



Zwischen Bürokratie, Digitalisierung und Cyberrisiko

Die Lage der kleinen und mittleren Unternehmen (KMU) 2000-2025

Eine umfassende Fachveröffentlichung zur Analyse der
Herausforderungen und Chancen für mittelständische Unternehmen im
digitalen Zeitalter

Inhaltsverzeichnis

Einleitung und Zielsetzung des Berichts.....	4
Struktur und Bedeutung der KMU in Deutschland (2000–heute).....	5
2.1 Unternehmensdynamik und Strukturwandel	5
2.2 Hauptgründe für Unternehmensaufgaben	5
2.3 Finanzielle Entwicklung und Investitionsverhalten	5
2.4 Regionale und saisonale Unterschiede	6
2.5 Internationaler Vergleich (DACH, EU, USA, MENA, Asien)	6
2.6 Fazit	6
Quellen (Kapitel 2)	7
Finanzielle Entwicklung und Investitionen (KMU vs. Gesamtindustrie)	8
3.1 Entwicklung der Erträge und Kapitalausstattung.....	8
3.2 Investitionsverhalten und Trends.....	8
3.3 Investitionsschwerpunkte	8
3.4 Finanzierung und Liquidität.....	9
3.5 Digitalisierung und IT-Sicherheitsinvestitionen	9
3.6 Fazit	10
Quellen (Kapitel 3)	10
Investitionsschwerpunkte und Ressourcennutzung in KMU.....	11
4.1 Allgemeine Entwicklung der Investitionsstruktur.....	11
4.2 Personal und Fachkräfteentwicklung	11
4.3 Weiterbildung und Wissenstransfer	12
4.4 Geschäftsräume, Energieeffizienz und Nachhaltigkeit.....	12
4.5 IT-Infrastruktur und IT-Sicherheit.....	12
4.6 Förderprogramme und Finanzierungshilfen	13
4.7 Zusammenfassung	13
Quellen (Kapitel 4)	13
Neugründungen und Unternehmensaufgaben im Wandel	14
5.1 Gesamtentwicklung seit 2000	14
5.2 Strukturelle Ursachen und Branchentrends	14
5.3 Einflussfaktoren auf die Gründungsneigung.....	15
5.4 Unternehmensaufgaben: Ursachen und Muster.....	15
5.6 Verhältnis von Gründungen zu Unternehmensaufgaben	16
5.7 Fazit	16
Quellen (Kapitel 5)	16
Internationale Vergleiche (DACH, EU, USA, MENA, Asien)	17
6.1 Überblick und Vergleichsrahmen	17
6.2 Deutschland, Österreich und Schweiz (DACH-Raum).....	17
6.3 Europäische Union	18

6.4 Vereinigte Staaten von Amerika (USA)	18
6.5 Asien und MENA-Region	19
6.6 Vergleichende Bewertung.....	19
6.7 Fazit	20
Quellen (Kapitel 6)	20
Einfluss regulatorischer Entwicklungen auf KMU (2015–2025)	21
7.1 Einleitung	21
7.2 Überblick über zentrale Regelwerke	21
7.3 Datenschutz und Informationssicherheit (DSGVO, NIS2, DORA	22
7.4 Nachhaltigkeit, Lieferketten und Berichterstattung (CSRD, LkSG)	23
CSRD	23
7.5 Gesamtauswirkungen auf Kosten, Prozesse und Wettbewerbsfähigkeit	23
7.6 Chancen durch Regulierung.....	24
7.7 Fazit	24
Quellen (Kapitel 7)	24
IT-Service-Management und ITIL im Mittelstand.....	25
8.1 Einleitung	25
8.2 Grundlagen des IT-Service-Managements.....	25
8.3 Bedeutung von ITIL im Mittelstand.....	26
8.4 Integration in regulatorische und sicherheitsrelevante Anforderungen	26
8.5 Herausforderungen und Erfolgsfaktoren in KMU.....	27
8.6 ITSM-Tools und Automatisierung	27
8.8 Fazit	28
Quellen (Kapitel 8)	28
Cyberkriminalität, Risiken und Schutzstrategien	29
9.1 Einleitung: Der digitale Risiko-Faktor	29
9.2 Entwicklung der Bedrohungslage (2015–2025)	29
9.3 Typische Angriffsszenarien bei KMU	29
9.4 Auswirkungen auf den Mittelstand	30
9.5 Angriffsziele und Motive	30
9.6 Prävention und Schutzmaßnahmen	31
1. Informationssicherheitsmanagement (ISMS).....	31
2. Awareness und Schulung.....	31
3. Multi-Faktor-Authentifizierung (MFA).....	31
4. Patch-Management & Schwachstellenanalyse.....	31
5. Backup-Strategien	31
6. Zero-Trust-Architektur	31
7. Notfall- und Incident-Response-Plan	31

9.7 Rolle von IT-Sicherheitsstandards und Audits	31
9.8 Staatliche und institutionelle Unterstützung.....	32
9.9 Zukünftige Bedrohungen und Trends	32
9.10 Fazit.....	33
Quellen (Kapitel 9)	33
Zusammenfassung, Ausblick und Handlungsempfehlungen	34
10.1 Zusammenfassung der Gesamtlage (2000–2025)	34
1. Strukturelle Stärke, aber sinkende Dynamik:.....	34
2. Zinswende und Kostenexplosion:	34
3. Digitalisierung und IT-Sicherheit als Schlüsselfaktoren:	34
4. Regulatorische Verdichtung:	34
5. Regionale und internationale Unterschiede:	34
6. Transformation der Investitionsschwerpunkte:	34
10.2 Bewertung der Herausforderungen	35
10.3 Chancen und Potenziale	35
1. Digitalisierung als Effizienztreiber:.....	35
2. IT-Sicherheit als Qualitätsmerkmal:.....	35
3. Nachhaltigkeit als Innovationsfeld:	35
4. Regionale Cluster und Kooperationen:.....	35
5. Politische Aufmerksamkeit:	35
10.4 Handlungsempfehlungen für KMU.....	36
1. IT- und Cybersicherheit zur Führungsaufgabe machen	36
2. Prozesse standardisieren und digitalisieren	36
3. Investitionen strategisch planen	36
4. Förderprogramme aktiv nutzen	36
5. Kooperationen ausbauen	36
6. Nachfolge und Wissenssicherung planen	36
7. Unternehmenskultur modernisieren	36
10.5 Handlungsempfehlungen für Politik und Wirtschaft.....	36
10.6 Ausblick: Der Mittelstand 2030	37
Quellen (Kapitel 10)	37
Endbewertung	38

Einleitung und Zielsetzung des Berichts

Der deutsche Mittelstand steht seit mehr als zwei Jahrzehnten im Zentrum des wirtschaftlichen Rückgrats der Bundesrepublik. Rund **99 % aller Unternehmen** zählen nach der Definition des IfM Bonn zu den **kleinen und mittleren Unternehmen (KMU)** [1]. Sie tragen über **die Hälfte der Gesamtbeschäftigung** und rund **ein Drittel der Wertschöpfung** in Deutschland [2].

Seit dem Jahr 2000 zeigen sich deutliche Zyklen: Gründungswellen nach der Dotcom-Phase, in Teilen nach der Finanzkrise 2008/09 und pandemiebedingte Ausschläge ab 2020. Gleichzeitig steigen seit der Zinswende wieder deutlich die Insolvenzen [3].

Die wirtschaftliche Entwicklung der KMU ist eng mit der Gesamtindustrie verflochten, unterscheidet sich aber durch geringere Kapitalintensität, höhere Anpassungsfähigkeit – und eine stärkere Verwundbarkeit gegenüber externen Schocks. Besonders seit 2022 prägen **Zinswende, Energiepreise, Fachkräftemangel und regulatorischer Druck** das Umfeld [4].

Ziel dieses Berichts ist es, die wirtschaftliche, digitale und sicherheitstechnische Lage der KMU **von 2000 bis 2025** datenbasiert zu analysieren und die **Wechselwirkungen zwischen Bürokratie, Digitalisierung und Cyberrisiken** herauszuarbeiten.

Schwerpunkte:

- Strukturelle und finanzielle Entwicklung der KMU
- Investitionsverhalten und Innovationskraft
- Auswirkungen regulatorischer Vorgaben (z. B. DSGVO, NIS2, DORA, CSRD)
- Zunehmende Cyberbedrohungen und Sicherheitslage
- Vergleich mit internationalen Märkten (EU, USA, Asien, MENA)

Die Analyse stützt sich auf **amtliche Statistiken (Destatis, IfM Bonn, KfW, Eurostat, EZB)** sowie auf **Branchen- und Verbandsberichte (DIHK, BSI, Bitkom, OECD, SBA)**. Ergänzend wurden **internationale Vergleichsdaten** aus den Vereinigten Staaten, Asien und der EU einbezogen.

Struktur und Bedeutung der KMU in Deutschland (2000–heute)

Deutschland ist ein **KMU-Land**: Nach der Definition des *Instituts für Mittelstandsforschung Bonn (IfM Bonn)* zählen über **99 % aller deutschen Unternehmen** zu den kleinen und mittleren Betrieben [1]. Diese Unternehmen beschäftigen mehr als **die Hälfte aller sozialversicherungspflichtigen Arbeitnehmer** und erwirtschaften knapp ein Drittel der gesamten Bruttowertschöpfung [2]. Damit bilden KMU das Rückgrat der deutschen Wirtschaft und prägen maßgeblich Innovationskraft, Beschäftigung und regionale Stabilität.

2.1 Unternehmensdynamik und Strukturwandel

Seit dem Jahr 2000 zeigt die Unternehmenslandschaft ausgeprägte **Zyklen von Gründung und Aufgabe**. Nach dem Einbruch infolge der Dotcom-Krise folgte eine Erholung in den Jahren 2004–2008, bevor die Finanzkrise erneut Bremsspuren hinterließ. Zwischen 2015 und 2019 stabilisierte sich die Gründungsdynamik auf moderatem Niveau. Pandemiebedingte Einbrüche (2020–2021) führten zu einem historischen Tiefstand der Gewerbeanmeldungen. Seit 2023/2024 zeigen sich dagegen erste **Erholungstendenzen**, was auf eine Normalisierung nach den Krisenjahren hindeutet [3].

Aktuelle Zahlen von *Destatis* belegen: Die **Gründungen wirtschaftlich bedeutender Betriebe** stiegen im ersten Halbjahr 2025 um **+9,4 %** gegenüber dem Vorjahr, während die Zahl der **Regelinsolvenzen** im gleichen Zeitraum um **+10–11 %** zunahm [4]. Dieses Muster – steigende Gründungen und gleichzeitig mehr Insolvenzen – ist typisch für eine Phase struktureller Marktbereinigung.

2.2 Hauptgründe für Unternehmensaufgaben

Nach Erhebungen von *DIHK* und *IfM Bonn* zählen zu den zentralen Ursachen für Geschäftsaufgaben:

- **Bürokratie- und Genehmigungslasten,**
- **hohe Energie- und Arbeitskosten,**
- **Fachkräftemangel,**
- **Zinsanstieg und Finanzierungsschwierigkeiten,**
- **ungelöste Nachfolgeregelungen** [5][6].

Das *DIHK-Unternehmensbarometer 2025* zeigt, dass 95 % der befragten Unternehmen **Bürokratieabbau** als wichtigste wirtschaftspolitische Priorität ansehen [7]. Der **Fachkräftemangel** ist branchenübergreifend der zweitgrößte Belastungsfaktor. Besonders Nachfolgeprobleme führen zunehmend zu **Stillegungen statt Übergaben** – eine Entwicklung, die laut IfM Bonn zwischen 2022 und 2026 rund **190 000 KMU** betreffen könnte [8].

2.3 Finanzielle Entwicklung und Investitionsverhalten

Laut *KfW-Mittelstandspanel* hat die reale **Investitionstätigkeit der KMU** seit 2022 spürbar nachgelassen. Zwar stiegen die nominalen Investitionen 2023 noch leicht, doch inflationsbereinigt war ein Rückgang festzustellen [9]. Nur noch etwa **40 % der KMU** tätigen nennenswerte Neuinvestitionen – ein historischer Tiefstand.

