenAI gibt es mit Azure AI Studio eine vollständige Entwicklungsumgebung für KI-Applikationen. Hier können Unternehmen nicht nur auf fertige Modelle zugreifen, sondern eigene Modelle trainieren, Fine-Tuning betreiben, Promptflow-Workflows erstellen und RAG-Architekturen aufbauen. RAG – Retrieval Augmented Generation – ist das Prinzip, das hinter vielen Enterprise-KI-Lösungen steckt: Das Sprachmodell bekommt nicht nur die Anfrage, sondern auch relevante Dokumente aus dem eigenen Wissensspeicher – und kann so präzisere, unternehmensspezifische Antworten liefern.

Azure Machine Learning, das ältere Geschwisterprodukt, richtet sich an Data Scientists und ML-Ingenieure, die eigene Modelle in Produktionsumgebungen betreiben wollen. Es unterstützt MLOps – also die Industrialisierung von Machine-Learning-Prozessen – und ist für Unternehmen relevant, die bereits eigene KI-Modelle entwickeln oder vorhaben, dies zu tun. Für die meisten Entscheider in mittleren und großen Unternehmen ist Azure Machine Learning zunächst nachrangig. Es wird relevant, wenn ein Unternehmen die nächste Stufe erreicht: eigene KI-Applikationen statt vorkonfigurierter Produkte.

## Power Platform KI – Automatisierung für alle

Die Power Platform – Power Automate, Power Apps, Power BI – hat Microsoft schrittweise mit KI-Funktionen ausgestattet. Power Automate kann seit 2023 natürlichsprachliche Prozessbeschreibungen in automatisierte Workflows übersetzen. Power Apps generiert auf Basis von Textbeschreibungen einfache Applikationen. Power BI bietet mit Copilot die Möglichkeit, Datenanalysen in natürlicher Sprache abzufragen und Berichte in Sekunden zu generieren.

Für Unternehmen, die bereits intensiv auf die Power Platform setzen, sind diese KI-Funktionen oft der niedrigschwelligste Einstieg: Die Plattform ist bekannt, die Governance ist aufgebaut, die Nutzer sind geschult. KI-Features werden als Erweiterung wahrgenommen, nicht als neues Produkt. Das ist ein strategischer Vorteil, den viele Unternehmen noch nicht systematisch nutzen. Power BI Copilot zum Beispiel kann erfahrungsgemäß die Zeit für die Erstellung von Standardberichten erheblich reduzieren – sofern die Datenqualität stimmt. Letzteres ist meistens der bremsende Faktor.

## Wo beginnt KI und wo endet Marketing?

Eine ehrliche Einordnung: Nicht alles, was Microsoft als KI vermarktet, ist generative KI oder ein Large Language Model. Einige Features, die unter dem

Copilot-Label laufen, sind hochwertige Automatisierungen oder statistisches Machine Learning — Technologien, die bereits vor dem GPT-Zeitalter existierten. Das macht diese Features nicht wertlos, aber es ist wichtig, die Unterschiede zu verstehen, weil sie unterschiedliche Governance-Anforderungen und Datenschutzfragen aufwerfen.

Generative KI — also Systeme, die neue Inhalte erzeugen können: Texte schreiben, Code generieren, Zusammenfassungen erstellen, Bilder produzieren — ist das, was den wirklichen Paradigmenwechsel darstellt. Klassisches Machine Learning, also Anomalieerkennung, Klassifizierung, Vorhersagemodelle, ist wertvoll und in vielen Microsoft-Produkten schon seit Jahren enthalten. Der wesentliche Unterschied für Datenschutz und Compliance: Generative KI verarbeitet und reproduziert möglicherweise Informationen in einer Weise, die bei klassischem ML nicht auftritt. Eine DSFA kann für generative KI in vielen Fällen Pflicht sein — mehr dazu in Kapitel 6.

Was das für Sie bedeutet: Wenn ein Anbieter oder ein internes Team mit 'KI-Features' argumentiert, fragen Sie konkret: Handelt es sich um generative KI auf Basis eines Large Language Models? Oder um traditionelle Automatisierung mit neuem Label? Die Antwort ändert nichts an der Nützlichkeit — aber sie ändert die Governance-Anforderungen erheblich.

## **i TECHNISCHER HINTERGRUND — Microsoft Copilot vs. Azure OpenAI vs. Copilot Studio: Der Unterschied auf einen Blick**

### **Microsoft 365 Copilot**

- Zielgruppe: Endanwender in Word, Excel, PowerPoint, Outlook, Teams
- Datenzugriff: Über Microsoft Graph — alle Daten, auf die der Nutzer Rechte hat
- Lizenz: 30 \$/Nutzer/Monat + M365 E3/E5
- Compliance: Im Microsoft-365-Tenant, EU Data Boundary verfügbar

### **Azure OpenAI Service**

- Zielgruppe: Entwickler, die eigene KI-Applikationen bauen
- Datenzugriff: Nur was die Anwendung explizit übergibt — kein automatischer Zugriff
- Lizenz: Token-basiert, variabel nach Nutzung
- Compliance: In der Azure-Region des Kunden, kein Training auf Kundendaten

### **Copilot Studio**

- Zielgruppe: IT-Power-User, die Chatbots und Agenten ohne Code bauen
- Datenzugriff: Über konfigurierte Connectors und Wissensdatenbanken
- Lizenz: Tenant-Lizenz (~200 \$/Monat) + Message-Kosten
- Compliance: Power Platform Umgebung — konfigurationsabhängig

Die häufigste Verwechslung: Viele meinen 'Azure OpenAI', wenn sie sagen 'Copilot' — und umgekehrt. Klären Sie in jedem Meeting zuerst, über welches Produkt Sie sprechen.

