„IT im Mittelstand: Was intern bleiben sollte – und was besser rausgeht“

Ein Whitepaper für Geschäftsführer und Inhaber mittelständischer Unternehmen (ca. 30–100 PCs) zur optimalen Verteilung von IT-Aufgaben zwischen internen Mitarbeitern und externen IT-Dienstleistern.

Inhalt

Einleitung

Die IT ist heute das Rückgrat nahezu jedes Unternehmens. Gerade in mittelständischen Betrieben mit 30–100 IT-Arbeitsplätzen hängen Betriebsabläufe stark von zuverlässig funktionierender IT ab. **IT-Ausfälle können den Geschäftsbetrieb massiv beeinträchtigen**, bis hin zur völligen Lahmlegung der Prozesse. Dennoch stehen viele Geschäftsführer vor der Frage: **Welche IT-Aufgaben sollten wir mit eigenem Personal abdecken und was geben wir besser an externe Dienstleister (z. B. Managed Service Provider) ab?**

Dieses Whitepaper liefert einen Überblick über **typische IT-Aufgaben im Mittelstand**, bewertet die **Eignung von interner vs. externer Erledigung** aus verschiedenen Blickwinkeln und gibt konkrete Empfehlungen. Dabei fließen Überlegungen zu **Kosten, Personal, Verfügbarkeit, Sicherheit, Flexibilität und Compliance** ein. Zudem bieten wir **Praxisbeispiele** und **eine tabellarische Entscheidungshilfe**, um Ihnen als Geschäftsführer die Entscheidungsfindung zu erleichtern. Ziel ist es, eine **strategisch sinnvolle Aufgabenteilung** zu skizzieren, die **Wirtschaftlichkeit** und **Sicherheit** vereint.

1. Typische IT-Aufgaben im Mittelstand

Mittelständische Unternehmen müssen eine **Vielzahl von IT-Aufgaben** bewältigen, um den laufenden Betrieb sicherzustellen. Die wichtigsten Aufgabengebiete sind unter anderem:

- **Endnutzer-Support (Helpdesk):** Unterstützung der Mitarbeiter bei IT-Problemen, Einrichtung von PCs, Laptops, Druckern und mobilen Geräten, Beheben von Störungen im Arbeitsalltag (Passwortreset, E-Mail-Probleme etc.).
- **Betrieb der IT-Infrastruktur:** Wartung und Administration von Servern (on-premise oder Cloud-Servern), Netzwerkkomponenten (Router, Switches, WLAN), Telefonanlagen und Peripherie. Hierzu zählen regelmäßige **Updates, Patches und Konfigurationsanpassungen**, um die Betriebsbereitschaft sicherzustellen.
- **Microsoft 365 und Software-Management:** Verwaltung von Cloud-Diensten wie Microsoft 365 (Exchange Online, Teams, SharePoint) oder anderen genutzten Software-as-a-Service-Angeboten. Lizenzmanagement, Benutzerverwaltung und **Sicherstellen der Kompatibilität** gehören dazu.
- **IT-Security (IT-Sicherheit):** Schutz der Systeme und Daten vor Cyberangriffen und Malware. Aufgaben umfassen Firewall-Management, Antivirus-Lösungen, Security-Updates, **Überwachung sicherheitsrelevanter Systeme** sowie Schulung der Mitarbeiter in IT-Sicherheit.
- **Cloud-Services und Virtualisierung:** Betreuung von Cloud-Infrastruktur (z. B. Azure/AWS-Dienste) oder virtualisierten Umgebungen. Planung von Cloud-Migrationen, Management von Cloud-Backups, Monitoring der Cloud-Ressourcen.
- **Backup und Disaster Recovery:** Tägliche Datensicherungen (auf externen Medien oder Cloud-Backup), regelmäßige Wiederherstellungstests, Pflege eines Notfallplans für IT-Ausfälle. **Datenverluste vorbeugen** und im Ernstfall schnelle Wiederherstellung ermöglichen.
- **IT-Projektmanagement:** Planung und Umsetzung von IT-Projekten wie z. B. **Einführung neuer Software**, Upgrades von Hardware, Migrationen (etwa auf Microsoft 365 oder in

die Cloud) oder Ausbau der Infrastruktur. Koordination von Ressourcen, Zeitplänen und Tests, um **Ausfallzeiten gering zu halten**.