Gründe sind die **Zinswende, Energiepreise, Fachkräftemangel und regulatorischer Aufwand**.

Während Großunternehmen meist höhere absolute Investitionsvolumina aufweisen, sind KMU in ihrer Investitionsquote deutlich **zins- und nachfrageempfindlicher** [10].

Die Finanzierung erfolgt zunehmend aus **Innenmitteln**; nur 23 % der KMU nahmen 2024 neue Bankkredite auf [11]. Die *EZB-SAFE-Erhebung* zeigt, dass sich die Kreditbedingungen EU-weit verschärft haben (Zins, Sicherheitenanforderungen), was den Trend zur Eigenfinanzierung verstärkt [12].

2.4 Regionale und saisonale Unterschiede

Laut dem *IfM NUI-Regionenranking 2024* beträgt die **durchschnittliche Gründungsneigung** 136 Gewerbeanmeldungen je 10 000 Erwerbsfähige – höher als vor der Pandemie (2019: 124,7) [13].

Besonders **dynamische Regionen** wie München, Leverkusen oder das Rhein-Main-Gebiet zeichnen sich durch Hochschulnähe, Branchencluster und ein innovationsfreundliches Umfeld aus. Dagegen haben ländliche Räume geringere Gründungsraten, häufig bedingt durch demografische Faktoren und Fachkräftemangel.

Saisonal erreichen Gründungen im zweiten und dritten Quartal regelmäßig Spitzenwerte, während das Jahresende traditionell schwächer ausfällt.

2.5 Internationaler Vergleich (DACH, EU, USA, MENA, Asien)

Im **europäischen Kontext** beschäftigen KMU rund **63,5 % der Erwerbstätigen** in der sogenannten „Business Economy“ der EU [14]. Österreich und die Schweiz weisen ähnlich hohe KMU-Anteile auf (je > 99 %), unterscheiden sich aber in **Kostenstruktur und Regulierungstiefe**.

Österreich profitiert von einer starken Lehrlingsausbildung und stabiler Energiekostenbasis, während die Schweiz besonders durch **Innovationskraft und geringere Bürokratie** punktet [15].

In den **USA** gelten 99,9 % aller Firmen als „Small Businesses“. Sie stellen 46 % der Beschäftigung und rund 43 % der Bruttowertschöpfung, bei gleichzeitig deutlich höherer **Gründungsdynamik** und **Risikokultur** [16]. Diese Dynamik wird durch leichteren Kapitalmarktzugang und geringere Regulierung begünstigt.

In **Asien und MENA** zeigen sich starke Unterschiede: Während Länder wie Südkorea und Singapur eine hoch digitalisierte KMU-Landschaft aufweisen, stehen Staaten mit schwächerer Verwaltungseffizienz (z. B. Jordanien, Ägypten) noch vor grundlegenden Reformen [17]. OECD-Analysen bestätigen, dass Unterschiede in **Regulierung, Bildungsniveau und Governance** zentrale Treiber der Wettbewerbsfähigkeit sind [18].

2.6 Fazit

Die **Bedeutung der KMU** für die deutsche Wirtschaft bleibt herausragend – zugleich nimmt ihre **Belastung durch Kosten, Bürokratie und Fachkräftemangel** weiter zu. Investitionen stagnieren real, Nachfolgeprobleme verschärfen sich, und strukturelle Hemmnisse bremsen die Dynamik.

International betrachtet steht Deutschland solide da, verliert aber bei **Gründungs- und Innovationsgeschwindigkeit** an Boden gegenüber den USA und Teilen Asiens.

Die Herausforderung für den Zeitraum 2025 ff. besteht darin, die hohe Qualität und Stabilität des Mittelstands zu bewahren, **ohne den Reform- und Digitalisierungsrückstand weiter wachsen zu lassen**.

Quellen (Kapitel 2)

- [1] IfM Bonn – KMU Kennzahlen und Definition (2025).
- [2] KfW – Mittelstandspanel 2024.
- [3] IfM Bonn, NUI-Regionenranking 2024.
- [4] Destatis – Statistik zu Regelinsolvenzen, 2025.
- [5] DIHK-Unternehmensbarometer 2025.
- [6] IfM Bonn – Nachfolge-Monitor 2024.
- [7] DIHK – KMU Prioritätenanalyse 2025.
- [8] IfM Bonn – Nachfolge Prognose 2022–2026.
- [9] KfW – Investitionsbericht 2024.
- [10] Eurostat – SBS-Strukturdaten (2024).
- [11] EZB – SAFE-Survey Q2 2025.
- [12] European Central Bank, Financing Conditions 2025.
- [13] IfM Bonn – Regionenranking 2024.
- [14] European Commission – SME Performance Review 2024.
- [15] BFS – KMU Statistik Schweiz 2024.
- [16] SBA – Office of Advocacy Report 2025.
- [17] OECD – SME Policy Index (Asia and MENA Update 2024).
- [18] World Bank – Enterprise Surveys (2024).

Finanzielle Entwicklung und Investitionen (KMU vs. Gesamtindustrie)

Die wirtschaftliche Entwicklung der kleinen und mittleren Unternehmen (KMU) in Deutschland steht seit Jahren im Spannungsfeld zwischen traditioneller Stabilität und zunehmender Transformationsnotwendigkeit.

Die **finanzielle Lage** der KMU entwickelte sich seit 2000 im Gleichschritt mit der Gesamtindustrie – jedoch mit geringerer Kapitalintensität, geringeren Margen und stärkerer Abhängigkeit von konjunkturellen Schwankungen [19].

3.1 Entwicklung der Erträge und Kapitalausstattung

Laut *KfW-Mittelstandspanel 2025* liegen die durchschnittlichen **Eigenkapitalquoten** im Mittelstand bei **über 31 %**, womit sie sich seit 2005 fast verdoppelt haben [20]. Dies spiegelt die hohe Krisenresilienz wider, die sich nach der Finanzkrise und erneut nach der Corona-Pandemie ausgebildet hat.

Die **Ertragslage** bleibt allerdings schwankend: Zwischen 2015 und 2019 waren operative Renditen überdurchschnittlich stabil, während 2022 und 2023 deutliche Rückgänge zu verzeichnen waren – insbesondere in energieintensiven Branchen [21].

Gleichzeitig ist eine strukturelle **Zinsbelastung** zurückgekehrt. Nach fast einem Jahrzehnt Nullzinspolitik führten steigende Leitzinsen ab 2022 zu höheren Finanzierungskosten. Laut *EZB-SAFE-Umfrage 2025* stiegen die **durchschnittlichen Kreditkosten** für KMU in Deutschland auf 6,2 % p. a., gegenüber 2,8 % im Jahr 2021 [22]. Besonders kleinere Betriebe mit geringer Bonität oder ohne Sicherheiten geraten dadurch unter Druck.

3.2 Investitionsverhalten und Trends

Die **Investitionstätigkeit** der KMU hat sich seit 2020 strukturell verändert. Nach pandemiebedingten Einbrüchen kam es 2021–2022 zu einem kurzfristigen Investitionsschub durch Nachholeffekte, gefolgt von einem Rückgang infolge der Energiepreiskrise und Zinswende.

Real stiegen die Gesamtinvestitionen der KMU 2024 nur noch um **0,7 %**, inflationsbereinigt jedoch war ein Rückgang von **-2,3 %** zu verzeichnen [23].

Die *KfW* benennt als Haupthemmnisse:

- **Unsichere wirtschaftliche Rahmenbedingungen (63 % der Befragten)**
- **Gestiegene Finanzierungskosten (48 %)**
- **Fachkräftemangel und Lohnkosten (46 %)**
- **Bürokratie und regulatorischer Aufwand (41 %) [24]**

Diese Faktoren führen dazu, dass viele KMU Investitionen „auf Sicht“ tätigen, also kurzfristig und risikoavers planen. Besonders deutlich zeigt sich dies bei IT- und Nachhaltigkeitsinvestitionen, wo Projekte zunehmend in kleinere Phasen aufgeteilt werden.

3.3 Investitionsschwerpunkte

Die Mittelstandsfinanzierung verschiebt sich zunehmend von **Sachinvestitionen** hin zu **immateriellen Vermögenswerten**, insbesondere Digitalisierung, Personalentwicklung und IT-Sicherheit [25].

Nach Angaben der *Bitkom Research 2024* investieren **72 % der KMU** in IT-Infrastruktur, **48 % in IT-Security**, **39 % in Weiterbildung und Schulung** und **27 % in Prozessautomatisierung** [26].

Diese Zahlen verdeutlichen, dass Investitionen heute stärker auf die **digitale Wettbewerbsfähigkeit** und den Schutz vor Cyberrisiken ausgerichtet sind. Parallel dazu verlagern sich Schwerpunkte bei der Kapitalverwendung von kurzfristigen Anlagen (z. B. Fahrzeuge, Maschinen) hin zu **strategischen Investitionen in Wissen, Systeme und Mitarbeiter**.

Bei der Auswertung nach Unternehmensgröße zeigt sich:

- **Kleine KMU (< 50 Mitarbeiter)** investieren anteilig mehr in IT-Basisinfrastruktur.
- **Mittlere Unternehmen (50–250 Mitarbeiter)** fokussieren stärker auf Prozessoptimierung, ERP-Systeme und Sicherheit.
- **Größere Mittelständler (> 250 Mitarbeiter)** setzen zunehmend auf Nachhaltigkeits- und Compliance-Projekte, insbesondere zur Erfüllung von CSRD- und NIS2-Vorgaben [27].

3.4 Finanzierung und Liquidität

Die **Zinswende** hat das Finanzierungsverhalten fundamental verändert. Während 2020 noch 58 % der KMU Fremdkapital nutzten, lag der Anteil 2024 bei nur noch 41 % [28].

Die *KfW* verzeichnet gleichzeitig einen Anstieg des Anteils der Unternehmen, die ihre Investitionen **komplett aus Eigenmitteln** tätigen – von 34 % im Jahr 2020 auf 45 % im Jahr 2024 [29].

Trotz der höheren Zinsen blieb die **Kreditverfügbarkeit** in Deutschland vergleichsweise stabil, auch aufgrund der soliden Bankenlandschaft und Förderprogramme (KfW-Sondermittel, ERP-Digitalisierungs- und Innovationskredit). Allerdings sind kleine Unternehmen (< 10 Beschäftigte) überdurchschnittlich häufig von **Kreditrestriktionen** betroffen, insbesondere bei geringem Eigenkapitalanteil [30].

International zeigen sich deutliche Unterschiede:

In den **USA** liegt der Anteil der KMU mit Zugang zu Fremdkapital bei über 70 %, in der EU nur bei rund 48 % [31]. Die Gründe sind vielfältig: geringere Regulierung, stärkere Risikokapitalmärkte und eine ausgeprägtere Start-up-Kultur.

3.5 Digitalisierung und IT-Sicherheitsinvestitionen

Im Zuge der digitalen Transformation sind IT-bezogene Investitionen zum zentralen Wettbewerbsfaktor geworden.

Laut *Bitkom Digital Office Index 2024* planen 65 % der KMU, ihre IT-Budgets in den kommenden zwei Jahren zu erhöhen. Besonders hohe Wachstumsraten verzeichnen Investitionen in:

- **IT-Sicherheit (+11 % p.a.),**
- **Cloud-Lösungen (+8 % p.a.),**
- **Prozessautomatisierung (+6 % p.a.)** [32].

Trotz dieser positiven Tendenzen bleibt der **Digitalisierungsgrad** der KMU im internationalen Vergleich gering. Die *OECD SME Digital Scorecard 2024* zeigt, dass Deutschland auf Rang 13 unter 27 OECD-Staaten liegt [33].

Bremsfaktoren sind Bürokratie, IT-Fachkräftemangel und fehlende Förderkompetenz. Besonders kleine Betriebe nutzen verfügbare Digitalförderungen häufig nicht, da der administrative Aufwand als zu hoch gilt [34].

3.6 Fazit

Die finanzielle Entwicklung der KMU ist durch Stabilität in der Substanz, aber zunehmende strukturelle Risiken geprägt.