### Microsoft KI-Produkte im Vergleich — M365 Copilot vs. Azure OpenAI vs. Copilot Studio

Kriterium	M365 Copilot	Azure OpenAI	Copilot Studio
<b>Zielgruppe</b> Wer nutzt es?	Endanwender in M365 (Wissensarbeiter)	Entwickler / DevOps (API-Zugang)	Power-User / IT (No-Code-Agenten)
<b>Kosten / Monat</b> pro Nutzer (ca.)	<b>30 \$ / Nutzer</b> + M365 E3/E5 Voraussetzung	<b>nach Verbrauch</b> Token-basiert, variabel	<b>200 \$/Monat</b> + Message-Kosten
<b>Datenschutz</b> DSGVO / EU-Grenze	●●● EU Data Boundary verfügbar	●●● Eigene Region wählbar	●●○ Abhängig von Konfiguration
<b>Anpassbarkeit</b> Eigene Inhalte / Logik	●●○ Begrenzt (Plugins, Connectors)	●●● Vollständige Kontrolle	●●● Visual Builder + Connectors
<b>Implementierung</b> Aufwand bis Go-Live	●●● Gering (Lizenz + Freigabe)	●○○ Hoch (Entwicklung nötig)	●●○ Mittel (No-Code-Konfiguration)
<b>M365-Voraussetzung</b> Welche Lizenzen nötig?	●○○ M365 E3/E5 zwingend	●●● Keine M365-Abhängigkeit	●●○ Power Platform Lizenz
<b>Empfehlung für</b> Idealer Einsatzfall	<b>Produktivitätssteigerung</b> für Wissensarbeiter	<b>Eigene KI-Applikation</b> mit vollst. Kontrolle	<b>Interne Chatbots &amp;</b> Prozess-Agenten

Abb. 1.3 — M365 Copilot vs. Azure OpenAI vs. Copilot Studio — ●●● gut / ●●○ mittel / ●○○ schwach

Abb. 1.3 — Microsoft KI-Produktvergleich: M365 Copilot, Azure OpenAI, Copilot Studio im direkten Vergleich

### Tabelle 1.2 — Copilot-Varianten im Überblick

Produkt	Zweck	Zielgruppe	Lizenzmodell
M365 Copilot	KI in Office-Apps + Teams	Wissensarbeiter	30 \$/Nutzer/Monat
Azure OpenAI	KI-API für eigene Apps	Entwickler	Token-basiert
Copilot Studio	Eigene Agenten bauen	IT/Power-User	~200 \$/Monat + Messages
GitHub Copilot	Code-Assistent	Softwareentwickler	19–39 \$/Nutzer/Monat
Copilot for Security	Sicherheitsanalyse	SOC/CISO-Teams	Per Security Compute Unit
Copilot+	KI in Windows-Geräten	Endanwender (Hardware)	Im Gerät enthalten

Produkt	Zweck	Zielgruppe	Lizenzmodell
Copilot (Bing/Web)	Öffentlicher KI-Assistent	Alle Internetnutzer	Kostenlos / Pro-Version

Tabelle 1.2 – Die Copilot-Familie: Sieben Produkte unter einem Namen – mit sehr unterschiedlichen Anforderungen

**Tabelle 1.3 – Wettbewerbsvergleich: Microsoft vs. Google vs. Salesforce vs. SAP**

Kriterium	Microsoft Copilot	Google Workspace AI	Salesforce Einstein	SAP Business AI
KI-Modell	GPT-4o (OpenAI)	Gemini (eigene Entwicklung)	GPT-4 + eigene LLMs	Eigene + Partner-Modelle
Integration	Tief in M365 + Azure	Tief in Google Workspace	Tief in Salesforce CRM	Tief in SAP ERP/S4HANA
Datenschutz EU	EU Data Boundary	EU-Rechenzentren verfügbar	Abhängig von Konfiguration	Clean Core-Prinzip
Preis/Nutzer	~30 \$/Monat	~30 \$/Monat (Duet AI)	Variable, CRM-abhängig	Im SAP-Vertrag enthalten
Marktposition	<b>Marktführer Enterprise</b>	Stark bei Google-Kunden	Stark bei CRM-Prozessen	Stark bei ERP-Kunden
Empfehlung für	M365-Kunden	Google Workspace-Kunden	Salesforce-Kunden	SAP-Kunden

Tabelle 1.3 – Wettbewerbsvergleich KI-Suites: Microsoft, Google, Salesforce und SAP im direkten Gegenüber