- **IT-Strategie und Beratung:** Entwicklung einer langfristigen IT-Strategie, die die Geschäftsziele unterstützt (z. B. Digitalisierung von Prozessen, Einführung neuer Technologien). Beratung der Geschäftsführung in IT-Fragen, Planung von Budgets und **Innovationen**, sowie **Compliance-Management** (Datenschutz, gesetzliche Vorgaben in der IT).

Jede dieser Aufgaben erfordert spezifisches Know-how und ausreichende personelle Ressourcen. Häufig müssen **alltägliche Routinearbeiten (z. B. Benutzer-Support, Backup-Kontrolle)** ebenso abgedeckt werden wie **anspruchsvolle Spezialthemen (z. B. IT-Sicherheit oder strategische IT-Architektur)**. Im nächsten Schritt betrachten wir, welche dieser Aufgabenfelder typischerweise **besser intern** durch eigene Mitarbeiter oder **besser extern** durch einen Dienstleister erledigt werden – und warum.

2. Intern vs. extern: Welche Aufgaben gehören wohin?

Nicht alle IT-Aufgaben sind gleichermaßen für eine **interne Bearbeitung** geeignet. Ebenso wenig sollte man blind alles auslagern. Es gilt, **pro Aufgabenbereich zu bewerten, was aus wirtschaftlicher, organisatorischer und sicherheitstechnischer Sicht am sinnvollsten ist**. Oft läuft es in der Praxis auf einen **Hybrid-Ansatz** hinaus: eine **Kombination aus interner und externer IT-Betreuung**, um die Vorteile beider Seiten zu nutzen.

Grundsatzentscheidung: Für Unternehmen mit 30–100 PCs ist eine rein interne IT-Betreuung in der Regel **nicht wirtschaftlich sinnvoll**. Man bräuchte mindestens zwei, eher drei IT-Mitarbeitende, um Support und Betrieb lückenlos abzudecken – insbesondere bei **Urlaub, Krankheit, Fortbildung oder internen Besprechungen**. Das erzeugt erhebliche **Fixkosten**, ohne dass diese Ressourcen durchgängig ausgelastet wären.

Im Gegensatz dazu profitieren externe IT-Dienstleister von **Skaleneffekten**: Ein externer Partner mit einem **Support-Team von 8 Personen**, das z. B. rund 800–900 PCs betreut, kann den laufenden Betrieb **effizient und wirtschaftlich sicherstellen**. In dieser Struktur entfällt beim Kunden der Bedarf, interne Redundanz vorzuhalten – die **Schicht- und Durchhaltefähigkeit** wird durch den Dienstleister übernommen.

Noch deutlicher wird der Unterschied bei anspruchsvolleren Tätigkeiten wie IT-Architektur, Planung oder Security-Konzeption: Ein **Senior-Techniker** kostet schnell **zwischen 70.000 und 100.000 Euro im Jahr**, ist jedoch in mittelständischen Unternehmen selten **voll ausgelastet**. Dienstleister können diese Expertise über mehrere Kunden hinweg einsetzen – ein erfahrener Techniker betreut oft **bis zu 10 Kunden parallel**. So erhalten Mittelständler Zugang zu einem **fachlichen Niveau, das inhouse weder wirtschaftlich noch personell darstellbar wäre**.

Fazit: Eine **ausschließlich interne Lösung ist in dieser Unternehmensgröße kaum wirtschaftlich sinnvoll** – weder in Bezug auf Skalierbarkeit noch auf fachliche Tiefe. In der Praxis ergibt sich daraus fast zwangsläufig eine **Kombination aus internem Ansprechpartner und externer Betreuung** – ein Modell, das sowohl wirtschaftlich als auch organisatorisch überzeugt.

