WHITE PAPER

Moderner IT-Support im deutschen Mittelstand

Anforderungen, Modelle und Best Practices für eine zukunftsfähige IT-Betreuung

2026 - CETOS Services AG

81%
der Unternehmen von Cyberangriffen betroffen

267 Mrd.
Euro Gesamtschaden Cyberkriminalität DE 2024

1. Executive Summary

Der deutsche Mittelstand – Unternehmen mit 50 bis 500 Mitarbeitenden – ist das Rückgrat der deutschen Volkswirtschaft. Er steht jedoch vor einem strukturellen Paradox: Der Bedarf an professioneller IT-Betreuung wächst kontinuierlich, während die Möglichkeiten, qualifiziertes IT-Personal zu gewinnen und zu halten, deutlich abnehmen. Gleichzeitig steigen die Anforderungen an Verfügbarkeit, Sicherheit und Compliance der IT-Infrastruktur.

Dieses White Paper analysiert, was modernen IT-Support im Mittelstand auszeichnet, welche Leistungsmodelle sich in der Praxis bewährt haben und wie Unternehmen ihren IT-Betrieb strategisch aufstellen können. Die Darstellung stützt sich auf aktuelle Studien und Lageberichte des Bundesamts für Sicherheit in der Informationstechnik (BSI), des Digitalverbands Bitkom sowie des Marktforschungsunternehmens Lünendonk & Hossenfelder.

> *Professioneller IT-Support ist im Mittelstand kein Luxus, sondern eine betriebswirtschaftliche Notwendigkeit. Unternehmen, die IT-Betrieb und -Support strukturiert und proaktiv organisieren, erzielen nachweislich höhere Verfügbarkeit, geringere Ausfallkosten und eine bessere Ausgangslage gegenüber regulatorischen Anforderungen.*

2. Ausgangslage: IT im deutschen Mittelstand 2025

2.1 Wachsende Komplexität, begrenzte Ressourcen

Die Digitalisierung hat die IT mittelständischer Unternehmen grundlegend verändert. Was vor zehn Jahren ein lokales Netzwerk mit einigen Arbeitsplätzen war, ist heute eine hybride Infrastruktur aus On-Premises-Systemen, Cloud-Diensten, mobilen Endgeräten und einer Vielzahl von Softwareanwendungen. Eine IDC-Studie (International Data Corporation) im Auftrag von Atos SE (2024) zeigt, dass der Reifegrad der digitalen Infrastruktur im deutschen Mittelstand erheblich variiert: Während sogenannte „Digitale Champions“ 33 Prozent ihres IT-Budgets für neue Projekte einsetzen, hinken kleinere Unternehmen in puncto Cloud-Nutzung, Sicherheit und Automatisierung deutlich hinterher.

Gleichzeitig haben sich die Anforderungen an IT-Sicherheit, Datenschutz und regulatorische Compliance massiv erhöht. Die NIS-2-Richtlinie (Network and Information Security Directive 2), die DSGVO (Datenschutz-Grundverordnung) und branchenspezifische Regularien verlangen von Unternehmen ein deutlich höheres Maß an Dokumentation, Sicherheitsmaßnahmen und Incident-Management, als es vor wenigen Jahren noch der Fall war.

2.2 Der IT-Fachkräftemangel als systemisches Problem

Parallel zur steigenden Komplexität verschlimmert sich der IT-Fachkräftemangel. Laut Bitkom (2025) fehlen in deutschen Unternehmen derzeit rund 109.000 IT-Fachkräfte. IT-Stellen bleiben im Schnitt 7,7 Monate unbesetzt (Bitkom 2023), und 79 Prozent der Unternehmen erwarten eine weitere Verschlechterung der Lage. Das hat direkte Auswirkungen auf den IT-Betrieb im Mittelstand: Vorhandene IT-Mitarbeitende werden überlastet, die Abhängigkeit von einzelnen Schlüsselpersonen steigt, und strategische IT-Projekte werden zugunsten des Tagesgeschäfts zurückgestellt.