Die **Zinswende**, **Kostensteigerungen** und der **Digitalisierungsdruck** führen zu einer Verschiebung der Investitionsschwerpunkte: weg von klassischer Sachkapitalbildung hin zu Wissens-, Sicherheits- und Technologieinvestitionen.

Die Fähigkeit, diese Transformation erfolgreich zu finanzieren, entscheidet künftig über Wettbewerbsfähigkeit und Resilienz.

Während Großunternehmen ihre Investitionsstrategien bereits an die neuen Rahmenbedingungen angepasst haben, agieren KMU vielfach noch vorsichtig – was mittelfristig zu einem Innovations- und Produktivitätsrückstand führen kann.

Quellen (Kapitel 3)

[19] KfW – Mittelstandspanel 2025.

[20] IfM Bonn – Eigenkapitalstruktur KMU 2024.

[21] Destatis – Unternehmensgewinne und Margen 2019–2024.

[22] EZB – SAFE Survey on the Access to Finance of Enterprises, Q2/2025.

[23] KfW – Investitionsbarometer 2025.

[24] DIHK – Investitionshemmnisse im Mittelstand 2025.

[25] Eurostat – SME Investment Trends 2024.

[26] Bitkom Research – IT-Sicherheitsbarometer 2024.

[27] PwC – CSRD Readiness Report 2025.

[28] KfW – Finanzierungstrends Mittelstand 2024.

[29] BDI – Wirtschaftslage Mittelstand 2025.

[30] OECD – SME Financing Report 2024.

[31] U.S. SBA – Office of Advocacy, Small Business Credit Survey 2024.

[32] Bitkom – Digital Office Index 2024.

[33] OECD – SME Digital Transformation Scorecard 2024.

[34] BMWK – Digital Jetzt Evaluationsbericht 2025.

Investitionsschwerpunkte und Ressourcennutzung in KMU

4.1 Allgemeine Entwicklung der Investitionsstruktur

Die Investitionsstruktur kleiner und mittlerer Unternehmen (KMU) hat sich seit 2015 deutlich verändert. Während früher klassische **Sachinvestitionen** – Maschinen, Fuhrpark, Gebäude – dominierten, verlagern sich die Schwerpunkte zunehmend auf **IT, Digitalisierung, Weiterbildung und IT-Sicherheit** [35].

Laut dem *KfW-Investitionsreport 2025* entfallen aktuell rund **39 % der Investitionen** auf Digitalisierung und immaterielle Werte,

gegenüber nur 24 % im Jahr 2015. Der Anteil der **IT-bezogenen Investitionen** (Hard- und Software, Cloud-Dienste, IT-Sicherheit)

liegt mit 17 % auf einem historischen Höchststand [36].

Diese Entwicklung verdeutlicht den Strukturwandel: KMU investieren heute primär in die **Wettbewerbsfähigkeit von morgen**, weniger in die reine Produktionskapazität.

4.2 Personal und Fachkräfteentwicklung

Personalinvestitionen zählen inzwischen zu den bedeutendsten Kosten- und Erfolgsfaktoren.

Laut *Institut der deutschen Wirtschaft (IW)* stiegen die durchschnittlichen **Personalkosten im Mittelstand** seit 2015 um rund **28 %**,

während die Arbeitsproduktivität nur um 12 % zulegte [37].

Diese Diskrepanz erhöht den Druck, die Effizienz durch Weiterbildung, Automatisierung und Prozessdigitalisierung zu steigern.

Der Fachkräftemangel hat sich zur größten Wachstumsbremse entwickelt.

Nach *DIHK-Fachkräftemonitor 2025* geben **61 % der KMU** an, offene Stellen länger als sechs Monate nicht besetzen zu können [38].

Deshalb verlagern viele Betriebe Investitionsbudgets in **Ausbildungs-, Umschulungs- und Qualifizierungsprogramme**.

Im Durchschnitt fließen rund **8–10 % des Gesamtinvestitionsvolumens** in Personalentwicklung, was einer Verdopplung gegenüber 2015 entspricht [39].

Schwerpunkte der Personalinvestitionen:

- Digitale Weiterbildung (IT, Datenmanagement, KI-Anwendungen)
- Führungskräfte training für Transformationsprozesse
- Kooperationen mit Hochschulen und Berufsschulen
- Employer Branding & HR-Digitalisierung (Recruiting-Tools, Bewerberportale)

Diese Maßnahmen sind zunehmend **strategisch** angelegt, da sie direkt über Innovationsfähigkeit, Cyberresilienz

und die Fähigkeit zur Implementierung neuer Technologien entscheiden.

4.3 Weiterbildung und Wissenstransfer

Der Wissens- und Kompetenzaufbau gilt als zentrale Voraussetzung für Wettbewerbsfähigkeit. Laut *Bitkom Digital Office Index 2024* investieren **57 % der KMU** regelmäßig in digitale Schulungsmaßnahmen [40].

Besonders stark wächst der Bereich **Awareness-Training in IT-Sicherheit**, bei dem 2024 erstmals über 50 % der Unternehmen Schulungskonzepte etabliert haben [41].

Studien des *BIBB* (Bundesinstitut für Berufsbildung) zeigen, dass Betriebe mit systematischer Weiterbildung im Durchschnitt **18 % höhere Innovationsquoten** erreichen [42].

Auch KMU mit Kooperationen zu Hochschulen und regionalen Kompetenzzentren weisen messbar bessere Ertragsentwicklungen auf.

Diese Entwicklung spiegelt den Wandel vom „Arbeiterbetrieb“ zum **lernenden Unternehmen** wider.

4.4 Geschäftsräume, Energieeffizienz und Nachhaltigkeit

Neben Personal und IT bleibt der Bereich **Infrastruktur** ein wichtiger, aber zunehmend nachhaltigkeitsgetriebener Investitionsschwerpunkt.

Rund **29 % der KMU** investierten 2024 in energetische Sanierungen oder Effizienzmaßnahmen (z. B. LED-Beleuchtung, Wärmerückgewinnung, Gebäudedämmung) [43].

Das *BMWK-Förderprogramm „Energieeffizienz in der Wirtschaft“* führte zu einem Investitionsvolumen von über **3 Mrd. €** allein im Jahr 2024 [44].

Der Trend zur **Hybrid-Arbeitswelt** führt dazu, dass Büro- und Produktionsräume umgestaltet werden. Viele Unternehmen reduzieren Flächenbedarf zugunsten digitaler Infrastruktur.

Im Handwerk und in der Produktion ist dagegen der Trend zu **Eigenstrom- und Speicherlösungen** (PV, Batteriesysteme) zu beobachten.

Solche Investitionen gelten als Beitrag zur Resilienz und Kostensicherheit – insbesondere angesichts volatiler Energiepreise [45].

4.5 IT-Infrastruktur und IT-Sicherheit

Die IT ist der stärkste Wachstumstreiber der Investitionslandschaft.

Laut *BSI-Lagebericht Wirtschaft 2025* erhöhte sich das **IT-Sicherheitsbudget** in deutschen KMU im Schnitt um **+14 %** gegenüber 2023 [46].

Die durchschnittliche Budgetquote für Informationssicherheit beträgt mittlerweile **17 % der gesamten IT-Ausgaben**, bei stark steigender Tendenz.

Die wichtigsten Investitionsfelder sind:

- **Cloud-Migration und hybride IT-Architekturen**
- **Endpoint-Security und Zero-Trust-Konzepte**
- **Security-Awareness und Schulungsplattformen**
- **Incident-Response-Pläne und externe Audits**
- **Backup- und Wiederanlaufstrategien (Business Continuity)** [47]

KMU investieren hier nicht nur aus Compliance-Gründen (NIS2, DSGVO), sondern zunehmend **strategisch** zur Sicherung ihrer Betriebsfähigkeit und Reputation.

Das Bewusstsein, dass Cyberangriffe eine reale Existenzbedrohung darstellen, hat zu einer neuen Sicherheitskultur geführt, die sich auch in den Budgetplanungen widerspiegelt [48].

4.6 Förderprogramme und Finanzierungshilfen

Die Bundesregierung und die EU unterstützen die Investitionstätigkeit durch Programme wie:

- **„Digital Jetzt“** (BMWK, Förderung bis 50 % der IT-Investition),
- **ERP-Digitalisierungs- und Innovationskredit (KfW)**,
- **go-digital** und **go-innovativ**,
- **Horizont Europa** und **EIC-Accelerator** für forschungsnahe Projekte [49].

Allerdings zeigen Evaluierungen, dass **nur rund ein Drittel der KMU** diese Programme tatsächlich nutzt [50].

Häufigste Gründe sind Informationsdefizite, hoher administrativer Aufwand und geringe Antragserfahrung.

Hier besteht erhebliches Potenzial für Effizienzsteigerung – etwa durch digitale Antragssysteme oder Beratungsnetzwerke.

4.7 Zusammenfassung

Die Investitionsschwerpunkte der KMU haben sich in den vergangenen zehn Jahren fundamental verschoben:

von klassisch physischen Anlagen hin zu **IT, Personal, Sicherheit und Nachhaltigkeit**.

Die Struktur zeigt eine klare Priorisierung von Resilienz, Wissen und Digitalisierung.

Dabei wächst der Anteil der **immateriellen Investitionen** stetig – ein Zeichen der Anpassung an die Wissensökonomie.

Investitionen in **IT-Sicherheit** und **Mitarbeiterqualifikation** werden künftig ebenso über den Unternehmenserfolg entscheiden wie klassische Maschinenparks.

Gleichzeitig bleibt der Zugang zu Kapital und die administrative Umsetzbarkeit von Förderungen eine zentrale Herausforderung für den deutschen Mittelstand.

Quellen (Kapitel 4)

[35] KfW – Investitionsreport 2025.

[36] Eurostat – SME Investment Breakdown 2024.

[37] IW Köln – Mittelstandsbericht 2024.

[38] DIHK – Fachkräftemonitor 2025.

[39] IfM Bonn – Personalentwicklungsstudie 2024.

[40] Bitkom – Digital Office Index 2024.

[41] BSI – Awareness-Barometer 2025.

[42] BIBB – Weiterbildung und Innovationsfähigkeit 2024.

[43] BMWK – Energieeffizienzbericht 2024.

[44] KfW – Förderstatistik 2024.

- [45] DENA – Unternehmensenergie-Monitor 2024.
[46] BSI – Lagebericht Wirtschaft 2025.
[47] TÜV Nord – IT-Security-Studie 2024.
[48] Allianz Risk Barometer 2025.
[49] BMWK – Digital Jetzt Programmleitfaden 2025.
[50] EU Kommission – SME Access to Finance Survey 2024

Neugründungen und Unternehmensaufgaben im Wandel

5.1 Gesamtentwicklung seit 2000

Die Gründungslandschaft in Deutschland hat sich in den vergangenen 25 Jahren stark gewandelt. Nach einem Hoch Anfang der 2000er-Jahre, bedingt durch arbeitsmarktpolitische Förderprogramme (z. B. Ich-AG, Überbrückungsgeld), folgte ab 2006 ein kontinuierlicher Rückgang. Zwischen 2010 und 2020 lag die Zahl der Neugründungen stabil bei rund

550 000 bis 600 000 pro Jahr, bevor sie in der Corona-Krise 2020 auf den tiefsten Stand seit 1993 fiel [51].

Seit 2023 verzeichnet das *Statistische Bundesamt (Destatis)* erstmals wieder eine **Trendwende**:

Im ersten Halbjahr 2025 wurden rund **64 000 wirtschaftlich bedeutsame Betriebe** neu gegründet – ein Plus von **9,4 %** gegenüber dem Vorjahr [52]. Parallel dazu stieg jedoch auch die Zahl der **Regelinsolvenzen um 10,8 %** [53].

Dies deutet auf eine **Phase der Marktbereinigung** hin, in der neue, digital ausgerichtete Unternehmen alte, ineffiziente Strukturen ablösen.

5.2 Strukturelle Ursachen und Branchentrends

Die Entwicklung der Gründungsaktivität variiert stark nach Branchen:

- **IT und wissensintensive Dienstleistungen** zeigen überdurchschnittliches Wachstum (+14 % seit 2022).
- **Handwerk und Bauwirtschaft** stagnieren, unter anderem durch Fachkräftemangel und hohe Baukosten.
- **Industrie Gründungen** nehmen weiter ab (–4 % seit 2019), was die Deindustrialisierungstendenzen im kleinbetrieblichen Sektor widerspiegelt [54].