Aufgaben, die oft intern bleiben sollten: Bereiche, in denen **tiefes Unternehmenswissen, ständige Präsenz vor Ort oder besondere Vertraulichkeit** gefordert sind, werden besser intern betreut. Beispiele: **Geschäftskritische Systeme in der Produktion**, die ein permanentes

Eingreifen erfordern oder spezielles Anwenderwissen voraussetzen – etwa Server, die direkt Maschinen steuern. Hier ist es sinnvoll, eigene IT-Mitarbeiter bereitzuhalten, um sofort reagieren zu können und weil externe Personen ohne dieses Domänenwissen kaum helfen könnten. Auch in **hochvertraulichen Bereichen** (z. B. ein Forschungs- und Entwicklungslabor mit sensiblen Daten) wird man externen Dienstleistern keinen Zugriff erlauben wollen. In solchen Fällen bleibt die IT-Betreuung gezielt intern.

Aufgaben, die sich für extern anbieten: Viele IT-Aufgaben sind **standardisiert oder erfordern Spezial-Know-how**, das ein mittelständisches Unternehmen nicht dauerhaft selbst vorhalten kann. Typische Beispiele: **IT-Security-Maßnahmen** (wie Firewall-Monitoring, Angriffserkennung, Security-Updates) – hier bringen externe Profis Erfahrung aus vielen Projekten ein und bleiben auch am Puls neuester Bedrohungen. **Cloud- und Infrastruktur-Themen** sind ebenfalls oft extern besser aufgehoben, da externe Dienstleister Teams von Spezialisten für Server, Netzwerk, Cloud, Backup etc. bereitstellen. **Komplexe Projekte oder Migrationen** (z. B. Einführung eines neuen ERP-Systems, Umzug von lokalen Servern in die Cloud) profitieren stark von externer Expertise, um **Fallstricke zu vermeiden und einen reibungslosen Ablauf sicherzustellen**. Externe Partner haben hier oft **bewährte Prozesse und Tools**, die intern nicht verfügbar sind. Insgesamt gilt: Aufgaben, die **hochspezialisiertes Fachwissen** verlangen oder die **kontinuierliche Verfügbarkeit eines Teams** (24/7-Betrieb, sehr kurze Reaktionszeiten) voraussetzen, sind prädestiniert fürs Outsourcing an einen externen IT-Dienstleister.

Hybrid-Modelle etablieren: In vielen KMU bewährt sich ein Modell, bei dem ein **Key-User** im Unternehmen benannt wird – oft ein technikaffiner Mitarbeiter mit anderer Hauptfunktion – der kleinere Aufgaben übernehmen kann, die ansonsten einen kostenintensiven Vor-Ort-Einsatz auslösen würden. Dazu zählen z. B. **Austausch defekter Hardware, das Einsetzen von Druckerpatronen oder einfache Sichtprüfungen**. Die Nutzer dürfen sich grundsätzlich direkt an den externen Support wenden, werden aber angehalten, sich zunächst an den Key-User zu wenden. Dieser entscheidet dann, ob der Fall an den IT-Dienstleister weitergegeben wird.

In Unternehmen mit komplexer oder strategisch relevanter IT-Infrastruktur sollte zusätzlich ein **technischer Mitarbeiter mit fundierter IT-Kompetenz** im Haus sein. Dieser ist in der Lage, strategische Fragestellungen zu bewerten, die richtigen Rückfragen an den Dienstleister zu stellen und IT-Entscheidungen im Kontext des Unternehmens zu verorten. Der externe Partner unterstützt beratend, aber die fachliche Einordnung und Verantwortung bleibt intern verankert. Dieses Modell vereint **wirtschaftliche Effizienz, technologische Tiefe und unternehmensspezifische Kontrolle**.

Unabhängig vom gewählten Modell müssen **Kommunikation und Dokumentation** stimmen. Stellen Sie sicher, dass **Wissen über Ihr IT-System zentral festgehalten wird** (Konfigurationen, Passwörter, Netzwerkpläne etc.), sodass bei Ausfall einer Person – ob intern oder extern – der Betrieb weitergehen kann. Mit einem abgestimmten Aufgabenmix lässt sich erreichen, dass Ihre **IT 365 Tage im Jahr betreut ist**, Risiken minimiert werden **und Kernkompetenzen optimal eingesetzt sind**.