109.000	**7,7 Mon.**	**79 %**
fehlende IT-Fachkräfte in Deutschland (Bitkom: In Deutschland fehlen weiterhin mehr als 100.000 IT-Fachkräfte, August 2025)	*durchschn. Vakanzzeit offener IT-Stellen (Bitkom: Rekord-Fachkräftemangel – 149.000 IT-Jobs unbesetzt, Dezember 2023)*	*erwarten weitere Verschlechterung (Bitkom: In Deutschland fehlen weiterhin mehr als 100.000 IT-Fachkräfte, August 2025)*

Das sogenannte Key-Person-Risk – der Ausfall einer einzigen zentralen IT-Person durch Krankheit, Urlaub oder Kündigung – ist im Mittelstand besonders ausgeprägt. In Unternehmen mit einer oder zwei IT-Personen kann ein solcher Ausfall den gesamten IT-Betrieb lähmen. Dieses strukturelle Risiko ist einer der wichtigsten Treiber für die wachsende Nachfrage nach externen IT-Support-Modellen.

2.3 Marktentwicklung: Wachsende Nachfrage nach IT-Dienstleistungen

Der Markt für IT-Dienstleistungen in Deutschland wächst trotz konjunktureller Herausforderungen. Laut Lünendonk-Studie 2025 erzielten führende IT-Service-Unternehmen 2024 ein Umsatzwachstum von 4,8 Prozent – getrieben insbesondere durch Nachfrage nach IT-Modernisierung und Investitionen in die Absicherung von Unternehmensnetzwerken. Für 2025 und 2026 rechnen IT-Dienstleister mit deutlich höheren Wachstumsraten, insbesondere in den Bereichen Managed Services (+9,8 %), Cyber Security (+11,4 %) und Cloud-Transformation (+13,5 %).

Diese Entwicklung spiegelt einen grundlegenden Wandel im Mittelstand wider: IT-Support wird zunehmend nicht mehr als internes Kostenzentrum, sondern als strategisch ausgelagerter Dienstleistungsbestandteil begriffen.

3. Was modernen IT-Support ausmacht

Moderner IT-Support im Mittelstand unterscheidet sich grundlegend vom klassischen „Break-Fix“-Modell, im Volksmund auch „Feuerwehr-Tarif“ genannt, bei dem ein Dienstleister erst dann gerufen wird, wenn etwas nicht mehr funktioniert. Er ist proaktiv, strukturiert und ganzheitlich – und umfasst weit mehr als die Behebung von Störungen.

3.1 Proaktiv statt reaktiv: Das Paradigma des modernen IT-Betriebs

Der entscheidende Unterschied zwischen modernem und traditionellem IT-Support liegt im Zeitpunkt der Reaktion. Reaktiver Support wartet auf Probleme. Proaktiver Support überwacht Systeme kontinuierlich, identifiziert Anomalien frühzeitig und ergreift Maßnahmen, bevor es zu Ausfällen kommt.

Technologische Grundlage des proaktiven Ansatzes ist das Remote Monitoring & Management (RMM). Professionelle Monitoring-Lösungen wie Paessler PRTG, N-able N-central oder Auvik erfassen kontinuierlich den Zustand von Servern, Netzwerkkomponenten, Speichersystemen und Sicherheitslösungen. Automatische Alerts bei definierten Schwellenwerten ermöglichen es IT-Teams, zeitnah zu reagieren; häufig, noch bevor Mitarbeitende des Kundenunternehmens ein Problem bemerken.

> *Praxishinweis: Ein IT-Ausfall kostet mittelständische Unternehmen nach Einschätzung von Branchenexperten im Durchschnitt mehrere tausend Euro pro Stunde – durch Produktivitätsverlust, Kundenkommunikation und Wiederherstellungsaufwand. Proaktives Monitoring amortisiert sich in der Regel bereits durch die Verhinderung eines einzigen ungeplanten Ausfalls.*

3.2 Service Level Agreements: Verbindlichkeit als Qualitätsmerkmal

Ein wesentliches Merkmal professionellen IT-Supports sind klar definierte und verbindlich vereinbarte Service Level Agreements (SLAs). SLAs regeln Reaktionszeiten (Zeit bis zur ersten Reaktion auf eine Anfrage), Lösungszeiten (Zeit bis zur vollständigen Behebung), Verfügbarkeiten, Eskalationspfade und Kommunikationspflichten.