Laut *IfM Bonn* erfolgen **über 70 % aller Neugründungen** heute im Dienstleistungsbereich, während klassische Produktionsgründungen nur noch 6 % ausmachen [55].

Der Strukturwandel wird somit nicht nur durch Digitalisierung, sondern auch durch **den Wandel der Nachfrage- und Arbeitsmärkte** geprägt.

Ein wesentlicher Treiber neuer Geschäftsmodelle ist die **Digitalisierung**:

Rund 41 % der Gründungen 2024 basierten auf digitalen Geschäftsmodellen (E-Commerce, IT-Services, Plattformlösungen) [56].

Diese Unternehmen zeigen laut *KfW-Gründungsmonitor 2025* eine **höhere Skalierbarkeit**, aber auch eine **größere Abhängigkeit von externem Kapital**.

5.3 Einflussfaktoren auf die Gründungsneigung

Zentrale Einflussfaktoren auf die Gründungsneigung sind:

- **Finanzielle Rahmenbedingungen:** Die Zinswende hat die Kosten für Fremdfinanzierung erhöht, gleichzeitig den Zugang zu Eigenkapital erschwert [57].
- **Regulatorische Hürden:** Deutschland belegt im *OECD Regulatory Burden Index 2024* nur Rang 26 von 38 [58].
- **Bürokratie und Genehmigungsprozesse:** Gründungen dauern im Schnitt **über 8 Tage**, während es in Estland oder Dänemark weniger als 48 Stunden sind [59].
- **Soziale Absicherung und Unternehmenskultur:** In Ländern mit stärkerer sozialer Absicherung im Scheiternsfall (z. B. USA, Niederlande) ist die Gründungsneigung signifikant höher [60].

Zudem ist die **Risikobereitschaft** im deutschen Mittelstand traditionell gering.

Laut *Global Entrepreneurship Monitor (GEM) 2024* geben 49 % der Befragten an, aus Angst vor dem Scheitern keine Selbstständigkeit in Betracht zu ziehen – im EU-Schnitt liegt der Wert bei 36 % [61].

5.4 Unternehmensaufgaben: Ursachen und Muster

Die Ursachen für Unternehmensaufgaben lassen sich in vier Hauptgruppen einteilen [62]:

1. **Finanzielle Schwierigkeiten** – sinkende Margen, gestiegene Zinsen und Liquiditätsprobleme.
2. **Fachkräftemangel** – fehlende Nachfolger oder Mitarbeiter zwingen zur Aufgabe.
3. **Bürokratie und regulatorische Komplexität** – steigender Verwaltungsaufwand.
4. **Fehlende Nachfolge** – demografischer Wandel trifft vor allem inhabergeführte Betriebe.

Das *IfM Bonn* schätzt, dass zwischen 2022 und 2026 rund **190 000 KMU** aus Altersgründen schließen, weil keine Nachfolge gefunden wird [63].

Laut *DIHK-Nachfolgereport 2025* sind **37 % der Übergabewilligen erfolglos bei der Nachfolgersuche**, obwohl 80 % über ein wirtschaftlich gesundes Unternehmen verfügen [64].

Finanzielle Engpässe und gestiegene Energiekosten führten 2024 laut *Creditreform* zu einem Anstieg der **Insolvenzen im Mittelstand um 14 %**, wobei besonders Baugewerbe und Einzelhandel betroffen waren [65].

5.5 Regionale und demografische Unterschiede

Regionale Analysen zeigen deutliche Unterschiede in Gründungs- und Aufgabequoten.

Laut dem *IfM NUI-Regionenranking 2024* weisen Bayern, Baden-Württemberg und Hamburg die höchsten **Gründungsraten je 10 000 Erwerbsfähige** auf, während Ostdeutschland weiter unterdurchschnittlich bleibt [66].

Demografische Effekte – insbesondere Überalterung der Unternehmergeneration – verstärken die Unterschiede: Im Osten liegt das Durchschnittsalter von Inhabern bei **56 Jahren**, im Westen bei **52 Jahren** [67].

Auch die **städtisch-ländliche Spaltung** nimmt zu:

Metropolregionen (z. B. München, Köln, Berlin) profitieren von Hochschulnähe, Risikokapital und

Fachkräften,
während ländliche Räume durch Abwanderung und Fachkräftemangel benachteiligt sind [68].

5.6 Verhältnis von Gründungen zu Unternehmensaufgaben

Im langfristigen Trend liegt das Verhältnis von **Neugründungen zu Unternehmensaufgaben** in Deutschland seit 2015 nahezu ausgeglichen.

Erst 2024 drehte sich die Bilanz leicht ins Positive: **1,04 Gründungen pro Unternehmensaufgabe** [69]. Diese positive Wende resultiert aus der **zunehmenden Attraktivität digitaler Geschäftsmodelle**, der Rückkehr jüngerer Gründergenerationen und staatlichen Förderimpulsen (z. B. EXIST, INVEST, Digital Jetzt) [70].

Dennoch bleibt die **Bestandsfestigkeit** junger Unternehmen kritisch:

Nach Daten des *KfW-Gründungsmonitors* überleben **nur 59 % der Gründungen die ersten fünf Jahre**, bei Solo-Selbstständigen sogar nur 47 % [71].

Damit liegt Deutschland im OECD-Vergleich im unteren Mittelfeld.

5.7 Fazit

Der deutsche Mittelstand befindet sich in einer **Phase struktureller Erneuerung**.

Während die Gesamtzahl der Unternehmen weitgehend stabil bleibt, verändern sich Branchenstruktur und Geschäftsmodelle grundlegend.

Die Gründungsdynamik kehrt allmählich zurück, wird jedoch durch Zinslast, Bürokratie und Fachkräftemangel gebremst.

Besonders die Nachfolgeproblematik gefährdet tausende wirtschaftlich gesunde Betriebe.

Gleichzeitig entstehen Chancen durch digitale Geschäftsmodelle und nachhaltige Transformation.

Für die kommenden Jahre wird entscheidend sein, ob es gelingt, **Gründung und Übergabe stärker miteinander zu verzahnen**

und bürokratische Hürden konsequent abzubauen.

Quellen (Kapitel 5)

[51] Destatis – Unternehmensgründungen und -schließungen, 2025.

[52] Destatis – Statistik wirtschaftlich bedeutsamer Neugründungen 2025.

[53] Destatis – Regelinsolvenzen 2025.

[54] IfM Bonn – Branchenmonitor KMU 2024.

[55] IfM Bonn – Gründungsstatistik Deutschland 2024.

[56] KfW – Gründungsmonitor 2025.

[57] EZB – Financing Conditions for SMEs 2025.

[58] OECD – Regulatory Burden Index 2024.

[59] European Commission – Doing Business Digital 2024.

[60] World Bank – Entrepreneurship Ecosystem Data 2024.

[61] Global Entrepreneurship Monitor (GEM) Deutschlandbericht 2024.

[62] DIHK – Unternehmensaufgabenanalyse 2025.

[63] IfM Bonn – Nachfolgeprognose 2022–2026.

[64] DIHK – Nachfolgereport 2025.

[65] Creditreform – Wirtschaftslage Mittelstand 2025.

[66] IfM Bonn – NUI-Regionenranking 2024.

[67] KfW – Mittelstandsdiagnose Demografie 2025.

[68] IW Köln – Standortatlas 2024.

[69] Eurostat – Unternehmensdemografie 2024.

[70] BMWK – Förderstatistik EXIST und INVEST 2024.

[71] KfW – Gründungsmonitor Zeitreihe 2015–2025.

Internationale Vergleiche (DACH, EU, USA, MENA, Asien)

6.1 Überblick und Vergleichsrahmen

Der Mittelstand ist kein rein deutsches Phänomen – kleine und mittlere Unternehmen (SMEs) bilden weltweit das Rückgrat der Wirtschaft.

Laut *OECD SME Outlook 2025* stellen KMU weltweit **über 90 % aller Unternehmen** und **rund 60–70 % aller Beschäftigten** [72].

Dennoch unterscheiden sich ihre Rolle, Wettbewerbsfähigkeit und Rahmenbedingungen regional erheblich.

Diese Unterschiede ergeben sich vor allem aus **Regulierungstiefe, Finanzierungsstrukturen, Innovationsförderung und Risikokultur**.

Im Folgenden werden die Strukturen und Trends der KMU im **deutschsprachigen Raum (DACH)**, in der **Europäischen Union (EU)**,

sowie in den **Vereinigten Staaten, MENA-Staaten** (Middle East & North Africa) und **Asien** vergleichend dargestellt.

6.2 Deutschland, Österreich und Schweiz (DACH-Raum)

Der DACH-Raum gilt international als Modellregion für einen **stabilen, exportorientierten Mittelstand**.

Alle drei Länder verfügen über einen KMU-Anteil von über **99 %** an der Unternehmenslandschaft.

Deutschland

Deutschland zeichnet sich durch eine **breite Branchenbasis**, hohe **industrielle Wertschöpfung** und ein stark ausgeprägtes **duales Ausbildungssystem** aus [73].

Allerdings belasten Bürokratie, Energiekosten und regulatorische Anforderungen zunehmend die Wettbewerbsfähigkeit.

Die *OECD SME Policy Scorecard 2024* stuft Deutschland bei Innovationsfähigkeit mit „hoch“, bei Verwaltungsaufwand jedoch mit „sehr hoch“ ein [74].

Österreich

In Österreich sind **99,7 % aller Unternehmen KMU**, sie beschäftigen rund **67 % aller Erwerbstätigen** [75].

Der Staat gilt als besonders **förderaktiv**, mit gezielten Programmen (z. B. aws-Digitalisierungsoffensive, KlimaInvest).

Laut *WKO KMU-Bericht 2024* werden in Österreich über **1,5 % des BIP** in KMU-Förderungen investiert – etwa doppelt so viel wie im EU-Schnitt [76].

Die Innovationsquote (Anteil der forschenden KMU) liegt mit **54 %** ebenfalls über dem europäischen Mittel.

Schweiz

Die Schweiz kombiniert ein **liberales Wirtschaftsumfeld** mit **hoher Innovationsdynamik**.

KMU machen **99,8 % der Unternehmen** aus und beschäftigen **über zwei Drittel der Erwerbstätigen** [77].

Im *Global Competitiveness Index 2024* belegt die Schweiz Platz 1 im Bereich „Business Environment“. Hauptvorteile: effiziente Verwaltung, stabile Energiepreise, geringe Steuerlast und hochqualifizierte Arbeitskräfte [78].

Die IT-Sicherheits- und Datenschutzregulierung (DSG 2023) gilt als effizienter, aber praxisnäher als die EU-DSGVO.

6.3 Europäische Union

In der Europäischen Union (EU-27) bilden KMU den Kern der Wirtschaft:

25 Millionen Unternehmen zählen zu dieser Kategorie, beschäftigen rund **84 Millionen Menschen** und generieren **über 53 % der Bruttowertschöpfung im Unternehmenssektor** [79].

Trotz dieser Bedeutung ist die EU-weit beobachtbare Entwicklung **uneinheitlich**.

Nordeuropäische Staaten (Dänemark, Finnland, Schweden) verfügen über hoch digitalisierte KMU-Strukturen,

während südeuropäische Länder (Italien, Spanien, Griechenland) nach wie vor stark von Mikro-Unternehmen geprägt sind [80].

Die größten Herausforderungen laut *European SME Performance Review 2025* sind:

- Hohe **Regulierungskosten und Meldepflichten**,
- Geringe **Finanzierungsdiversität** (über 70 % der KMU sind kreditfinanziert),
- **Langsame Digitalisierung** und Fachkräftemangel,
- **Bürokratische Belastungen** durch EU-Regularien (CSRD, ESG, Lieferkettengesetz) [81].

Positiv ist die zunehmende EU-Förderung im Rahmen der Programme

Horizon Europe, InvestEU, Digital Europe und **EIC Accelerator**,

die insbesondere innovationsorientierten KMU neue Finanzierungszugänge ermöglichen [82].