## Klassischer Chatbot vs. Microsoft Copilot — Der entscheidende Unterschied

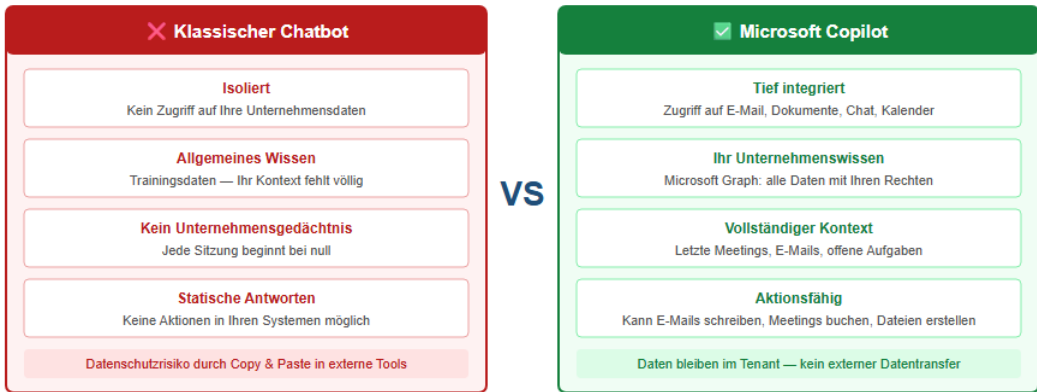


Abb. 1.5 — Chatbot vs. Copilot: Warum Copilot kein Chatbot ist — und warum das Ihre Vorbereitung ändert

Abb. 1.5 — Chatbot vs. Microsoft Copilot: Warum Copilot kein Chatbot ist — und was das für Ihre Vorbereitung bedeutet

## KI-Anbieter im Enterprise-Vergleich — Marktpositionierung 2024

Bewertung nach Enterprise-Integration und KI-Fähigkeit

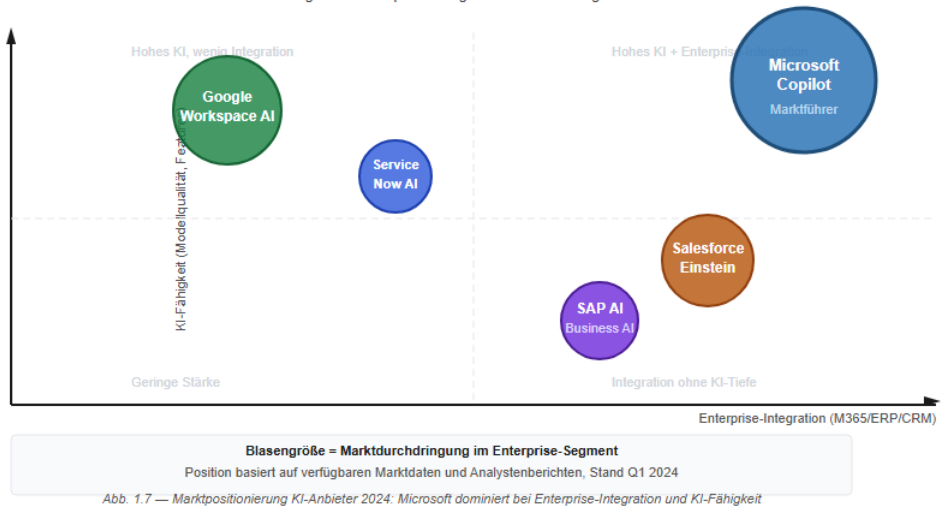


Abb. 1.7 — Marktpositionierung KI-Anbieter 2024: Microsoft dominiert bei Enterprise-Integration und KI-Fähigkeit

Abb. 1.7 — Marktpositionierung KI-Anbieter 2024: Enterprise-Integration vs. KI-Fähigkeit

## 💡 TIPP — Wie Sie den Überblick im Microsoft-KI-Portfolio behalten

Drei Fragen klären neunzig Prozent der Verwirrung:

- Wer nutzt es? Endanwender → M365 Copilot. Entwickler → Azure OpenAI. IT ohne Code → Copilot Studio.
- Auf welche Daten greift es zu? Alles was der Nutzer sieht → M365 Copilot. Nur was Sie übergeben → Azure OpenAI.
- Wer bezahlt und wie viel? M365 Copilot: 30 \$ pro Person, fix. Azure OpenAI: variabel, nach Verbrauch. Copilot Studio: Grundgebühr + Nutzung.

Wenn jemand in einem Meeting sagt 'wir wollen Copilot einsetzen', stellen Sie diese drei Fragen. Sie sparen sich damit mindestens zwei Folgemeetings.

Für einen Schnellüberblick: Tabelle 1.2 in diesem Kapitel gibt Ihnen alle wesentlichen Unterschiede auf einer Seite.

### 1.3 Warum 'wir schauen erst mal' keine Strategie ist

'Wir beobachten das.' Diese vier Wörter haben in den letzten zwei Jahren in mehr Führungsrunden gestanden als jede andere KI-bezogene Aussage. Sie klingen klug. Sie klingen bedacht. Sie klingen, als hätte jemand eine fundierte Entscheidung getroffen. Meistens ist das Gegenteil der Fall.