Für mittelständische Unternehmen sind SLAs aus zwei Gründen wichtig: Erstens schaffen sie Planungssicherheit und klare Erwartungshaltungen auf beiden Seiten. Zweitens machen sie IT-Support messbar und damit steuerbar. Ein IT-Dienstleister ohne SLAs ist kein Partner – er ist ein Dienstleister auf Abruf.

Branchenstandards unterscheiden typischerweise zwischen verschiedenen Prioritätsstufen: Kritische Ausfälle (P1) erfordern Reaktionszeiten im Bereich von Minuten, Standardanfragen (P3) können innerhalb eines Arbeitstages bearbeitet werden. Die genaue Ausgestaltung hängt von den Anforderungen des jeweiligen Unternehmens ab.

3.3 Festpreismodelle: Planbarkeit als Wettbewerbsvorteil

Ein zentrales Merkmal moderner IT-Support-Modelle ist die Abkehr von der Stundenabrechnung hin zu monatlichen Festpreisen. Managed-Service-Verträge mit Pauschalen pro Arbeitsplatz oder pro System machen IT-Kosten kalkulierbar und eliminieren das Risiko unerwarteter Ausgaben.

Marktdaten zeigen, dass professionelle Managed Services für KMU in Deutschland bei 30 bis 80 Euro pro Arbeitsplatz und Monat liegen – je nach Leistungsumfang und Unternehmensgröße. Im Vergleich zu den Gesamtkosten eines eigenen IT-Mitarbeiters (Gehalt, Sozialabgaben, Weiterbildung, Urlaubs- und Krankheitsvertretung) von 60.000 bis 80.000 Euro jährlich stellt dies für viele mittelständische Unternehmen die wirtschaftlichere Option dar.

Darüber hinaus hat das Festpreismodell einen strukturellen Vorteil: Der Dienstleister hat ein innewohnendes Interesse daran, Probleme zu verhindern, statt von ihnen zu profitieren. Proaktiver Betrieb ist bei Festpreisen für beide Seiten vorteilhafter als reaktive Schadensbeseitigung.

3.4 Ganzheitlicher Ansatz: Die Leistungsbausteine im Überblick

Moderner IT-Support ist kein punktuelles Angebot, sondern ein strukturierter Leistungsverbund. Die wichtigsten Bausteine umfassen den folgenden Umfang.

Beim Remote-Support werden Anfragen von Mitarbeitenden zeitnah per Fernwartung bearbeitet, ohne Wartezeit auf einen Vor-Ort-Termin. Der Vor-Ort-Service ergänzt den Remote-Support bei physischen Aufgaben wie Hardwareinstallation, Verkabelung oder gerätespezifischen Problemen. Proaktives Monitoring überwacht Server, Netzwerk, Speicher und Sicherheitslösungen kontinuierlich. Regelmäßige Wartungen umfassen Software-Updates, Log-Analysen, Festplattenprüfungen und Systemoptimierungen. Das Backup-Management implementiert und überwacht Datensicherungsstrategien und führt regelmäßige Recovery-Tests durch. IT-Security-Maßnahmen beinhalten Virenschutz, Firewall-Management und Netzwerksicherheit. Die Benutzer- und

Rechteverwaltung verwaltet Konten, Zugriffsrechte und On-/Offboarding-Prozesse. IT-Beratung und Beschaffungsmanagement unterstützt bei Hardware-Entscheidungen und der strategischen Weiterentwicklung der IT-Infrastruktur.

In der Praxis deckt ein einzelner IT-Dienstleister nicht immer alle Bereiche mit gleicher Tiefe ab – bei hochspezialisierten Anforderungen wie Penetrationstests, Security-Audits oder Security-Awareness-Schulungen arbeiten MSP häufig mit zertifizierten Spezialpartnern zusammen. Entscheidend ist, dass Koordination und Verantwortung dabei klar geregelt sind.

4. Backup, Recovery und IT-Security: Pflichtbausteine des modernen IT-Betriebs

4.1 Datensicherung nach dem 3-2-1-Prinzip

Datenverlust durch Ransomware, Hardware-Ausfall oder menschliches Versagen zählt zu den folgenreichsten IT-Risiken für mittelständische Unternehmen. Das BSI empfiehlt als Goldstandard der Datensicherung die 3-2-1-Strategie: drei Kopien der Daten, auf zwei verschiedenen Medien, davon eine Kopie außerhalb des Unternehmens (offsite oder Cloud).