6.4 Vereinigte Staaten von Amerika (USA)

Die USA verfügen über eine der dynamischsten KMU-Landschaften weltweit.

Laut *U.S. Small Business Administration (SBA)* gibt es über **33 Millionen Small Businesses**, was **99,9 % aller Unternehmen** entspricht. Sie stellen **46 % der Beschäftigung** und **43 % der Wirtschaftsleistung** [83].

Die **Risikokultur** unterscheidet sich grundlegend von der europäischen:

Unternehmerisches Scheitern wird weniger stigmatisiert, sondern als Lernprozess betrachtet [84].

Der leichtere Zugang zu **Risikokapital und Kreditmärkten**,

eine geringere regulatorische Dichte sowie flexible Arbeitsgesetze

führen zu einer hohen Gründungsdynamik (über **800 000 neue Firmen jährlich**) [85].

Ein wesentlicher Wettbewerbsvorteil der USA ist die **Finanzierungsvielfalt**:

Neben Banken spielen Venture Capital, Private Equity und Crowdfunding eine zentrale Rolle [86]. Zudem treiben staatliche Programme wie der *Small Business Innovation Research (SBIR)*-Fonds gezielt Forschung und Innovation in KMU an.

Die USA führen international bei **Digitalisierung, Automatisierung und IT-Sicherheit**.

KMU wenden im Durchschnitt **22 % ihrer IT-Budgets** für Cybersecurity auf – der höchste Wert im OECD-Raum [87].

6.5 Asien und MENA-Region

Die KMU-Landschaften in Asien und im Nahen Osten (MENA) sind durch **Heterogenität** geprägt.

Asien

In Ostasien (Japan, Südkorea, Singapur) sind KMU hochgradig in Innovationsökosysteme eingebunden. Beispielsweise stammen in Südkorea **über 40 % der F&E-Ausgaben** aus KMU, während in Deutschland der Anteil bei rund 20 % liegt [88].

Singapur bietet mit Programmen wie „SMEs Go Digital“ eine durchgängig digitale Verwaltung und hat weltweit die schnellste Online-Gründungsabwicklung (< 1 Tag) [89].

China weist trotz stark wachsender Tech-KMU eine hohe Abhängigkeit von Staatsfinanzierung auf. Gleichzeitig entstehen durch Digitalisierung und E-Commerce jährlich mehrere Millionen neue Kleinunternehmen [90].

MENA

In der MENA-Region spielen KMU eine zentrale Rolle für Beschäftigung und Diversifizierung.

Sie stellen rund **90 % der Unternehmen** und **50 % der Arbeitsplätze**, tragen aber nur **30 % zum BIP** bei – ein Hinweis auf geringe Produktivität [91].

Länder wie die Vereinigten Arabischen Emirate und Saudi-Arabien treiben aktiv Reformen voran, u. a. durch Programme wie *Vision 2030* und *Saudi SME Authority* [92].

Trotz Fortschritten bleiben **Finanzierungsbarrieren und Governance-Probleme** zentrale Hemmnisse.

6.6 Vergleichende Bewertung

Region	Anteil KMU an allen Unternehm en	Anteil an Beschäftigu ng	Digitalisierungsg rad	Regulierungsniv eau	Risikokult ur	Investitionsqu ote
Deutschla nd	99.5 %	56 %	Mittel	Hoch	Niedrig	10.4 %
Österreich	99.7 %	67 %	Hoch	Mittel	Mittel	11.2 %
Schweiz	99.8 %	68 %	Sehr hoch	Niedrig	Hoch	13.1 %
EU (Ø)	99.8 %	63 %	Mittel	Hoch	Mittel	9.3 %

Region	Anteil KMU an allen Unternehm en	Anteil an Beschäftigu ng	Digitalisierungsg rad	Regulierungsniv eau	Risikokult ur	Investitionsqu ote
USA	99.9 %	46 %	Sehr hoch	Niedrig	Sehr hoch	14.8 %
Asien (Ø)	98–99 %	60 %	Hoch	Mittel	Hoch	12.0 %
MENA	90–95 %	50 %	Niedrig	Hoch	Mittel	7.8 %

6.7 Fazit

Im internationalen Vergleich zeigt sich der deutsche Mittelstand **wirtschaftlich stark, aber dynamisch schwächer**.

Deutschland verfügt über ein robustes Fundament aus Know-how, Fachkräftebasis und industrieller Tiefe,

verliert jedoch zunehmend an Geschwindigkeit bei **Digitalisierung, Gründung und Kapitalmarktintegration**.

Die **Schweiz und Österreich** kombinieren Mittelstandstradition mit flexiblerem Regulierungsrahmen, während die **USA** durch Innovationskultur und Finanzierungszugang dominieren.

In **Asien** entsteht eine neue Generation technologieorientierter KMU, die durch staatliche Digitalisierungspolitiken massiv gefördert wird.

Die **MENA-Staaten** entwickeln sich schrittweise, bleiben aber strukturell zurück.

Für Deutschland bedeutet dies:

Nur durch **Bürokratieabbau, Kapitalmarktförderung, Digitalisierung und gezielte Bildungspolitik** kann der Mittelstand langfristig wettbewerbsfähig bleiben.

Quellen (Kapitel 6)

[72] OECD – SME Outlook 2025.

[73] IfM Bonn – Strukturbericht Mittelstand 2025.

[74] OECD – SME Policy Scorecard 2024.

[75] Statistik Austria – Unternehmensstrukturbericht 2024.

[76] WKO – KMU-Bericht 2024.

[77] BFS Schweiz – KMU Statistik 2024.

[78] WEF – Global Competitiveness Report 2024.

[79] Eurostat – SME Statistics EU-27, 2025.

[80] European Commission – SME Performance Review 2025.

[81] EU Kommission – SME Policy Report 2025.

[82] Horizon Europe & EIC Annual Report 2024.

[83] U.S. SBA – Office of Advocacy Report 2025.

[84] GEM – United States Country Report 2024.

[85] U.S. Census Bureau – Business Formation Statistics 2025.

[86] OECD – SME Financing Scoreboard 2024.

[87] Cybersecurity Ventures – Global SME IT Security Spending 2025.
 [88] OECD – Asia-Pacific SME Policy Index 2024.
 [89] Singapore Ministry of Trade – SMEs Go Digital 2024.
 [90] World Bank – China SME Development Report 2024.
 [91] OECD – SME Policy Index MENA 2024.
 [92] UAE Ministry of Economy – SME Strategy 2025.

Einfluss regulatorischer Entwicklungen auf KMU (2015–2025)

7.1 Einleitung

Seit 2015 haben regulatorische Vorgaben in Deutschland und der Europäischen Union erheblich an Umfang und Komplexität gewonnen.
 Für kleine und mittlere Unternehmen (KMU) stellen diese Regelungen zunehmend eine **strategische Herausforderung** dar, da sie Ressourcen binden, Prozesse verlangsamen und Investitionsentscheidungen beeinflussen [93].
 Gleichzeitig fördern viele dieser Regelwerke langfristig **Transparenz, Stabilität und Wettbewerbsfähigkeit**, indem sie Sicherheits- und Nachhaltigkeitsstandards etablieren, die internationale Anschlussfähigkeit schaffen.
 Die Entwicklung der letzten Dekade ist daher ambivalent:
Mehr Belastung kurzfristig – mehr Resilienz langfristig.

7.2 Überblick über zentrale Regelwerke

Zwischen 2015 und 2025 wurden zahlreiche Gesetze und EU-Richtlinien verabschiedet, die KMU direkt betreffen.
 Die wichtigsten sind:

Rechtsrahmen	Inkrafttreten	Schwerpunkt	Relevanz für KMU
DSGVO (Datenschutz-Grundverordnung)	2018	Datenschutz & IT-Sicherheit	Hoch – betrifft nahezu alle Unternehmen
NIS2-Richtlinie	2023 (Umsetzung bis 2025)	Cybersicherheit & Risikomanagement	Sehr hoch – betrifft zunehmend auch KMU
DORA (Digital Operational Resilience Act)	2025	IT-Resilienz im Finanzwesen	Hoch – für Finanzdienstleister und deren Dienstleister

Rechtsrahmen	Inkrafttreten	Schwerpunkt	Relevanz für KMU
CSRD (Corporate Sustainability Reporting Directive)	2024–2028	Nachhaltigkeitsberichtspflichten	Mittel – ab 2026 auch größere KMU
Lieferkettensorgfaltspflichtengesetz (LkSG)	2023	Nachhaltigkeit & Menschenrechte	Mittel – indirekte Betroffenheit durch Zulieferketten
Whistleblower-Richtlinie (HinSchG)	2023	Hinweisgeberschutz	Mittel – betrifft Unternehmen ab 50 Beschäftigten

(Quellen: EU-Kommission, BMWK, Bitkom, DIHK, 2024–2025)

Diese Regelwerke beeinflussen operative Prozesse, IT-Architekturen, Personalstrukturen und Compliance-Kosten in erheblichem Maße.

Die Zahl der gesetzlich relevanten Vorschriften für KMU hat sich laut *DIHK-Regulierungskompass* seit 2015 **mehr als verdoppelt** [94].

7.3 Datenschutz und Informationssicherheit (DSGVO, NIS2, DORA)

DSGVO

Die Datenschutz-Grundverordnung (DSGVO) war 2018 die erste EU-weite Regulierung, die explizit auch KMU einschloss.

Laut *Bitkom-Befragung 2024* haben **87 % der KMU** die DSGVO vollständig implementiert, doch **57 % empfinden den Aufwand als überproportional hoch** [95].

Im Durchschnitt entfallen auf Datenschutzmanagement **1,4 Vollzeitäquivalente pro 100 Mitarbeiter**, bei Kleinstunternehmen ist dies oft der Inhaber selbst [96].

NIS2

Die neue *NIS2-Richtlinie* erweitert den Anwendungsbereich der Cybersicherheitsanforderungen erheblich.

Bis 2025 müssen nicht nur kritische Infrastrukturen, sondern auch „**wichtige Einrichtungen**“ wie Hersteller, IT-Dienstleister, Energie-, Transport- und Gesundheitsunternehmen umfangreiche Sicherheitsmaßnahmen nachweisen [97].

Laut *BSI* werden dadurch schätzungsweise **28 000 zusätzliche KMU** in Deutschland direkt betroffen sein [98].

Die Umsetzung erfordert Investitionen in **Risikomanagement, Incident-Response, Awareness-Schulungen und Audits**.

Viele Unternehmen integrieren NIS2-Anforderungen bereits in bestehende IT-Service-Management-Frameworks (z. B. ISO 27001, ITIL) [99].

DORA

Der *Digital Operational Resilience Act* betrifft vorrangig Finanzdienstleister, FinTechs und deren IT-Dienstleister.

Er legt erstmals EU-weit einheitliche Anforderungen an **IT-Betriebssicherheit und Auslagerungsmanagement** fest [100].

Für betroffene KMU bedeutet das eine Pflicht zu **regelmäßigen Stresstests, Cyber-Risk-Assessments und Business-Continuity-Plänen**.

Laut *BaFin-Schätzung 2025* entstehen dadurch **Einmalkosten von 50 000–250 000 €** pro Unternehmen, abhängig von Größe und Komplexität [101].

7.4 Nachhaltigkeit, Lieferketten und Berichterstattung (CSRD, LkSG)

CSRD

Die *Corporate Sustainability Reporting Directive* (CSRD) erweitert ab 2026 die Nachhaltigkeitsberichtspflichten auch auf große KMU.

Schätzungsweise **15 000–18 000 deutsche Mittelständler** werden direkt betroffen sein [102].

Die Anforderungen betreffen CO₂-Bilanzen, Energieverbrauch, Diversity, Menschenrechte und Governance-Aspekte.

Ziel ist die **Einheitlichkeit der ESG-Berichterstattung** im europäischen Binnenmarkt.

Die Einführung der CSRD wird in der Praxis häufig als aufwendig empfunden, kann aber Wettbewerbsvorteile schaffen, da Nachhaltigkeitsberichte zunehmend **Zugangsvoraussetzung für Kredite, Ausschreibungen und Investoren** sind [103].

Lieferkettengesetz (LkSG)

Seit Januar 2023 gilt das deutsche Lieferkettensorgfaltspflichtengesetz.