3. Entscheidungsfaktoren: Warum interne oder externe IT-Betreuung?

Bei der Bewertung „intern vs. extern“ spielen mehrere Faktoren eine Rolle. Im Folgenden begründen wir die empfohlene Aufgabenteilung anhand der wichtigsten Kriterien:

Kosten und Wirtschaftlichkeit

Personal- vs. Dienstleisterkosten: Auf den ersten Blick scheint ein interner IT-Mitarbeiter günstiger als ein externer Dienstleister. Doch **eine interne IT bringt versteckte Kosten mit sich** – Gehälter, Lohnnebenkosten, fortlaufende Weiterbildung, Ausfallzeiten, Investitionen in Tools, Hardware-Abschreibungen etc. Wenn **alle Kosten knallhart eingerechnet** werden, relativiert sich der vermeintliche Preisvorteil interner IT deutlich. Externe IT-Dienstleister bieten hingegen oft **transparente Pauschalpakete** (z. B. monatlicher Festpreis für definierten Serviceumfang), was die **Budgetierung erleichtert**. Auch Skaleneffekte spielen eine Rolle: Ein externer Dienstleister betreut viele Kunden und kann **Ressourcen effizient auslasten**, während ein interner Mitarbeiter in einem kleinen Team nicht durchgehend ausgelastet ist oder im Gegenteil überlastet wird.

Skalierbarkeit und Auslastung

In einem Unternehmen mit ~50 PCs wären **mindestens 2–3 IT-Mitarbeiter nötig**, um alle Bereiche (Software, Infrastruktur, Security) abzudecken. Diese Mitarbeiter kosten nicht nur Gehalt, sie müssen auch sinnvoll beschäftigt werden. Bei Wachstum des Unternehmens entstehen zusätzliche Kosten, weil man weitere Mitarbeiter einstellen oder Überstunden leisten muss. Ein externer Partner kann hier **flexibel mitwachsen**, ohne dass Sie sich um Rekrutierung kümmern müssen – zusätzliche Leistungen werden einfach dazugebucht. **Skalierung nach unten** (z. B. in einer Auftragsflaute) ist intern schwierig, während man externe Verträge oft anpassen kann. Allerdings: **Komplettes Outsourcing kann auch teuer werden**, wenn der Dienstleister alles von A bis Z managen soll – je nach Vertragsmodell. Ein **Hybrid-Modell** erlaubt es, **teure Spitzen zu glätten**: leichte Routinetätigkeiten durch kostengünstigere interne Kräfte, Spezialaufgaben extern nach Bedarf.

Spezialisierung vs. Generalisten

Kosten und Qualität hängen eng zusammen mit der Qualifikation des Personals. **IT-Fachkräfte mit spezialisiertem Know-how sind teuer**, insbesondere wenn man sie fest einstellt. Im Mittelstand beschäftigt man oft eher **Generalisten**, die „alles ein bisschen“ können. Das kann kurzfristig Kosten sparen, birgt aber Risiken (siehe Know-how). **Externe Anbieter beschäftigen Spezialisten für verschiedene Bereiche**, die ein einzelnes KMU sich nicht leisten könnte. So **bekommen Sie hochkarätiges Know-how, ohne einzelne Experten in Vollzeit bezahlen zu müssen**. Insgesamt gilt: **Interne IT verursacht einen hohen Fixkostenblock**, während Outsourcing **Kosten variabilisiert** und oft **Planbarkeit** schafft (Pauschalen, SLAs). Diese wirtschaftlichen Aspekte sollten gründlich durchgerechnet werden.

Verfügbarkeit und Reaktionszeit

Abdeckung von 24/7 und Ausfallsicherheit: IT-Probleme halten sich nicht an Geschäftszeiten – Ausfälle können jederzeit auftreten. **Eine interne Einzelperson kann unmöglich 365 Tage im Jahr verfügbar sein.** Urlaub, Krankheit und normale Arbeitszeiten begrenzen die Abdeckung.

„Einer ist keiner“– so bringt es eine Studie auf den Punkt: Man braucht zwingend mehrere IT-Mitarbeiter, um dauerhafte Betreuung sicherzustellen, doch genau solche personellen Redundanzen fehlen oft im Mittelstand. Externe Dienstleister hingegen bieten meist **klar geregelte SLAs (Service Level Agreements)**, die 24/7-Bereitschaft oder definierte Reaktionszeiten garantieren. **Ein gutes MSP-Team steht im Notfall rund um die Uhr bereit**, verteilt die Arbeitslast auf mehrere Schultern und stellt sicher, dass auch bei Krankheit oder Fluktuation immer jemand zur Stelle ist. So kann die **Betriebsbereitschaft der IT-Infrastruktur jederzeit gewährleistet** werden[1].