Moderne Backup-Lösungen kombinieren lokale NAS-Systeme (Network Attached Storage) mit Cloud-Sicherungen, um sowohl schnelle Wiederherstellungszeiten (Recovery Time Objective, RTO) als auch Offsite-Sicherheit zu gewährleisten. Entscheidend ist dabei nicht nur das Vorhandensein eines Backup-Systems, sondern seine regelmäßige Überprüfung: Ein Backup, das im Ernstfall nicht funktioniert, ist kein echtes Backup. Das BSI-Grundschutz-Kompendium empfiehlt regelmäßige Recovery-Tests als verpflichtenden Bestandteil jedes Backup-Konzepts.

> *Praxishinweis: Recovery-Tests sollten mindestens quartalsweise durchgeführt und dokumentiert werden. Erst der erfolgreiche Test einer vollständigen Wiederherstellung beweist, dass ein Backup-System im Ernstfall tatsächlich funktioniert. Viele Unternehmen stellen im Schadensfall fest, dass ihre Backup-Lösung fehlerhaft konfiguriert war – zu spät.*

4.2 IT-Security als integraler Bestandteil des IT-Supports

IT-Sicherheit ist längst kein eigenständiges Thema mehr, das separat vom IT-Betrieb betrachtet werden kann. Sie ist integraler Bestandteil professionellen IT-Supports. Das BSI-Grundschutz-Kompendium definiert über 100 Bausteine für eine systematische Informationssicherheit, die von Server-Härtung und Patch-Management über Netzwerksegmentierung bis hin zu Zugriffskontrolle und Notfallmanagement reichen.

Für mittelständische Unternehmen sind dabei folgende Maßnahmen besonders relevant: professioneller Endpoint-Schutz (Virenschutz) mit regelmäßiger Überprüfung der Reports auf Auffälligkeiten, Hardware-Firewalls zum Schutz des Netzwerkperimeters, Netzwerksegmentierung zur Begrenzung der Ausbreitung im Schadensfall, Multi-Faktor-Authentifizierung (MFA) für alle externen Zugänge sowie regelmäßiges Patch-Management für alle eingesetzten Systeme.

Laut BSI-Lagebericht 2025 (Berichtszeitraum Juli 2024 bis Juni 2025) wurden täglich durchschnittlich 119 neue Schwachstellen in IT-Systemen bekannt – ein Anstieg von rund 24 Prozent gegenüber dem Vorjahreszeitraum. Ransomware und Phishing-Kampagnen zählen zu den häufigsten Angriffsvektoren. Besonders alarmierend: Kleine und mittlere Unternehmen (KMU) werden zunehmend nicht gezielt,

sondern als Teil automatisierter Kampagnen getroffen – was sie zu einem ebenso attraktiven Ziel macht wie Großunternehmen.

119	81%	267 Mrd.
neue Schwachstellen täglich, +24 % ggü. Vorjahr (BSI: Die Lage der IT-Sicherheit in Deutschland 2025, Berichtszeitraum Juli 2024–Juni 2025)	*Der deutschen Unternehmen von Cyberangriffen betroffen (Bitkom: Wirtschaftsschutz 2024, Berlin August 2024)*	*Euro Gesamtschaden Cyberkriminalität DE 2024 (Bitkom: Wirtschaftsschutz 2024, Berlin August 2024*

5. Organisationsmodelle für den IT-Support im Mittelstand

Die Frage nach dem optimalen Organisationsmodell für den IT-Support ist eine der zentralen strategischen IT-Entscheidungen mittelständischer Unternehmen. In der Praxis lassen sich drei Grundmodelle unterscheiden, die in der Realität häufig als Hybride auftreten.

5.1 Inhouse-IT

Beim Inhouse-Modell werden alle IT-Aufgaben durch eigene Mitarbeitende wahrgenommen. Dieses Modell bietet maximale Kontrolle, tiefes Unternehmenswissen und kurze Kommunikationswege. Es eignet sich besonders für Unternehmen mit spezifischen IT-Anforderungen, sensiblen Daten oder einer Unternehmenskultur, die Kontrolle und Autonomie priorisiert.