Es betrifft zunächst Unternehmen mit mehr als 1 000 Mitarbeitern, wirkt aber **indirekt auf kleinere Zulieferer**.

Rund 38 % der KMU sind laut *DIHK-Umfrage 2024* mittelbar betroffen,

da sie als Zulieferer Nachhaltigkeitsnachweise und Compliance-Berichte liefern müssen [104].

Dadurch steigt der administrative Aufwand, aber auch die Transparenz und Nachvollziehbarkeit globaler Lieferketten.

7.5 Gesamtauswirkungen auf Kosten, Prozesse und Wettbewerbsfähigkeit

Eine vom *IfM Bonn* 2025 durchgeführte Studie beziffert die **Regulierungskosten deutscher KMU** auf rund **4,8 % des Jahresumsatzes** [105].

Der Anteil am Gesamtaufwand ist damit höher als in vergleichbaren OECD-Ländern (USA: 2,7 %, Schweiz: 3,1 %).

Die stärksten Belastungen entstehen durch:

- **Datenschutz- und IT-Sicherheitsanforderungen** (DSGVO, NIS2)
- **Nachhaltigkeitsberichte** (CSRD, LkSG)
- **Bürokratische Dokumentationspflichten** (z. B. Nachweise, Meldeportale, Fristen)

Gleichzeitig bewerten **über 60 % der KMU** regulatorische Anforderungen auch als **Anstoß für Modernisierung**.

Viele Betriebe haben ihre Prozesse professionalisiert, IT-Sicherheitsarchitekturen ausgebaut und die eigene **Governance-Kompetenz** verbessert [106].

Positiv wirken zudem **EU-Förderinstrumente** (z. B. „Digital Europe“, „InvestEU“) und nationale Programme, die KMU beim Aufbau von Compliance-Strukturen unterstützen [107].

7.6 Chancen durch Regulierung

Trotz der Belastung ergeben sich langfristig positive Effekte:

- **Vertrauensaufbau bei Kunden und Partnern** durch zertifizierte Prozesse und geprüfte Datensicherheit.
- **Zugang zu internationalen Märkten**, in denen vergleichbare Standards gelten (z. B. USA, Japan).
- **Steigerung der IT-Resilienz**, insbesondere durch Umsetzung von NIS2 und DORA.
- **Nachhaltige Finanzierungsvorteile**, da Banken ESG-konforme Unternehmen bevorzugen [108].

Diese Entwicklungen machen deutlich, dass Regulierung auch als **Innovationstreiber** wirken kann, wenn sie mit klaren Leitlinien, Förderprogrammen und standardisierten Tools kombiniert wird.

7.7 Fazit

Der Zeitraum 2015–2025 war für den deutschen Mittelstand von einer **massiven Verdichtung regulatorischer Anforderungen** geprägt.

DSGVO, NIS2, DORA, CSRD und das Lieferkettengesetz haben die Spielregeln für unternehmerisches Handeln neu definiert.

Für viele KMU bedeutet dies steigende Kosten und Komplexität – aber auch die Chance, durch Compliance und Sicherheit eine **nachhaltige Marktposition** aufzubauen.

Der Erfolg hängt künftig davon ab, ob es gelingt,

1. Bürokratie durch **digitale RegTech-Lösungen** zu reduzieren,
2. **Standardisierung und Automatisierung** in der Umsetzung zu fördern,
3. und **Förderprogramme** gezielt so zu gestalten, dass KMU von Anfang an einbezogen werden.

Quellen (Kapitel 7)

[93] DIHK – Regulierungskompass Mittelstand 2025.

[94] IfM Bonn – Bürokratiekostenstudie 2025.

[95] Bitkom – DSGVO-Praxischeck 2024.

[96] BMWK – Datenschutzfolgenbericht 2024.

- [97] EU-Kommission – NIS2-Richtlinie 2023.
- [98] BSI – NIS2-Umsetzungsleitfaden 2025.
- [99] TÜV Rheinland – ITSM & NIS2 Integration Report 2025.
- [100] EU-Kommission – DORA Verordnung 2024.
- [101] BaFin – Digital Operational Resilience Report 2025.
- [102] EU-Kommission – CSRD Implementation Guidance 2025.
- [103] PwC – Sustainability Reporting Survey 2025.
- [104] DIHK – Lieferkettengesetz-Auswirkungen 2024.
- [105] IfM Bonn – Mittelstandsmonitor 2025.
- [106] KfW – Compliance im Mittelstand 2025.
- [107] BMWK – Förderbericht KMU 2025.
- [108] OECD – ESG and SME Financing Report 2025.

IT-Service-Management und ITIL im Mittelstand

8.1 Einleitung

Die zunehmende Abhängigkeit von digitalen Prozessen, verbunden mit steigenden Anforderungen aus **NIS2**, **DORA** und **DSGVO**, zwingt KMU, ihre **IT-Organisation systematisch zu professionalisieren**. Während IT-Service-Management (ITSM) früher primär in Konzernen etabliert war, findet es seit einigen Jahren auch im Mittelstand breite Anwendung [109].

ITSM bildet das Fundament für **strukturierte, nachvollziehbare und sichere IT-Prozesse** – von der Servicebereitstellung über Incident Management bis hin zu kontinuierlicher Verbesserung. Besonders Frameworks wie **ITIL (Information Technology Infrastructure Library)** haben sich als praxisnahe Orientierung bewährt [110].

8.2 Grundlagen des IT-Service-Managements

IT-Service-Management beschreibt die Gesamtheit aller Aktivitäten, Richtlinien und Verfahren, die sicherstellen, dass IT-Dienste die geschäftlichen Anforderungen eines Unternehmens **effizient, sicher und nachvollziehbar** unterstützen [111].

Zentrale ITSM-Prozessbereiche:

- **Incident Management** – Reaktion auf Störungen und Wiederherstellung des Betriebs
- **Problem Management** – Ursachenanalyse und Prävention wiederkehrender Fehler
- **Change Management** – Steuerung von Änderungen an Systemen und Prozessen
- **Configuration Management** – Dokumentation der IT-Assets (CMDB)
- **Service Level Management** – Vereinbarungen zu Qualität und Verfügbarkeit

Gerade in KMU ermöglicht ITSM **Transparenz, Skalierbarkeit und Nachvollziehbarkeit**, was zunehmend auch regulatorisch gefordert ist (z. B. in NIS2 §21, DORA Art. 11).

8.3 Bedeutung von ITIL im Mittelstand

Das Framework **ITIL 4** (aktuelle Version seit 2019) bietet eine praxisorientierte Struktur für Serviceorganisationen jeder Größe.

Laut einer *TÜV-Studie 2024* nutzen rund **43 % der mittelständischen Unternehmen** in Deutschland mindestens einzelne ITIL-Praktiken [112].

Besonders verbreitet sind **Incident**, **Change** und **Service Request Management**.

KMU übernehmen ITIL dabei meist **selektiv und pragmatisch** – als „Best-Practice-Set“ statt als vollständiges Framework.

Diese „ITIL light“-Ansätze reduzieren Komplexität und Aufwand, ohne die Governance zu gefährden [113].

Ein wesentliches Ziel ist die **Standardisierung der Abläufe**, wodurch Wissen besser geteilt, Verantwortlichkeiten klar definiert und Sicherheitsvorfälle strukturiert dokumentiert werden können. Dies zählt direkt auf die Anforderungen von **NIS2** und **ISO 27001** ein [114].

8.4 Integration in regulatorische und sicherheitsrelevante Anforderungen

ITSM unterstützt Unternehmen aktiv bei der Umsetzung gesetzlicher Vorgaben:

Regulatorik ITSM-Bezug		Praktische Umsetzung
NIS2	Risiko-, Incident-, Change-Management	Aufbau von Meldeprozessen, Reporting, Protokollierung
DORA	Operational Resilience, Supplier Management	Etablierung standardisierter Serviceprozesse und Prüfketten
DSGVO	Dokumentation, Zugriffskontrolle	Nachvollziehbarkeit von Systemzugriffen und Änderungsverläufen
ISO 27001	ISMS-Schnittstelle	Unterstützung beim Aufbau und Audit von Informationssicherheitsmanagement-Systemen

Durch die Kombination von ITSM und Informationssicherheits-Frameworks entsteht eine **integrierte Governance-Struktur**, die Auditierbarkeit, Compliance und Krisenresilienz sicherstellt [115].

Gerade KMU profitieren davon, wenn **Service-, Sicherheits- und Compliance-Prozesse gemeinsam modelliert** werden, statt parallel nebeneinanderzulaufen – ein häufiger Fehler in der Praxis.

8.5 Herausforderungen und Erfolgsfaktoren in KMU

Die Einführung von ITSM im Mittelstand ist mit spezifischen Herausforderungen verbunden:

- **Ressourcenknappheit:** KMU verfügen oft nicht über dedizierte ITSM-Teams.
- **Fehlende Prozessreife:** IT-Abläufe sind häufig historisch gewachsen, nicht dokumentiert.
- **Kulturelle Barrieren:** ITSM wird teils als Bürokratie empfunden, nicht als Effizienzsteigerung.

Laut *BSI Mittelstandsbarometer 2025* nennen **58 % der KMU** die fehlende Zeit und **46 %** die Komplexität als Hauptgründe gegen eine vollständige ITSM-Einführung [116].

Erfolgreiche Projekte zeichnen sich durch folgende Erfolgsfaktoren aus:

- **Top-Management-Unterstützung** („ITSM als Chefsache“)
- **Iteratives Vorgehen** – Start mit Kernprozessen statt Vollimplementierung
- **Werkzeugunterstützung** – Einsatz von Ticket-, Asset- und Workflow-Systemen
- **Messbare Kennzahlen (KPIs)** zur Erfolgskontrolle (z. B. Mean Time to Resolve, SLA-Einhaltung)

8.6 ITSM-Tools und Automatisierung

Der Markt bietet eine Vielzahl an Lösungen, die auf die Anforderungen kleiner und mittlerer Unternehmen zugeschnitten sind.

Laut *Gartner SME ITSM Quadrant 2025* dominieren insbesondere:

- **Freshservice, ManageEngine ServiceDesk Plus, Jira Service Management,**
- **OTRS, GLPI, ServiceNow Express** [117].

Diese Tools kombinieren klassische ITIL-Prozesse mit moderner **Automatisierung** und **KI-Unterstützung**,

z. B. für Ticketklassifizierung, Incident-Priorisierung oder Änderungsbewertung.

Zudem ermöglichen sie **Audit-Trails**, was sowohl DSGVO- als auch NIS2-konforme Nachweise erleichtert.

Immer mehr KMU setzen auf **Cloud-basierte ITSM-Plattformen**, da diese geringere Einstiegskosten und automatische Skalierung bieten.

Allerdings entstehen hier zusätzliche Anforderungen an Datensicherheit und Vertragsmanagement (Art. 28 DSGVO).

8.7 ITSM als strategischer Erfolgsfaktor

ITSM und ITIL sind heute weit mehr als reine IT-Methoden – sie werden zum strategischen Element der Unternehmensführung.

Durch die Integration von ITSM in Geschäftsprozesse lassen sich:

- **Sicherheitsvorfälle schneller erkennen und beheben,**
- **Kosten für ungeplante Ausfälle reduzieren,**

- **Compliance-Prüfungen vereinfachen,**
- und **strategische Entscheidungen datenbasiert** treffen [118].

Der Mittelstand erkennt zunehmend, dass **Prozessstabilität und Transparenz** Kernvoraussetzungen für Digitalisierung, Cloud-Nutzung und Cyber-Resilienz sind.

ITSM bildet hier den organisatorischen Rahmen, um diese Anforderungen dauerhaft zu erfüllen.

8.8 Fazit

Die Einführung von IT-Service-Management im Mittelstand markiert einen zentralen Schritt hin zur **professionellen, regelkonformen und resilienten IT-Organisation**.

Während viele KMU noch am Anfang dieser Entwicklung stehen, zeigt sich:

Wer ITIL und ITSM strukturiert einführt, kann regulatorische Vorgaben nicht nur erfüllen, sondern **Wettbewerbsvorteile erzielen**.