Schnelligkeit vor Ort vs. Remote-Support: Interne IT hat den Vorteil der **örtlichen Nähe** – der IT-Administrator ist direkt im Haus und kann oft **sofort eingreifen**, z. B. einen abgestürzten PC an einem Arbeitsplatz neu starten oder ein Kabel im Serverraum umstecken. Diese **unmittelbare Reaktionsfähigkeit** ist im täglichen Betrieb wertvoll. Ein externer Support arbeitet meist **remote**: Viele Probleme lassen sich per Fernwartung lösen, jedoch nicht alle (Hardwaredefekte, Verkabelung, etc.). Bei externem Support muss ggf. ein Techniker anreisen, was **Zeit kostet**. Für mittlere Unternehmen bietet sich daher häufig an, **einen First-Level-Support intern** vorzuhalten (für schnell lösbare Probleme und Unterstützung der Anwender), während **Second-Level und Spezialfälle extern** abgedeckt werden. So werden einfache Fälle sofort intern gelöst, und bei größeren Störungen zieht der interne ITler den Dienstleister hinzu, der dank seines Teams trotzdem **zügig reagieren** kann.

Reaktionszeiten vertraglich absichern: Ob intern oder extern – wichtig ist, klar zu definieren, welche **maximalen Reaktionszeiten** akzeptabel sind. Interne Mitarbeiter haben hier natürliche Grenzen (wenn sie z. B. gleichzeitig in Meetings eingebunden sind oder am Wochenende nicht erreichbar). Ein externer Dienstleister lässt sich typischerweise auf **kurze Reaktionszeiten vertraglich festnageln** (etwa **Sofortreaktion innerhalb von x Minuten remote, vor Ort innerhalb von y Stunden** je nach Kritikalität). Für kritische Systeme kann das **höhere Servicelevel eines externen Partners** ein entscheidender Vorteil sein. Dennoch sollte ein Unternehmen abwägen, ob z. B. **ein interner Ansprechpartner während der Bürozeiten** kombiniert mit einer **externen Notfall-Hotline außerhalb der Zeiten** die optimale Lösung darstellt – oft eine kostengünstige Mischung.

Fachkräftemangel und Know-how-Verfügbarkeit

IT-Fachkräftemangel in Deutschland: Qualifiziertes IT-Personal ist rar und heiß umkämpft. Ende 2023 waren rund **149.000 Stellen für IT-Experten unbesetzt** – ein neuer Rekord[2]. IT-Stellen bleiben im Schnitt **über 7 Monate vakant**, selbst wenn aktiv gesucht wird. Gerade **kleinere und mittlere Unternehmen leiden darunter**, dass sie **benötigtes Know-how intern kaum noch rekrutieren** können. Wenn doch, sind hohe Gehälter nötig, um Fachkräfte zu halten. Viele KMU behelfen sich mit **„Quereinsteigern“ oder Mitarbeitern mit IT-Affinität**, die IT nebenbei betreuen. Das funktioniert oft eine Weile „gut genug“, birgt aber erhebliche Risiken: Sobald die IT-Umgebung wächst oder ein Spezialproblem auftritt, stoßen diese Allrounder an Grenzen.

Generalist vs. Spezialist: In **den meisten KMU übernimmt ein einzelner IT-Generalist** die IT-Betreuung – teilweise müssen sogar fachfremde Mitarbeiter mithelfen. Diese Person steht **allein vor immer komplexeren Anforderungen**. Moderne IT-Landschaften erfordern Kenntnisse in diversen Bereichen (Netzwerk, Security, Cloud, Anwendungen, Compliance…). Ein einzelner

[1] itmagazine.ch
[2] bitkom.org

kann unmöglich in allem Experte sein. **Interne IT-Spezialisten benötigen zudem viel Zeit für Weiterbildung**, insbesondere in kleinen Teams: Man schätzt, dass IT-Fachleute **mindestens 50 % ihrer Arbeitszeit für Schulung, Recherche und Tests** einplanen müssen, um auf dem neuesten Stand zu bleiben[3]. Je kleiner das Team, desto größer der relative Aufwand pro Kopf – schließlich muss jeder mehrere Rollen ausfüllen. **Externes Know-how schafft hier Abhilfe:** Dienstleister sehen **ähnliche Probleme bei vielen Kunden** und haben dadurch einen Erfahrungsvorsprung; sie können **Lösungen standardisieren und wiederverwenden**, was die Effizienz steigert. Ihr IT-Team profitiert also vom gebündelten Wissen vieler Spezialisten, ohne selbst jeden Trend nachjagen zu müssen.