Jedoch hat das Inhouse-Modell systemische Schwächen: Es ist abhängig vom verfügbaren Personalmarkt, unterliegt dem Key-Person-Risk, lässt sich bei schnellem Wachstum nur langsam skalieren und erfordert kontinuierliche Weiterbildungsinvestitionen, um mit dem technologischen Wandel Schritt zu halten.

5.2 Managed Services: Vollständige Auslagerung

Beim Managed-Service-Modell übernimmt ein externer Dienstleister (Managed Service Provider, MSP) den laufenden Betrieb der IT-Infrastruktur auf Basis definierter SLAs und monatlicher Festpreise. Der wesentliche Unterschied zum klassischen IT-Outsourcing liegt im proaktiven Ansatz: Während beim klassischen Outsourcing häufig reaktiv auf gemeldete Probleme reagiert wird, verpflichten sich Managed Service Provider vertraglich zu proaktivem Betrieb – mit kontinuierlichem Monitoring, definierten SLAs und regelmäßiger Wartung als Kern des Leistungsmodells.

Das Managed-Service-Modell bietet mittelständischen Unternehmen mehrere strukturelle Vorteile: planbare Kosten durch Festpreise, Zugang zu einem Team von Spezialisten statt einer einzelnen Person, Skalierbarkeit bei Wachstum oder Veränderungen, 24/7-Monitoring-Fähigkeiten, die intern kaum realisierbar wären, sowie die Eliminierung des Key-Person-Risks.

> *Zum Vergleich: Ein eigener IT-Mitarbeiter kostet inklusive Sozialabgaben, Weiterbildung und Vertretungskosten 60.000 bis 80.000 Euro jährlich – für eine einzelne Person mit begrenztem Kompetenzspektrum. Managed Services für 50 Arbeitsplätze kosten bei 30 bis 80 Euro pro Arbeitsplatz 1.500 bis 4.000 Euro monatlich – für ein ganzes Team mit breiter Expertise (Quelle: Lünendonk: Der Markt für IT-Dienstleistungen in Deutschland 2025, Mindelheim 2025).*

5.3 Co-Managed IT: Das Hybridmodell

Das Co-Managed-Modell kombiniert interne IT-Kompetenz mit externem Support. Interne IT-Mitarbeitende behalten die strategische Steuerung und das Unternehmenswissen, während ein MSP operative Aufgaben übernimmt: Monitoring, Wartung, Second-Level-Support, Spezialthemen wie Security oder Cloud-Migration.

Dieses Modell hat sich insbesondere für Unternehmen mit 100 bis 500 Mitarbeitenden bewährt, die eine eigene IT-Abteilung haben, aber deren Kapazitäten und Kompetenzen nicht für alle Anforderungen ausreichen. Es erlaubt eine flexible Arbeitsteilung und skaliert gut mit dem Unternehmenswachstum.

Bereich	Maßnahme	Priorität
Inhouse-IT	Maximale Kontrolle, tiefes Unternehmenswissen	**Risiko: Key-Person**
Managed Services	Planbare Kosten, breite Expertise, skalierbar	**Empfohlen ab 20 MA**
Co-Managed IT	Kombination interner und externer Kompetenz	**Empfohlen ab 100 MA**

Quelle: Brancheneinschätzungen auf Basis von Bitkom: IT-Mittelstandsbericht 2024 (Berlin 2024), Lünendonk: Der Markt für IT-Dienstleistungen in Deutschland 2025 (Mindelheim 2025) sowie Praxiserfahrungen von IT-Dienstleistern.

6. Regulatorischer Rahmen und Standards

6.1 BSI IT-Grundschutz: Praxisleitfaden für den Mittelstand

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt mit dem IT-Grundschutz-Kompendium ein umfassendes Werkzeug zur systematischen Informationssicherheit bereit. Das Kompendium umfasst über 100 Bausteine in zehn Schichten – von Informationssicherheitsmanagement über Server- und Netzwerksicherheit bis hin zu Notfallmanagement und Datenschutz.