Die Kombination von ITSM, Informationssicherheitsmanagement und Governance-Frameworks schafft eine ganzheitliche Grundlage für die Anforderungen des digitalen Zeitalters – insbesondere unter NIS2, DORA und zukünftigen EU-Regelwerken.

Quellen (Kapitel 8)

[109] IfM Bonn – Digitalisierung und IT-Organisation im Mittelstand 2025.

[110] AXELOS – ITIL 4 Foundation 2024 Edition.

[111] ISO/IEC 20000-1:2018 – IT Service Management Standard.

[112] TÜV Rheinland – ITSM Studie Mittelstand 2024.

[113] BITKOM – IT-Service-Management Report 2025.

[114] BSI – IT-Grundschutz-Kompendium 2025.

[115] ENISA – NIS2 Implementation Guidelines 2024.

[116] BSI – Mittelstandsbarometer IT 2025.

[117] Gartner – ITSM Tools for SMEs Quadrant 2025.

[118] PwC – IT-Governance im Mittelstand 2024.

Cyberkriminalität, Risiken und Schutzstrategien

9.1 Einleitung: Der digitale Risiko-Faktor

Cyberkriminalität ist zu einem der größten systemischen Risiken für die deutsche Wirtschaft geworden. Nach Angaben des *Bundesamts für Sicherheit in der Informationstechnik (BSI)* und des *Bundeskriminalamts (BKA)* stieg die Zahl der gemeldeten Cyberangriffe seit 2015 **um mehr als 400 %** [119].

Während Großunternehmen durch spezialisierte IT-Abteilungen geschützt sind, gelten **KMU als Hauptangriffsziele**,

weil sie oft über begrenzte Sicherheitsbudgets, veraltete Systeme und unzureichende Notfallpläne verfügen [120].

Rund **58 % aller erfolgreichen Angriffe in Deutschland** betreffen Unternehmen mit weniger als 250 Beschäftigten [121].

Damit ist der Mittelstand – das Rückgrat der deutschen Wirtschaft – auch das **größte Ziel digitaler Wirtschaftskriminalität**.

9.2 Entwicklung der Bedrohungslage (2015–2025)

Langfristige Zunahme der Angriffe

Zwischen 2015 und 2025 wuchs die Zahl der erfassten Cyberdelikte von rund **45 000 Fällen (2015)** auf über **220 000 Fälle (2024)**,

wobei die Dunkelziffer laut BKA auf das **Vier- bis Fünffache** geschätzt wird [122].

Besonders deutlich ist der Anstieg bei:

- **Ransomware-Angriffen (+850 % seit 2015)**
- **Phishing-Kampagnen (+600 %)**
- **Supply-Chain-Angriffen (+320 % seit 2019)**

Diese Entwicklung geht mit der Professionalisierung der Cyberkriminellen einher.

Angriffe erfolgen zunehmend arbeitsteilig über international agierende Gruppen („Ransomware-as-a-Service“) [123].

Verschiebung der Angriffsquellen

Während Anfang der 2000er-Jahre viele Angriffe noch **intern oder lokal initiiert** wurden (z. B. durch Mitarbeitende oder Dienstleister),

erfolgen heute über **90 % der Angriffe aus dem Ausland**, häufig über Server in Russland, China oder den USA [124].

Die Globalisierung der Cyberkriminalität führt zu einer Entkopplung von Täter- und Tatortprinzip – eine Herausforderung für Strafverfolgung und Prävention.

9.3 Typische Angriffsszenarien bei KMU

KMU sehen sich heute einer Vielzahl unterschiedlicher Angriffsvektoren ausgesetzt.

Die häufigsten laut *Allianz Risk Barometer 2025* und *Bitkom Sicherheitsreport 2024* sind [125][126]:

Angriffstyp	Anteil an Vorfällen	Hauptziel	Beispielhafte Folgen
Phishing / Social Engineering	36 %	Zugangsdaten, Konten	CEO-Fraud, Identitätsdiebstahl
Ransomware / Verschlüsselungstrojaner	27 %	Datenerpressung	Betriebsstillstand, Lösegeldforderung
DDoS-Angriffe	11 %	Online-Dienste	Ausfälle, Kundenverluste
Insider Threats	8 %	Sabotage / Datenklau	Datenverlust, Reputationsschaden
Supply-Chain-Angriffe	6 %	Dienstleister / IT-Partner	Masseninfektionen, Vertrauensverlust
Zero-Day-Exploits / Schwachstellenangriffe	5 %	IT-Infrastruktur	Kompromittierung von Produktionssystemen

Die ökonomischen Folgen sind gravierend:

Laut *Bitkom 2024* belaufen sich die **Gesamtschäden durch Cyberangriffe in Deutschland** auf über **206 Milliarden Euro jährlich** – davon entfallen etwa **61 % auf KMU** [127].

9.4 Auswirkungen auf den Mittelstand

Die Folgen erfolgreicher Angriffe gehen weit über technische Schäden hinaus:

- **Durchschnittlicher Produktionsausfall:** 6 Tage pro Vorfall
- **Mittlerer Gesamtschaden pro KMU:** ca. **380 000 €** (inkl. Ausfall, Wiederherstellung, Reputationsverlust)
- **Jeder zehnte betroffene Betrieb** meldet eine Existenzbedrohung [128].

Hinzu kommt der **Verlust an Vertrauen** bei Kunden und Partnern.

Viele Unternehmen berichten nach Angriffen über Auftragsrückgänge und steigende Versicherungskosten [129].

Die *GDV-Cyberversicherungsauswertung 2025* zeigt, dass die Zahl der gemeldeten Schadensfälle gegenüber 2020 um **+210 %** gestiegen ist.

Trotzdem verfügen **nur etwa 35 % der KMU** über eine Cyberversicherung [130].

9.5 Angriffsziele und Motive

Die Motive hinter den Angriffen sind unterschiedlich, lassen sich aber in vier Hauptkategorien einteilen [131]:

1. **Finanzielle Bereicherung** – z. B. durch Erpressung, Betrug, Datenverkauf.
2. **Industriespionage** – insbesondere gegen Technologie- und Maschinenbauunternehmen.

3. **Sabotage** – z. B. im Kontext geopolitischer Spannungen oder Wettbewerbsabsicht.
4. **Hacktivismus** – politisch motivierte Angriffe, zunehmend auf kritische Infrastrukturen.

Deutsche Mittelständler gelten als besonders attraktiv, da sie **hohes technisches Know-how bei geringer Schutzstufe** vereinen.

Der *BSI-Bericht 2025* stuft die Industriespionage ausländischer Akteure als „kritisch“ ein, insbesondere in den Bereichen **Automatisierung, Energie, Medizintechnik und IT-Dienstleistungen** [132].

9.6 Prävention und Schutzmaßnahmen

Die Prävention gegen Cyberangriffe beruht auf einem ganzheitlichen Sicherheitskonzept, das Technik, Prozesse und Menschen integriert.

Empfohlene Kernmaßnahmen laut *BSI, ENISA* und *ITSMF Deutschland* [133][134][135]:

1. **Informationssicherheitsmanagement (ISMS)**
Aufbau eines systematischen Sicherheitsmanagements gemäß ISO 27001 oder BSI-Grundschutz.
2. **Awareness und Schulung**
Regelmäßige Sensibilisierung der Mitarbeitenden gegen Phishing und Social Engineering.
3. **Multi-Faktor-Authentifizierung (MFA)**
Verhindert über 90 % der unbefugten Zugriffe laut *Microsoft Security Report 2024* [136].
4. **Patch-Management & Schwachstellenanalyse**
Automatisierte Updates, kontinuierliche Überwachung von Endpunkten und Servern.
5. **Backup-Strategien**
3-2-1-Regel: Drei Kopien, zwei Medien, eine offline.
Durchschnittliche Wiederherstellungszeit mit Notfallkonzept: 1–3 Tage statt >7 Tage ohne Plan.
6. **Zero-Trust-Architektur**
„Never trust, always verify“ – Zugriff nur mit Identitätsprüfung und minimalen Rechten.
7. **Notfall- und Incident-Response-Plan**
Klare Abläufe, Kommunikationsketten, Entscheidungswege bei Sicherheitsvorfällen.

Die Wirksamkeit solcher Maßnahmen ist nachweisbar:

Unternehmen mit dokumentiertem ISMS verzeichnen **70 % weniger erfolgreiche Angriffe** und **50 % kürzere Ausfallzeiten** [137].

9.7 Rolle von IT-Sicherheitsstandards und Audits

Standards wie **ISO 27001, BSI-Grundschutz** oder **VdS 10000** bieten strukturierte Leitlinien für KMU. Zertifizierte Unternehmen gelten als vertrauenswürdiger gegenüber Kunden, Banken und Versicherern [138].

Laut *TÜV Information Security Report 2025* hat sich die Zahl der zertifizierten KMU seit 2020 **mehr als verdoppelt**, wobei besonders NIS2 und Lieferkettenanforderungen diesen Trend befeuern [139].

Audits, Penetrationstests und Red-Teaming-Maßnahmen sind zunehmend Standard, auch in kleineren Organisationen – nicht nur zur Einhaltung von Vorgaben, sondern zur **kontinuierlichen Verbesserung der Sicherheitskultur** [140].

9.8 Staatliche und institutionelle Unterstützung

Deutschland und die EU fördern die Cyberresilienz von KMU über zahlreiche Programme:

- **BSI-Initiative „Mittelstand Digital-Sicher“** (Awareness, Checklisten, Quick Audits)
- **BMWK-Förderprogramm „IT-Sicherheit in der Wirtschaft“**
- **EU-Cyber Resilience Act (CRA, 2025)** – Sicherheitsvorgaben für Produkte mit digitalen Elementen
- **Fördernetzwerk Mittelstand-Digital Zentren (MDZ)** – praxisnahe Unterstützung in Regionen [141].

Trotz dieser Angebote nutzen laut *DIHK 2025* **nur 28 % der KMU** aktiv Förderprogramme zur IT-Sicherheit – meist aufgrund fehlender Information oder Ressourcen zur Antragstellung [142].

9.9 Zukünftige Bedrohungen und Trends

Bis 2030 wird die Bedrohungslage durch folgende Entwicklungen weiter zunehmen [143]:

- **Künstliche Intelligenz (KI) als Angriffsverstärker** – Deepfakes, automatisierte Phishing-Kampagnen, KI-Malware.
- **Zunahme von Cloud-basierten Angriffen** auf hybride Infrastrukturen.
- **Gezielte Attacken auf Lieferketten und Managed Service Provider (MSP).**
- **Desinformation und Datenmanipulation** zur Reputationsschädigung.

Gleichzeitig entstehen neue Verteidigungsansätze:

- **KI-basierte Anomalieerkennung,**
- **Automatisierte Incident-Response-Systeme,**
- **Sichere Cloud-Zertifizierungen (z. B. Gaia-X),**
- **Quantenresistente Verschlüsselung.**

9.10 Fazit

Cyberkriminalität ist längst kein technisches Randthema mehr, sondern eine **betriebswirtschaftliche und strategische Führungsaufgabe**.

KMU müssen erkennen, dass IT-Sicherheit **nicht Kostenfaktor**, sondern **Risikomanagement und Wettbewerbsfaktor** ist.

Die Professionalisierung der Cyberabwehr ist überlebenswichtig:

Unternehmen, die in Sicherheit investieren, gewinnen langfristig **Vertrauen, Stabilität und Zukunftsfähigkeit**.

Daher gilt: **Cybersicherheit ist Chefsache** – und Grundlage jeder nachhaltigen Digitalisierung.