Know-how-Sicherung und -Transfer: Ein häufiger Engpass in KMU ist der **Wissensverlust, wenn ein interner IT-Administrator das Unternehmen verlässt**. Hat diese eine Person jahrelang alles alleine gemacht, steckt viel implizites Wissen in seinem Kopf (Passwörter, Tricks, Systemzusammenhänge). Beim Weggang drohen große Lücken. **Externen Dienstleistern passiert das nicht so leicht**, da sie interne Dokumentation führen und Team-intern Wissen teilen. Allerdings gibt man beim Outsourcing auch eigenes Wissen aus der Hand – wichtig ist daher, dass **trotz externer Hilfe ein Grundverständnis im Unternehmen bleibt**. Ein hybrider Ansatz kann z. B. vorsehen, dass **der interne IT-Koordinator sich von externen Experten schulen lässt** und so Know-how-Transfer stattfindet. Zudem sollte der **externe Partner verpflichtet werden, Dokumentationen** aktuell zu halten und dem Kunden zugänglich zu machen.

Fachkräftemangel strategisch begegnen: Für viele Mittelständler ist die **Zusammenarbeit mit einem externen Dienstleister eine Antwort auf den IT-Fachkräftemangel**. Anstatt monatelang vergeblich einen Security-Spezialisten oder Cloud-Architekten zu suchen, lagert man diese Aufgaben an Profis aus, die sofort verfügbar sind. Gleichzeitig kann man die **eigenen IT-Mitarbeiter entlasten und mit interessanteren Aufgaben betrauen**: Routinearbeiten gehen an den Dienstleister, während die internen Experten an strategischen oder innovativen Themen arbeiten. Dies erhöht die Zufriedenheit und Bindung der internen IT-Experten, was im **Kampf um Talente** ebenfalls wichtig ist. Kurz gesagt: **Externes Know-how bietet Zugang zu Spezialwissen trotz Fachkräftemangel**, und gut austarierte Aufgabenteilung hilft, die **eigenen Leute zu halten und zu motivieren**.

Flexibilität und Innovationsfähigkeit

Schnelligkeit bei neuen Entwicklungen: Die IT-Welt dreht sich schnell – ob neue Cloud-Services, Sicherheitsbedrohungen oder digitale Tools, ständig gibt es Neuerungen. **Externe IT-Dienstleister sind oft näher am Puls der Zeit**, weil sie sich aus Wettbewerbsgründen laufend mit neuesten Technologien beschäftigen und **gute Netzwerke** in der Branche haben. Spezialisierte Teams erfahren früh von Trends und können **Neuerungen mit hoher Geschwindigkeit umsetzen**. Ein interner Administrator in einem KMU hat dafür oft **wenig Kapazität**, da das Tagesgeschäft ihn vollständig beansprucht und er selten über den Tellerrand schauen kann (**„Feuerwehrmodus“ statt Innovation). Durch Outsourcing von Routine-Aufgaben kann intern **Zeit für Innovation** frei werden[4]. Beispielsweise könnte die interne IT sich um die **Digitalisierung spezifischer Geschäftsprozesse** kümmern, während der MSP für stabile Basis-IT sorgt.