Für mittelständische Unternehmen empfiehlt das BSI die sogenannte Basis-Absicherung als praxisnahen Einstieg: Sie fokussiert sich auf grundlegende Sicherheitsmaßnahmen wie Firewall-Konfiguration, Backup-Einrichtung und -Tests, automatisierte Updates, Zugriffsrechtsbeschränkungen und die Aktivierung von Multi-Faktor-Authentifizierung. Die vollständige BSI-Grundschutz-Zertifizierung ist für KMU in den meisten Fällen weder erforderlich noch wirtschaftlich sinnvoll – die Orientierung an den Grundschutz-Empfehlungen jedoch schon.

6.2 NIS-2-Richtlinie: Erweiterter Pflichtkreis

Die europäische NIS-2-Richtlinie erweitert den Kreis der Unternehmen, die konkrete IT-Sicherheitsmaßnahmen verbindlich umsetzen müssen, erheblich. Neben großen Unternehmen sind nun auch mittelständische Unternehmen in sogenannten „wichtigen“ und „besonders wichtigen“ Einrichtungen erfasst. Die Geschäftsführung haftet persönlich für die Umsetzung der geforderten Sicherheitsmaßnahmen.

Kernpflichten nach NIS-2 umfassen: Risikomanagement, Meldepflichten bei Sicherheitsvorfällen innerhalb von 24 Stunden, Maßnahmen zur Lieferkettensicherheit sowie den Nachweis implementierter Sicherheitsprozesse. Für Unternehmen, die ihre IT-Betreuung an einen MSP auslagern, ist die vertragliche Regelung von Verantwortlichkeiten, Datenschutz und Exit-Szenarien damit nicht nur empfehlenswert, sondern rechtlich notwendig.

7. Best Practices: Maßnahmen für einen zukunftssicheren IT-Betrieb

Die folgenden Maßnahmen basieren auf den Empfehlungen des BSI IT-Grundschutzes, Praxiserfahrungen führender IT-Dienstleister sowie den Erkenntnissen aus Bitkom- und Lünendonk-Studien. Sie sind nach Priorität sortiert und bilden einen strukturierten Fahrplan für die Professionalisierung des IT-Supports.

Bereich	Maßnahme	Priorität
Monitoring	Proaktives System-Monitoring mit automatischen Alerts einrichten	**Hoch**
Backup	3-2-1-Backup-Strategie implementieren, quartalsweise Recovery-Tests	**Hoch**
IT-Security	Professionellen Endpoint-Schutz und Hardware-Firewall einsetzen	**Hoch**
Authentifizierung	Multi-Faktor-Authentifizierung für alle externen Zugänge aktivieren	**Hoch**
SLAs	Verbindliche Reaktions- und Lösungszeiten vertraglich regeln	**Hoch**
Patch-Management	Automatisiertes Patch-Management für alle Systeme implementieren	**Hoch**
Zugriffsrechte	Least-Privilege-Prinzip umsetzen, Accounts regelmäßig überprüfen	**Mittel**
Dokumentation	IT-Systemlandschaft vollständig dokumentieren und aktuell halten	**Mittel**
Server-Wartung	Regelmäßige Serverwartungen: Updates, Logs, Speicherüberprüfung	**Mittel**
NIS-2	NIS-2-Betroffenheit prüfen und ggf. Maßnahmenplan aufsetzen	**Mittel**
Notfallplan	Business Continuity Plan (BCP) und IT-Notfallplan erstellen und üben	**Empfohlen**
IT-Reviews	Regelmäßige strategische IT-Reviews mit dem IT-Partner	**Empfohlen**

Prioritätseinstufung basiert auf BSI IT-Grundschutz Basis-Absicherung (BSI: IT-Grundschutz-Kompendium, www.bsi.bund.de/grundschutz) und Bitkom: Wirtschaftsschutz 2024, Berlin August 2024.

8. Handlungsempfehlungen

Der erste Schritt zu einem professionellen IT-Betrieb ist eine strukturierte Bestandsaufnahme. Eine IT-Analyse inventarisiert alle Systeme, Daten und Prozesse, identifiziert Schwachstellen und Risiken und priorisiert Handlungsbedarfe nach einem Kosten-Nutzen-Verhältnis. Das BSI bietet mit dem Cyber-Risiko-Check (basierend auf DIN SPEC 27076) ein niedrigschwelliges Instrument für KMU an, um einen ersten Überblick über die eigene Sicherheitslage zu gewinnen.