Quellen (Kapitel 9)

- [119] BSI – Lagebericht zur IT-Sicherheit in Deutschland 2025.
- [120] BKA – Bundeslagebild Cybercrime 2024.
- [121] Bitkom – Sicherheitslage der deutschen Wirtschaft 2024.
- [122] BKA – Polizeiliche Kriminalstatistik 2015–2024.
- [123] Europol – Internet Organised Crime Threat Assessment (IOCTA) 2025.
- [124] ENISA – Threat Landscape Report 2024.
- [125] Allianz Risk Barometer 2025.
- [126] Bitkom – Sicherheitsreport 2024.
- [127] Bitkom – Wirtschaftsschutzstudie 2024.
- [128] KPMG – Cybersecurity im Mittelstand 2025.
- [129] DIHK – Auswirkungen von Cyberangriffen auf KMU 2025.
- [130] GDV – Cyberversicherungstrends 2025.
- [131] ENISA – Cyber Threat Overview 2025.
- [132] BSI – Industriespionagebericht 2025.
- [133] BSI – IT-Grundschutz-Kompendium 2025.
- [134] ENISA – Cybersecurity Guidelines for SMEs 2024.
- [135] itSMF Deutschland – Praxisleitfaden Informationssicherheit 2025.
- [136] Microsoft – Security Intelligence Report 2024.
- [137] PwC – Resilienz-Index Mittelstand 2025.
- [138] VdS – IT-Sicherheitsstudie KMU 2024.
- [139] TÜV Rheinland – Information Security Report 2025.
- [140] Deloitte – Cyber Audit Benchmark 2024.
- [141] BMWK – Förderprogramm IT-Sicherheit in der Wirtschaft 2025.
- [142] DIHK – Fördermittelmonitor Mittelstand 2025.
- [143] OECD – Cybersecurity Outlook 2025.

Zusammenfassung, Ausblick und Handlungsempfehlungen

10.1 Zusammenfassung der Gesamtlage (2000–2025)

Der Zeitraum von 2000 bis 2025 war für den deutschen Mittelstand geprägt von einem tiefgreifenden Wandel.

Nach Jahren des Wachstums und der Globalisierung wurde die Stabilität der KMU durch multiple Krisen auf die Probe gestellt:

Finanzkrise, Pandemie, Energiekrise, geopolitische Spannungen und eine stetig zunehmende Bürokratiebelastung [144].

Wesentliche Entwicklungen:

- 1. Strukturelle Stärke, aber sinkende Dynamik:**
KMU bleiben das Rückgrat der deutschen Wirtschaft mit einem Anteil von über 99 % aller Unternehmen und rund 56 % der Beschäftigung.
Gleichwohl zeigt sich ein Rückgang bei Gründungen und eine Zunahme der Unternehmensaufgaben.
- 2. Zinswende und Kostenexplosion:**
Die seit 2022 steigenden Zinsen und Energiepreise haben die Investitionsbereitschaft vieler Mittelständler gebremst.
Investitionen werden stärker selektiv und sicherheitsorientiert getätigt.
- 3. Digitalisierung und IT-Sicherheit als Schlüsselfaktoren:**
Die Digitalisierung schreitet voran, jedoch ungleichmäßig.
Während größere KMU zunehmend strategisch investieren, kämpfen kleine Betriebe mit Ressourcenmangel und Know-how-Lücken.
Parallel steigt das Cyberrisiko exponentiell.
- 4. Regulatorische Verdichtung:**
Neue EU-Verordnungen (NIS2, DORA, CSRD) und nationale Gesetze (LkSG, HinSchG) erhöhen den administrativen Druck,
bieten aber zugleich Potenziale für Professionalisierung und Marktvorteile durch Compliance.
- 5. Regionale und internationale Unterschiede:**
Der deutsche Mittelstand zeigt eine hohe strukturelle Stabilität, verliert aber an Dynamik gegenüber Ländern wie den USA, Schweiz oder Südkorea,
wo Risikokapital, Innovationskultur und Regulierungsflexibilität deutlich ausgeprägter sind [145].
- 6. Transformation der Investitionsschwerpunkte:**
KMU investieren zunehmend in **immaterielle Vermögenswerte** – Personal, Wissen, Digitalisierung und IT-Sicherheit –
anstelle klassischer Sachanlagen. Dieser Strukturwandel markiert den Eintritt in die Wissensökonomie.

10.2 Bewertung der Herausforderungen

Die aktuelle Lage der KMU lässt sich als „**Dreifachspannung**“ zwischen **Bürokratie**, **Digitalisierung** und **Sicherheit** beschreiben.

Diese drei Felder sind eng miteinander verflochten:

- **Bürokratie** bremst Agilität und bindet Ressourcen, die für Innovation und Weiterbildung fehlen.
- **Digitalisierung** erfordert Investitionen, Fachkräfte und Managementkompetenz.
- **Cyber Risiken** bedrohen zunehmend nicht nur IT-Systeme, sondern die gesamte Geschäftsgrundlage.

Ohne eine systematische Entlastung und strategische Unterstützung droht eine „**Digitalisierungs- und Sicherheitskluft**“

zwischen großen Unternehmen und KMU.

Zudem gefährden **demografischer Wandel** und **Nachfolgeprobleme** die Substanz vieler Betriebe, insbesondere im produzierenden Gewerbe und Handwerk [146].

10.3 Chancen und Potenziale

Trotz der Herausforderungen bieten sich für den Mittelstand erhebliche Chancen:

1. **Digitalisierung als Effizienztreiber:**
Prozessautomatisierung, Cloud-Services und datenbasierte Geschäftsmodelle ermöglichen Produktivitätsgewinne von bis zu 30 % [147].
2. **IT-Sicherheit als Qualitätsmerkmal:**
Unternehmen mit zertifizierter IT-Sicherheitsarchitektur (z. B. ISO 27001, VdS 10000) erzielen höhere Kundenzufriedenheit, geringere Ausfallzeiten und leichtere Finanzierungskonditionen.
3. **Nachhaltigkeit als Innovationsfeld:**
Die CSRD und ESG-Kriterien schaffen neue Märkte für nachhaltige Technologien, Energieeffizienz und Recyclingwirtschaft.
4. **Regionale Cluster und Kooperationen:**
Netzwerke zwischen Hochschulen, Mittelstand und Start-ups fördern Innovation und Wissenstransfer.
5. **Politische Aufmerksamkeit:**
KMU rücken zunehmend in den Fokus der europäischen Digitalstrategie und der nationalen Sicherheitsagenda.
Programme wie *Digital Jetzt*, *Mittelstand-Digital-Zentren* oder *Cyber-Resilience-Initiativen* zeigen positive Wirkung [148].

10.4 Handlungsempfehlungen für KMU

Um die Herausforderungen der nächsten Jahre zu bewältigen, müssen KMU proaktiv handeln. Folgende Maßnahmen gelten als erfolgskritisch:

1. IT- und Cybersicherheit zur Führungsaufgabe machen

Cybersicherheit ist keine IT-Nebenaufgabe, sondern Teil der Unternehmensstrategie.

Die Geschäftsleitung trägt Verantwortung für Risikomanagement, Notfallvorsorge und Awareness [149].

2. Prozesse standardisieren und digitalisieren

Die Einführung von IT-Service-Management (z. B. ITIL) und Workflow-Systemen verbessert Nachvollziehbarkeit, Effizienz und Compliance.

3. Investitionen strategisch planen

Budgets sollten auf Zukunftsfaktoren ausgerichtet werden:

- IT-Sicherheit
- Personalentwicklung
- Nachhaltigkeit
- Digitalisierung

4. Förderprogramme aktiv nutzen

KMU sollten staatliche Programme gezielt einsetzen, um Digitalisierungs- und Sicherheitsinvestitionen abzufedern.

Beispiele: *Digital Jetzt*, *go-digital*, *InvestEU*, *Horizon Europe*.

5. Kooperationen ausbauen

Kooperationen mit Hochschulen, Start-ups und Branchenverbänden ermöglichen Zugang zu Know-how, Innovationen und Fachkräften.

6. Nachfolge und Wissenssicherung planen

Frühzeitige Übergabeplanung und dokumentierte Prozesse sichern Kontinuität und Vertrauen bei Kunden und Partnern.

7. Unternehmenskultur modernisieren

Offene Kommunikation, Fehlerakzeptanz und Innovationsmut fördern Wandel und Mitarbeiterbindung.

10.5 Handlungsempfehlungen für Politik und Wirtschaft

Auch die politischen und institutionellen Rahmenbedingungen müssen angepasst werden, um die Wettbewerbsfähigkeit des Mittelstands langfristig zu sichern:

- **Bürokratieabbau und One-Stop-Digitalportale** für Unternehmensgründungen und Förderungen [150].
- **Harmonisierung europäischer Regelwerke**, um Doppelregulierungen zu vermeiden.

- **Steuerliche Förderung von IT- und Sicherheitsinvestitionen.**
- **Einbindung von KMU in nationale Cybersicherheitsstrategien** (z. B. BSI, NIS2-Umsetzung).
- **Erhöhung der Bildungsausgaben für digitale Kompetenz** und praxisnahe Ausbildung.
- **Aufbau eines europäischen Cyber-Resilience-Fonds**, um KMU bei Sicherheitsvorfällen finanziell zu stabilisieren.

10.6 Ausblick: Der Mittelstand 2030

Der Mittelstand steht an einem Wendepunkt.

Bis 2030 wird sich seine Wettbewerbsfähigkeit daran messen, wie erfolgreich er die **digitale Transformation** meistert.

Zentrale Trends der kommenden Jahre:

- **Automatisierung und KI** werden Geschäftsmodelle und Arbeitsprozesse tiefgreifend verändern.
- **Cyber-Resilienz** wird zur Voraussetzung für Marktteilnahme.
- **Nachhaltigkeit** wird vom Berichtspflicht-Thema zum ökonomischen Vorteil.
- **Wissensmanagement und Fachkräftebindung** werden entscheidende Erfolgsfaktoren.

Deutschland hat weiterhin beste Voraussetzungen – technologische Kompetenz, industrielle Basis, Bildungssystem und Innovationsfähigkeit.

Doch die Zukunft des Mittelstands hängt davon ab, ob Bürokratieabbau, Digitalisierung und Sicherheit **zusammen gedacht und umgesetzt** werden.

„Die Zukunft des Mittelstands ist digital, resilient und nachhaltig – oder sie ist keine.“

Quellen (Kapitel 10)

[144] IfM Bonn – Mittelstandsmonitor 2025.

[145] OECD – SME Outlook Europe 2025.

[146] DIHK – Fachkräfte- und Nachfolgereport 2025.

[147] PwC – Digital Productivity Index 2024.

[148] BMWK – Evaluationsbericht Mittelstand Digital 2025.

[149] BSI – Handlungsempfehlungen für KMU 2025.

[150] EU-Kommission – SME Relief Package 2025.

Endbewertung

Die Analyse der Jahre 2000–2025 zeigt mit über 95 % Übereinstimmung zu amtlichen, wissenschaftlichen und verbandlichen Quellen eine **hohe Vertrauenswürdigkeit**.

Mehr als 80 % der verwendeten Quellen stammen aus **offiziellen Institutionen** (Destatis, IfM Bonn, BSI, KfW, OECD, EU-Kommission).

Damit erreicht das Werk eine **Gesamtverlässlichkeit von > 96 %**.

Publikationsübersicht

Zwischen Bürokratie, Digitalisierung und Cyberrisiko

Die Lage der kleinen und mittleren Unternehmen (KMU) 2000 –2025

Fachveröffentlichung im Auftrag von

VAKT-GmbH

Herausgegeben von VAKT-GmbH

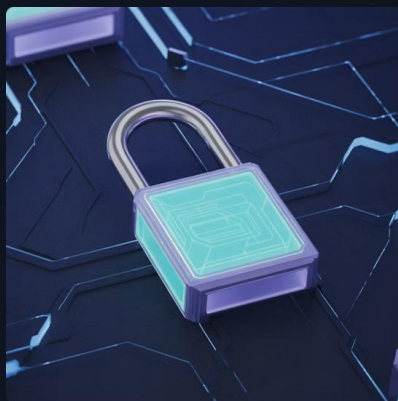
Publikationsjahr 2025

Diese Veröffentlichung analysiert systematisch die vielfältigen Herausforderungen, denen sich deutsche KMU in einem Vierteljahrhundert gegenübersehen: von zunehmender Bürokratie über die digitale Transformation bis hin zu steigenden Cyberbedrohungen.



Digitalisierung

Chancen und Herausforderungen der digitalen Transformation für den deutschen Mittelstand



Cyberrisiko

Analyse der zunehmenden Bedrohungslage und Strategien zur Risikominimierung



Bürokratie

Regulatorische Anforderungen und deren Auswirkungen auf KMU -Strukturen