[3] itmagazine.ch
[4] marktundmittelstand.de

Flexibilität in der Leistungserbringung: Unternehmen verändern sich – ein neuer Standort kommt hinzu, Home-Office wird für mehr Mitarbeiter nötig, eine zusätzliche Software wird eingeführt. **Ein externer Partner kann flexibel darauf reagieren**, da er Skalierungsspielraum und verschiedenes Know-how im Team hat. Benötigen Sie z. B. vorübergehend mehr Support-Kapazität (Rollout einer neuen Anwendung, viele Anfragen), kann der Dienstleister **kurzfristig zusätzliche Leute bereitstellen**. Interne Teams stoßen hier an Grenzen, da Neueinstellungen Zeit brauchen und temporäre Überlastung oft unbemerkt zu **Ticket-Staus, verzögerten Projekten und Frust** führt. Zeichen für mangelnde Flexibilität sind u. a. **liegengebliebene Tickets, verschobene Projekte, langsame Umsetzung neuer Anforderungen**– in solchen Fällen ist externes Backup sinnvoll.

Standardisierung und Automatisierung: Externen Profis gelingt es häufig, durch Standardprozesse und Automatisierung die Effizienz zu heben. Weil sie bewährte Methoden mitbringen, werden Fehler reduziert und Rollouts laufen störungsfreier ab. Diese **Professionalität** kommt gerade innovativen Initiativen zugute – z. B. Einführung eines neuen Tools: Ein externer Dienstleister hat eventuell bereits **Templates und Scripts**, um das schnell auszubreiten, wo eine interne IT erst experimentieren müsste. Das heißt nicht, dass interne IT nicht innovativ sein kann – im Gegenteil, durch Entlastung von Routine hat sie erst die **Kraft, Innovation voranzutreiben**. Die **Kombination** macht's: Externe sorgen dafür, dass **wichtige Themen wie IT-Security nicht im Alltagsstress untergehen**, und interne können sich auf die geschäftsrelevanten Verbesserungen fokussieren.

Wettbewerbsvorteil durch Technologie: Letztlich kann ein mittelständisches Unternehmen durch kluge IT-Aufgabenteilung **schneller neue Technologien einsetzen als seine Konkurrenz**. Etwa wenn ein externer Partner ein **neues Cloud-Feature** proaktiv vorschlägt, das Kosten spart oder neue Services ermöglicht. Oder wenn die interne IT dank externer Entlastung endlich Zeit hat, sich mit **Datenanalyse, KI oder Prozessautomation** zu beschäftigen. Diese **Innovationsfähigkeit** wird immer wichtiger, um im Wettbewerb zu bestehen. Ist die IT jedoch dauernd im **Reparatur- und Feuerwehrmodus**, verpasst das Unternehmen Chancen. Deshalb sollte die IT-Strategie immer auch die Frage berücksichtigen: **Wie stellen wir sicher, dass unser IT-Team (intern + extern) genügend Freiraum hat, um Neuerungen zu evaluieren und einzuführen?** Ein externer Dienstleister kann hier Impulse geben und **Best Practices aus anderen Unternehmen** einbringen.

Risiken und Compliance-Anforderungen

Single Point of Failure vermeiden: Eine ausschließlich interne IT mit kleinem Personalstand birgt das **Klumpenrisiko**, dass beim Ausfall einer Person die gesamte IT handlungsunfähig wird. **Was passiert, wenn Ihr einziger IT-Administrator morgen ausfällt – sei es durch Krankheit oder Kündigung?** Ohne Vertretung kann ein solcher Ausfall leicht zum **IT-Notfall** werden: Wichtige Passwörter oder Konfigurationskenntnisse fehlen, aktuelle Probleme bleiben ungelöst und **Geschäftsabläufe stehen still**. Tatsächlich haben **60 % der Unternehmen keinen IT-Notfallplan** für plötzliche Ausfälle oder Angriffe[5]. Das zeigt, wie häufig dieses Risiko unterschätzt wird. Die Einbindung eines externen Dienstleisters mindert dieses Risiko erheblich: Auch wenn Ihr interner Ansprechpartner fehlt, **kennt der externe Partner Ihr System und kann den Betrieb aufrechterhalten**. Zudem verteilt sich bei einer externen Betreuung das Know-how auf mehrere Experten, Ausfälle einzelner Personen dort tangieren Sie kaum.