'Wir beobachten das' ist keine neutrale Position. Es ist eine aktive Entscheidung — mit konkreten Konsequenzen. Während ein Unternehmen beobachtet, läuft die Zeit. Und in dieser Zeit passieren Dinge, die sich später nur noch schwer korrigieren lassen.

#### Shadow AI: Die Entscheidung haben Ihre Mitarbeiter schon getroffen

Laut verschiedenen Markterhebungen aus 2023 und 2024 nutzen zwischen 35 und 45 Prozent aller Büroangestellten in Deutschland KI-Tools im Arbeitsalltag — davon ein erheblicher Teil ohne Wissen oder Genehmigung des Arbeitgebers. Sie geben Texte in ChatGPT ein. Sie nutzen kostenlose KI-Tools für Übersetzungen. Sie lassen Kundendaten von Gratis-KI-Diensten zusammenfassen.

Das ist nicht Aufmüpfigkeit — das ist Effizienz. Mitarbeiter lösen Probleme mit den Mitteln, die verfügbar sind. Wenn das Unternehmen keine offizielle KI-Lösung bereitstellt, bauen Mitarbeiter sich selbst eine — mit Tools, über die die IT-Abteilung keine Kontrolle hat, die möglicherweise keine Datenschutzgarantien bieten, und die in keiner Datenschutz-Folgenabschätzung auftauchen.

Das offizielle Bild — Copilot-Adoptionsrate von circa drei Prozent — trägt vollständig. Der reale Anteil der Mitarbeiter, die täglich KI nutzen, liegt um ein Vielfaches höher. Der Unterschied: Die drei Prozent tun es mit einem lizenzierten, kontrollierten, DSGVO-konformen Tool. Die anderen tun es mit Tools, die niemand überprüft hat.

**⚠ RISIKO — Shadow AI: Wenn Mitarbeiter der IT-Abteilung vorseilen**

## Konkrete Risiken unkontrollierter KI-Nutzung:

- Datenpanne durch externe KI-Tools: Mitarbeiter geben Kundendaten, Vertragsdetails oder persönliche Mitarbeiterdaten in ChatGPT & Co. ein. Diese Daten können für Modelltraining genutzt werden.
- DSGVO-Verstoß ohne Auftragsverarbeitungsvertrag: Wer Personendaten in externe KI-Tools überträgt, ohne AVV, begeht möglicherweise einen meldepflichtigen Datenschutzvorfall.
- Unkontrollierte Wissensweitergabe: Betriebsgeheimnisse, Strategiepapiere, Gehaltsstrukturen — alles was Mitarbeiter in externe Tools einfügen, verlässt den Unternehmenskontext.
- Compliance-Risiko bei regulated industries: In Finanz-, Gesundheits- und Behördenumgebungen ist unkontrollierte KI-Nutzung möglicherweise regulatorisch relevant.

Was hilft: Nicht verbieten — das funktioniert nicht. Stattdessen: Eine offizielle, sichere Alternative bereitstellen und kommunizieren, dass diese genutzt werden soll. Mehr dazu in Kapitel 4 (Governance) und Kapitel 5 (Betriebsrat).

Zahlen zum Einordnen: In einer Studie von 2023 gaben 48% der befragten Mitarbeiter an, vertrauliche Arbeitsinformationen in KI-Tools eingegeben zu haben. 68% dieser Mitarbeiter wussten nicht, dass ihre Eingaben für Modelltraining genutzt werden könnten.

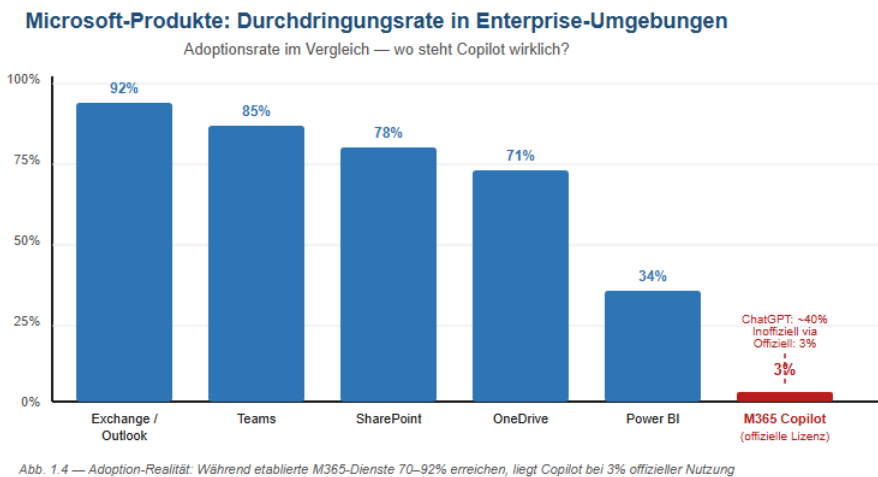


Abb. 1.4 — Adoption-Realität: Offizielle Copilot-Rate bei 3% — inoffizielle KI-Nutzung deutlich höher

## Was in der Zwischenzeit bei der Konkurrenz passiert

Der Abwartende hat eine implizite Annahme: Dass die Welt stehenbleibt, während er beobachtet. Diese Annahme ist falsch.