Die Ergebnisse der Analyse bilden die Grundlage für die Wahl des geeigneten IT-Support-Modells und die Priorisierung von Maßnahmen. Wichtig ist, dass die Analyse nicht einmalig bleibt: Der IT-Betrieb muss regelmäßig – mindestens jährlich oder nach wesentlichen Veränderungen – überprü ft und aktualisiert werden.

8.1 IT-Ist-Analyse als Ausgangspunkt

Der erste Schritt zu einem professionellen IT-Betrieb ist eine strukturierte Bestandsaufnahme. Eine IT-Analyse inventarisiert alle Systeme, Daten und Prozesse, identifiziert Schwachstellen und Risiken und priorisiert Handlungsbedarfe nach einem Kosten-Nutzen-Verhältnis. Das BSI bietet mit dem Cyber-Risiko-Check (basierend auf DIN SPEC 27076) ein niedrigschwelliges Instrument für KMU an, um einen ersten Überblick über die eigene Sicherheitslage zu gewinnen.

Die Ergebnisse der Analyse bilden die Grundlage für die Wahl des geeigneten IT-Support-Modells und die Priorisierung von Maßnahmen. Wichtig ist, dass die Analyse nicht einmalig bleibt: Der IT-Betrieb muss regelmäßig – mindestens jährlich oder nach wesentlichen Veränderungen – überprü ft und aktualisiert werden.

8.2 Auswahl eines geeigneten IT-Partners

Die Auswahl eines geeigneten Managed Service Providers ist eine der wichtigsten strategischen Entscheidungen im IT-Bereich. Kriterien für die Auswahl sollten Folgendes umfassen: nachgewiesene Erfahrung im Mittelstandsumfeld, klare und verbindliche SLAs, transparente Festpreismodelle, lokale Präsenz für Vor-Ort-Einsätze, zertifizierte Partnerschaften mit relevanten Herstellern (Microsoft, Security-Anbieter, Storage-Lösungen) sowie klare Regelungen zu Datenschutz, Auftragsverarbeitung (AVV) und Exit-Szenarien.

Besondere Vorsicht ist bei Anbietern geboten, die keine klaren SLAs definieren möchten oder deren Verträge keine Exit-Klauseln enthalten. Daten und Systemkonfigurationen müssen beim Anbieterwechsel vollständig und reibungslos übertragen werden können.

8.3 IT als strategischen Faktor verankern

Moderner IT-Support geht über die operative Ebene hinaus. Unternehmen, die IT als strategischen Erfolgsfaktor begreifen, binden ihren IT-Partner in strategische Überlegungen ein: Wachstumspläne, neue Geschäftsfelder, Digitalisierungsvorhaben und regulatorische Veränderungen haben direkte IT-Implikationen, die frühzeitig berücksichtigt werden müssen.

Regelmäßige IT-Reviews – mindestens einmal im Jahr – schaffen die Grundlage für eine langfristig stabile und skalierbare IT-Infrastruktur. Sie sind keine Kostenpositionen, sondern Investitionen in die betriebliche Resilienz.

9. Fazit

Moderner IT-Support im deutschen Mittelstand ist proaktiv, strukturiert, messbar und strategisch verankert. Er geht weit über die Behebung von Störungen hinaus und umfasst Monitoring, Backup, Security, Compliance und strategische Beratung als zusammenhängendes Leistungspaket.

Die Zahlen sprechen eine klare Sprache: Der IT-Fachkräftemangel wird sich in den nächsten Jahren nicht entspannen, die regulatorischen Anforderungen steigen, und die Bedrohungslandschaft wird

komplexer. Unternehmen, die ihren IT-Betrieb heute strukturieren, profitieren morgen von höherer Verfügbarkeit, geringeren Ausfallkosten und einer besseren Ausgangslage gegenüber regulatorischen Anforderungen.

Die drei wichtigsten Sofortmaßnahmen für mittelständische Unternehmen sind: erstens die Durchführung einer strukturierten IT-Analyse als Bestandsaufnahme, zweitens die Implementierung proaktiven Monitorings und eines getesteten Backup-Konzepts sowie drittens die vertragliche Verankerung klarer SLAs und Verantwortlichkeiten mit einem qualifizierten IT-Partner.