Wettbewerber, die jetzt KI in ihre Prozesse integrieren, sammeln Erfahrungen, die sich nicht kaufen lassen. Sie wissen, welche Anwendungsfälle funktionieren und welche nicht. Sie haben gelernt, wie man Mitarbeiter von KI-Tools überzeugt. Sie haben Governance-Strukturen aufgebaut, die funktionieren. In zwölf oder achtzehn Monaten haben diese Unternehmen einen Vorsprung, der sich in realen Produktivitätsunterschieden und möglicherweise in Personalentscheidungen niederschlägt — denn qualifizierte Mitarbeiter wählen zunehmend Arbeitgeber, die technologisch auf Augenhöhe sind.

Das ist keine Panikmache. Es ist eine nüchterne Einschätzung: In einer Welt, in der ein Tool für 30 Dollar pro Monat die Arbeitsproduktivität einzelner Wissensarbeiter um 20 bis 30 Prozent erhöht — auch wenn die Zahlen je nach Untersuchung schwanken —, ist das Abwarten kein risikoloses Verhalten. Es ist eine Entscheidung, deren Kosten man nur nicht sofort auf der Rechnung sieht.

### Die Halbwertszeit des Beobachtens

Ende 2022 war Abwarten eine vernünftige Haltung — die Technologie war neu, die Produkte waren unreif, die Rechtslage war unklar. Ende 2023 war Abwarten noch zu verteidigen — man konnte auf fehlende EU-Data-Boundary-Optionen oder unreifes Lizenzmodell verweisen. Ende 2024 ist Abwarten eine Entscheidung, die man vor dem Vorstand, dem Betriebsrat und den eigenen Mitarbeitern begründen muss.

Die Argumente, die 2022 für Abwarten sprachen, sind größtenteils weggefallen. M365 Copilot ist reif. Die EU Data Boundary ist verfügbar. Der AI Act ist in Kraft. DSGVO-Leitlinien für KI werden konkreter. Lizenzmodelle sind gestaffelt und zugänglich. Was bleibt, ist Unsicherheit — aber Unsicherheit ist kein Argument für Stillstand.

### Die echten Kosten des Abwartens

Abwarten hat einen Preis. Dieser Preis erscheint auf keiner Rechnung — deshalb wird er systematisch unterschätzt. Er setzt sich aus drei Komponenten zusammen, die selten gemeinsam betrachtet werden.

Die erste Komponente ist der Produktivitätsnachteil. Wenn ein Wissensarbeiter durch KI-Unterstützung täglich eine Stunde Routinearbeit einspart — Zusammenfassungen erstellen, E-Mails formulieren, Recherchen beschleunigen —, entspricht das bei 200 Arbeitstagen 25 Arbeitstagen pro Jahr und Mitarbeiter. Ob diese Zahl realistisch ist, hängt stark vom Aufgabenprofil ab. Selbst bei einem Drittel dieser Annahme sind die Zahlen bei 100 Mitarbeitern bedeutsam: über 800 Arbeitstage jährlich.

Die zweite Komponente ist das Qualifikationsgefälle. Mitarbeiter, die KI-Tools routiniert einsetzen, entwickeln Fähigkeiten, die sich nicht in einer Schulungsstunde nachholen lassen. Prompt-Engineering, kritisches Bewerten von KI-Outputs, effiziente Nutzung von Copilot-Features in Excel oder Word — das ist Erfahrungswissen, das sich in Monaten aufbaut. Ein Unternehmen, das ein Jahr wartet, hat einen Qualifikationsrückstand, der nicht durch eine einmalige Schulungsmaßnahme geschlossen wird.

Die dritte Komponente ist die Arbeitgeberattraktivität. Qualifizierte Fachkräfte, die mit KI-Tools vertraut sind, wählen Arbeitgeber, die diese Tools bereitstellen und fördern — nicht Unternehmen, die noch evaluieren, ob das ein Hype ist. In Recruiting-Gesprächen wird die Frage nach verfügbaren Tools zunehmend gestellt.

Copilot ist dabei nicht der einzige relevante Faktor, aber er ist ein sichtbares Signal für die technologische Reife eines Unternehmens.

### Was 'wir beobachten das' wirklich bedeutet

In der Praxis bedeutet 'wir beobachten das' meistens eines von drei Dingen: Erstens – und am häufigsten – bedeutet es, dass die Entscheidung auf die lange Bank geschoben wird, weil sie komplex ist und konkurrierende Prioritäten hat. Das ist menschlich verständlich, ändert aber nichts daran, dass die Konsequenzen trotzdem eintreten.

Zweitens bedeutet es manchmal, dass die Entscheidungsebene das Thema für weniger dringend hält als die operative IT-Ebene. In diesem Fall ist das Problem kein Abwarten – es ist ein Kommunikationsproblem. Die IT-Abteilung hat nicht überzeugend genug erklärt, warum das Thema jetzt relevant ist. Dieses Buch ist unter anderem dafür gedacht, diese Überzeugungsarbeit zu erleichtern – mit Zahlen, Fallbeispielen und konkreten Szenarien.

Drittens – und das ist die beste Version des 'Beobachtens' – bedeutet es, dass ein Unternehmen systematisch evaluiert: Was ist der richtige Zeitpunkt? Welche Voraussetzungen müssen erfüllt sein? Wer trägt die Verantwortung? Diese Form des Abwartens ist keine Untätigkeit – sie ist Vorbereitung. Der Unterschied zur ersten und zweiten Variante: Es gibt ein konkretes Datum, zu dem die Entscheidung getroffen wird, und konkrete Kriterien, nach denen entschieden wird. Wenn Sie sich in dieser dritten Variante wiedererkennen: Dieses Buch ist für Sie, um diese Evaluationsphase abzukürzen.

**Tabelle 1.4 – KI-Strategie-Reifegrad: Fünf Stufen mit konkreten Risiken und Empfehlungen**

Stufe	Typische Aussage	Konkretes Risiko	Empfehlung
1 – Ignorieren	'Das ist ein Hype'	Shadow AI unkontrolliert aktiv, Datenschutzvorfälle möglich	Sofort: Bestandsaufnahme Shadow AI
2 – Beobachten	'Wir schauen erst mal'	Wettbewerber sammeln Erfahrungen, Mitarbeiter nutzen externe Tools	Kap. 2: Standortbestimmung durchführen
3 – Testen	'Wir haben einen Pilot'	Pilot ohne Ziel endet ergebnislos, kein Governance-Rahmen	Kap. 4: Governance-Framework aufbauen
4 – Pilotieren	'Wir skalieren nach dem Piloten'	Piloten in Silos, kein zentrales Reporting, Kosten unbekannt	Kap. 9: Kostenstruktur analysieren
5 – Skalieren	'KI ist Teil unserer DNA'	Tempo vs. Compliance-Druck, AI Act ab 2026	Kap. 6+7: DSGVO und AI Act prüfen

Tabelle 1.4 – KI-Strategie-Reifegrad: Wo stehen Sie – und was sind die Risiken jeder Stufe?

## KI-Strategie-Reifegrad — Wo stehen Sie und was kostet das Abwarten?

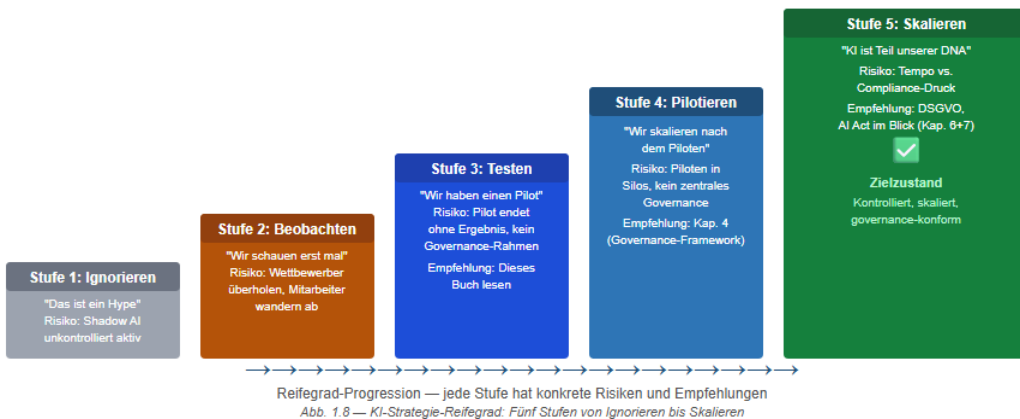


Abb. 1.8 — KI-Strategie-Reifegrad: Fünf Stufen von Ignorieren bis Skalieren — jede Stufe hat ihren Preis

## FALLSTUDIE — Musterwerk GmbH: 18 Monate 'erstmal schauen' — eine Bilanz

Thomas Berger ist IT-Leiter bei der Musterwerk GmbH, einem Maschinenbauer mit 800 Mitarbeitern in Dortmund. Er kennt seine Infrastruktur gut. Er hat SharePoint 2016 auf Microsoft 365 migriert, Exchange läuft stabil, Teams ist im Einsatz seit 2020. Seine Umgebung ist solide — und in vielen Bereichen gewachsen und undokumentiert.

Ende 2022 fragte die Geschäftsführung nach KI. Thomas Berger antwortete ehrlich: 'Wir beobachten das und evaluieren Optionen.' Das war korrekt. Das war vernünftig.

Zwölf Monate später: Die Geschäftsführung fragte erneut. Thomas Berger hatte noch immer keine Antwort — weil er in der Zwischenzeit anderes zu tun hatte. Betrieb. Migration. Teams-Rollout. Die typische IT-Leiter-Realität: Das Dringende verdrängt das Wichtige.

Was in dieser Zeit passiert war, ohne dass Thomas Berger es bemerkte:

- 14 Mitarbeiter hatten ChatGPT-Konten eingerichtet und nutzten sie regelmäßig für Arbeitsaufgaben.
- Drei Abteilungsleiter hatten eigene 'KI-Initiativen' gestartet — unkoordiniert, ohne IT-Wissen.
- Ein Angebot an einen Kunden war von einem Vertriebsmitarbeiter in ChatGPT eingegeben worden, um 'eine bessere Formulierung' zu bekommen.
- Die Personalabteilung hatte Stellenbeschreibungen mit einem kostenlosen KI-Tool optimiert — inklusive Gehaltsangaben.