> *IT-Support ist im Mittelstand längst kein Kostenfaktor mehr – er ist eine Voraussetzung für stabile Geschäftsprozesse und unternehmerische Handlungsfähigkeit. Die Frage ist nicht mehr, ob man sich professionellen IT-Support leisten kann. Die Frage ist, ob man es sich leisten kann, darauf zu verzichten.*

Quellenverzeichnis

BSI – Bundesamt für Sicherheit in der Informationstechnik

- Die Lage der IT-Sicherheit in Deutschland 2025. Berichtszeitraum: 1. Juli 2024 bis 30. Juni 2025. Bonn, November 2025. URL: www.bsi.bund.de/lagebericht
- Die Lage der IT-Sicherheit in Deutschland 2024. Berichtszeitraum: 1. Juli 2023 bis 30. Juni 2024. Bonn, Oktober 2024. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2024.html
- IT-Grundschutz-Kompendium 2023. URL: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html

Bitkom e. V. – Digitalverband Deutschland

- Wirtschaftsschutz 2024. Studie im Auftrag des Digitalverbands Bitkom. Bitkom Research, Berlin, August 2024. URL: https://www.bitkom.org/Presse/Presseinformation/Angriffe-auf-die-deutsche-Wirtschaft-nehmen-zu
- IT-Mittelstandsbericht 2024. Berlin 2024. URL: https://www.bitkom.org/Bitkom/Publikationen/Bitkom-IT-Mittelstandsbericht
- Rekord-Fachkräftemangel: In Deutschland sind 149.000 IT-Jobs unbesetzt. Presseinformation. Bitkom e. V., Berlin, Dezember 2023. URL: https://www.bitkom.org/Presse/Presseinformation/Rekord-Fachkraeftemangel-Deutschland-IT-Jobs-unbesetzt
- In Deutschland fehlen weiterhin mehr als 100.000 IT-Fachkräfte. Presseinformation. Bitkom e. V., Berlin, August 2025. URL: www.bitkom.org/Presse/Presseinformation/Deutschland-fehlen-IT-Fachkraefte

Lünendonk & Hossenfelder GmbH

- Der Markt für IT-Dienstleistungen in Deutschland 2025. Mindelheim 2025. URL: https://www.luenendonk.de/produkt/luenendonk-studie-2025-der-markt-fuer-it-dienstleistungen-in-deutschland/

IDC / Atos

- Digitaler Reifegrad im deutschen Mittelstand. IDC Infobrief im Auftrag von Atos. München, Februar 2024. URL: https://atos.net/de/2024/pressemeldungen_2024_02_26/digitaler-reifegrad-im-deutschen-mittelstand-idc-studie-von-atos-zeigt-dringenden-handlungsbedarf

Ponemon Institute

- Cost of IT Downtime 2023. Ponemon Institute LLC, Traverse City (Michigan) 2023.

Hinweis zur Quellenverwendung:
Alle in diesem White Paper genannten Zahlen und Fakten stammen aus den oben zitierten, öffentlich zugänglichen Studien und Berichten. Die Angaben wurden zum Zeitpunkt der Erstellung (Mai 2026) als aktuell verifiziert. Bei abweichenden Angaben ist die jeweils aktuelle Version der Originalquelle maßgeblich. Stand: Mai 2026

CETOS Services AG

Wir sind ein Berliner IT-Dienstleister mit über 20 Jahren Erfahrung in der Computer- und Softwareverwaltung, mit Kunden in ganz Deutschland und der DACH-Region.

Unser Portfolio reicht vom klassischen IT-Support für mittelständische Unternehmen bis hin zu hochspezialisierten Leistungen wie Softwarepaketierung, Softwareverteilung und der Arbeit in komplexen IT-Infrastrukturen von Konzernen und öffentlichen Einrichtungen.

CETOS Services AG - Wir sorgen für stabile IT-Systeme und hochspezialisierte Softwarebereitstellung.

Adresse

CETOS Services AG
econopark Pankstraße
Pankstraße 8, Haus Q
13127 Berlin

Kontakt

Telefon: +49 30 92 10 80 24-100
Telefax: +49 30 92 10 80 24-999
E-Mail: info@cetos.com

Online

www.cetos.com