Als Thomas Berger das Ausmaß erkannte, war sein erster Impuls ein Verbot. Sein zweiter Impuls — nach einem langen Gespräch mit dem Datenschutzbeauftragten — war eine Bestandsaufnahme, gefolgt von einer klaren Richtlinie und einer offiziellen Alternative.

Das Ergebnis: Musterwerk ist heute an Reifegrad-Stufe 3. Der Pilot läuft. Thomas Berger schläft besser. Der Verbotsimpuls wäre die schlechteste aller Optionen gewesen.

Was Sie daraus mitnehmen sollten: Das Problem ist nicht, dass Mitarbeiter KI nutzen. Das Problem ist, wenn sie es unkontrolliert tun.

## 1.4 Wie dieses Buch aufgebaut ist

Dieses Buch folgt einer Logik, die sich an der Entscheidungsreihenfolge orientiert, die in der Praxis sinnvoll ist. Sie müssen nicht von vorne nach hinten lesen — aber es schadet nicht.

### Die Kapitelstruktur im Überblick

Kapitel 1 (dieses) gibt den Überblick: Was ist Microsoft KI, wo steht der Markt, warum ist Abwarten eine Entscheidung.

Kapitel 2 hilft Ihnen bei der ehrlichen Standortbestimmung: Wo stehen Sie wirklich? Nicht wo Sie glauben zu stehen — sondern was wirklich in Ihrer Umgebung aktiv ist, wer was nutzt und welche Lücken Sie haben.

Kapitel 3 erklärt technisch präzise, wie Copilot auf Ihre Daten zugreift — über die Microsoft Graph API, über Berechtigungsstrukturen, und warum das mehr bedeutet als 'die KI liest Ihre E-Mails'. Das ist Pflichtlektüre für IT-Leiter und DSBs.

Kapitel 4 ist das zentrale Arbeitskapitel: Wie Sie ein Governance-Framework aufbauen, das nicht im ersten Quartal in der Schublade verschwindet. Mit konkreten Vorlagen, Rollendefinitionen und Entscheidungswegen.

Kapitel 5 behandelt das Thema, das oft vergessen wird, bis es zu spät ist: Betriebsrat und Belegschaft. Mitbestimmungsrechte, Betriebsvereinbarungen, Change-Management.

Kapitel 6 und 7 sind für DSBs und Compliance-Verantwortliche: Was die DSGVO von Ihnen verlangt, bevor Copilot live geht — und was der EU AI Act konkret bedeutet.

Kapitel 8 richtet sich an CISOs: Angriffsvektoren, Prompt Injection, KI als Waffe — und wie Copilot for Security helfen kann.

Kapitel 9 rechnet nach: Was Sie wirklich zahlen — inklusive aller Positionen, die in keinem Microsoft-Angebot stehen.

Kapitel 10 und 11 schließen den Kreis: Wie Sie die richtige Entscheidung treffen und worauf Sie sich vorbereiten sollten — auch wenn Sie heute noch keinen Copilot haben.

### **Tabelle 1.5 — Welche Kapitel für welche Rolle besonders relevant sind**

Ihre Rolle	Priorität-Kapitel	Warum?
CISO	Kap. 3, 8, 6, 7	Zugriff, Angriffsvektoren, DSGVO, AI Act — die vier Kernthemen der IT-Sicherheit
DSB / DPO	Kap. 3, 6, 7, 4	Datenzugriff verstehen, DSGVO-Pflichten, AI Act-Klassifizierung, Governance
IT-Leiter	Alle Kapitel	Technische, rechtliche und strategische Dimension — alles relevant
CIO	Kap. 1, 2, 4, 9, 10	Überblick, Standort, Governance, Kosten, Entscheidung
CFO	Kap. 9, 2, 10	Was kostet es wirklich? Wo stehen wir? Wie entscheiden wir strukturiert?
HR-Leiter	Kap. 5, 4, 7	Betriebsrat, Governance-Rollen, AI Act-Nutzerpflichten
Vorstand	Kap. 1, 2, 10, 11	Überblick, Status quo, Entscheidungsrahmen, Ausblick

Tabelle 1.5 — Leseanleitung nach Rolle: Wer welche Kapitel priorisieren sollte

## 1.5 Leseanleitung: Wie Sie dieses Buch am effektivsten nutzen

Dieses Buch ist für Menschen geschrieben, die viel zu tun haben. Es enthält keine Sätze, die um des Seitenfüllers willen stehen. Aber es enthält Struktur — und wenn Sie die Struktur verstehen, halbiert sich die Lesezeit.

### Management Summary Kästen — Das Wichtigste in fünf Minuten

Jedes Kapitel beginnt mit einem Management Summary. Wenn Sie nur drei Minuten haben: Lesen Sie den. Er enthält die Kernaussagen des Kapitels in verdichteter Form — nicht als Werbetexter-Zusammenfassung, sondern als Entscheider-Briefing.

Das Ziel der Management Summary Kästen ist nicht, das Lesen zu ersetzen — es ist, das Lesen vorzubereiten. Wer zuerst die Zusammenfassung liest, versteht den Haupttext besser und schneller.

### Fallstudien — Was Sie lernen können, und was nicht

Die drei Fallstudien-Unternehmen — Musterwerk GmbH, Sparfuchs & Partner und Trendforge Digital GmbH — sind fiktiv. Die Probleme, die sie haben, sind es nicht. Sie basieren auf typischen Mustern, die in realen Unternehmen beobachtbar sind.

Was Sie aus den Fallstudien lernen sollten: das Muster, nicht die Details. Musterwerk ist kein Maschinenbauer-Problem — es ist ein 'gewachsene-Strukturen-Problem'. Sparfuchs ist kein Steuerberater-Problem — es ist ein 'Compliance-trifft-Budgetknappheit-Problem'. Trendforge ist kein Softwarehaus-Problem — es ist ein 'zu-viel-Kompetenz-ohne-Entscheidungskultur-Problem'.

Das letzte davon ist übrigens häufiger als die meisten Führungskräfte zugeben würden.

### Tabellen — Entscheidungshilfen, keine Dekoration

Die Tabellen in diesem Buch sind nicht Schmuck. Sie sind Entscheidungswerkzeuge. Vergleichstabellen, Risikobewertungen, Checklisten – alles verdichtet auf das Wesentliche. Wenn Sie ein Kapitel gelesen haben und die Tabellen übersehen haben, lesen Sie das Kapitel noch einmal.

Spezifisch: Die Tabellen in Kapitel 9 (Kosten) und Kapitel 10 (Entscheidungsrahmen) sind für die meisten Leser das Wertvollste im gesamten Buch. Nicht weil der Fließtext irrelevant ist – sondern weil diese Tabellen direkt in Entscheidungen einfließen können.

### Risiko- und Tipp-Kästen – Kontext zu den Hauptaussagen

Die farbigen Kästen am Rand der Hauptaussagen geben Ihnen Kontext, den der Fließtext nicht immer liefern kann. Risiko-Kästen zeigen konkrete Konsequenzen von Fehlentscheidungen – mit realen Zahlen und Szenarien, soweit verfügbar. Tipp-Kästen sind Handlungsempfehlungen, die direkt angewendet werden können.

Die WAS JETZT ZU TUN IST-Kästen am Ende jedes Kapitels sind direkt umsetzbar. Keine vagen Empfehlungen wie 'Sie sollten KI-Governance prüfen'. Konkrete nächste Schritte, mit Zeitrahmen und Verantwortlichkeiten.

### Was dieses Buch nicht ist

Dieses Buch ist kein Handbuch für Techniker. Es erklärt technische Konzepte so weit, wie ein Entscheider sie verstehen muss – aber es gibt keine Schritt-für-Schritt-Anleitungen für die Konfiguration von Azure OpenAI oder die Einrichtung von Sensitivity Labels. Dafür gibt es Microsoft-Dokumentationen, technische Berater und Ulrich Boddenbergs Beratungsangebot (Anhang K).

Dieses Buch ist auch kein Juristentext. Es enthält rechtliche Einordnungen und konkrete Handlungsempfehlungen zu DSGVO und AI Act – aber keine Rechtsberatung. Für Ihr konkretes Unternehmen in Ihrer konkreten Situation brauchen Sie weiterhin einen Datenschutzbeauftragten und für komplexe Fragen einen Anwalt. Was dieses Buch Ihnen gibt, ist die Grundlage, um mit diesen Experten fundiert zu sprechen.

Was dieses Buch ist: Die ehrliche Einschätzung einer Situation, die für viele Unternehmen komplex und dringlich zugleich ist – von jemandem, der weder etwas verkaufen noch einen Lehrstuhl verteidigen muss.

## WAS JETZT ZU TUN IST – Fünf Maßnahmen nach Lektüre dieses Kapitels

- **Bestandsaufnahme Shadow AI durchführen: Welche KI-Tools nutzen Ihre Mitarbeiter bereits? Eine einfache anonyme Befragung gibt innerhalb einer Woche ein realistisches Bild. Kein Verbot – nur Inventur.**
- **Ihren Reifegrad bestimmen: Sind Sie auf Stufe 1 (Ignorieren), 2 (Beobachten), 3 (Testen)? Nutzen Sie Tabelle 1.4 als Selbstcheck. Ehrlichkeit zahlt sich hier aus.**

- **Klären, welches Copilot-Produkt überhaupt relevant ist: M365 Copilot für Wissensarbeiter, GitHub Copilot für Entwickler, Azure OpenAI für eigene Entwicklung? Tabelle 1.2 hilft bei der Einordnung.**
- **Den richtigen Kapitelpfad identifizieren: Nutzen Sie Tabelle 1.5 — welche Kapitel sind für Ihre Rolle und Situation am relevantesten?**
- **Einen KI-Jour-fixe einrichten: Monatlich, 30 Minuten, mit IT-Leiter, DSB und einem Fachbereichsvertreter. Nicht um Entscheidungen zu treffen — um informiert zu bleiben und Shadow-AI-Entwicklungen früh zu erkennen.**

Zeitaufwand für alle fünf Punkte: eine bis zwei Stunden. Das ist weniger als das Meeting, in dem Ihr Vorstand zuletzt über KI-Strategie gesprochen hat — mit weniger Ergebnis.