[5] ihk-muenchen.de

Risiken bei externem Outsourcing: Natürlich gibt es auch Risiken, wenn man IT-Leistungen nach außen gibt. Dazu zählen **Abhängigkeiten von einem Dienstleister** (man begibt sich in gewisses Vertrauen, dass der Partner dauerhaft liefert und wirtschaftlich stabil bleibt) und **mögliche Interessenskonflikte**. Wichtig ist daher, **vertragliche Klarheit** zu schaffen – z. B. in Form von klaren SLAs, Exit-Strategien (Was passiert, wenn man den Dienstleister wechseln will?) und **Eigentumsrechten an Daten und Dokumentation**. Ein weiterer Punkt ist **Datensicherheit und Zugriffskontrolle**: Ein externer Administrator hat Zugriffe auf Ihre sensitiven Systeme, hier müssen **Geheimhaltungsvereinbarungen, Datenschutzverträge (AVV/DPA)** und Zertifizierungen des Dienstleisters geprüft sein. Viele MSPs sind auf **Compliance** vorbereitet, aber die **Verantwortung verbleibt letztlich beim Unternehmen**, sicherzustellen, dass ausgelagerte Funktionen gesetzeskonform betrieben werden.

Compliance und regulatorische Anforderungen: Themen wie **Datenschutz (DSGVO)**, branchenspezifische IT-Regulierungen (z. B. im Finanz- oder Gesundheitswesen) und **IT-Governance** stellen hohe Anforderungen. Für ein internes, kleines IT-Team ist es extrem aufwendig, sämtliche **Compliance-Vorgaben korrekt umzusetzen**, zumal **der Teufel oft im Detail steckt**[6]. Externe Spezialisten haben hier oft **Erfahrung aus ähnlichen Projekten** und können helfen, etwa **IT-Policies, Dokumentationen und Sicherheitsmaßnahmen** auf dem geforderten Niveau einzuführen. So kann Outsourcing gerade im Security- und Compliance-Bereich **Risiken reduzieren**, indem man nichts übersieht. Allerdings ist wichtig, **Verantwortlichkeiten klar zu regeln**: Beispielsweise kann die operative Durchführung einer Sicherheitsmaßnahme extern erfolgen, aber die **Verantwortung im Sinne der DSGVO** (z. B. für personenbezogene Daten) bleibt beim auftraggebenden Unternehmen. Ein guter Dienstleister wird als **Partner agieren**, der aktiv auf Risiken hinweist und bei Audits unterstützt, während die Geschäftsführung intern die letztliche Kontrolle behält.

Betriebskontinuität und Notfallmanagement: Externe Dienstleister bieten häufig auch **zusätzliche Services zur Risikovorsorge**, etwa **Backup-Recovery-Services, Ausweichrechenzentren oder Notfallübungen**. Ein einzelnes KMU könnte solche umfassenden Maßnahmen alleine kaum stemmen. Gleichzeitig muss die interne Organisation vorbereitet sein: **Notfallpläne, Zuständigkeiten im Krisenfall und regelmäßige Tests** sollte man – egal ob intern oder extern – etablieren. Hier zahlt es sich aus, wenn externe Profis ihre **Expertise in Business Continuity** einbringen. Nicht selten zeigt sich erst in der Krise, ob das **Modell intern/extern robust** ist. Daher unsere Empfehlung: **Planen Sie „Was wäre wenn"-Szenarien** durch (z. B. Server fällt aus, Admin nicht erreichbar, Cyberangriff verschlüsselt Daten) und beziehen Sie Ihren IT-Partner in diese Planungen ein. So stellen Sie sicher, dass Risiken minimiert und Compliance-Anforderungen erfüllt werden, ohne dabei auf sich allein gestellt zu sein.

[6] zurichnetgroup.ch

4. Aufgabenmatrix: Intern, extern oder hybrid?

Die folgende Tabelle gibt eine Übersicht der typischen IT-Aufgaben und eine Empfehlung zur Zuweisung – ob diese eher intern, extern oder kombiniert (hybrid) erledigt werden sollten. Zusätzlich ist kurz begründet, warum diese Zuordnung sinnvoll ist:

IT-Aufgabe	Empfehlung	Begründung (Kurz)
Endnutzer-Support (Helpdesk)	Hybrid	Key-User im Unternehmen übernimmt einfache Aufgaben (z. B. Drucker, Hardware-Tausch). Nutzer wenden sich bei Bedarf direkt an externen Support. Wirtschaftlich effizient und alltagsnah.
Infrastruktur-Betrieb	Extern (ggf. Hybrid)	Standardisierte Aufgaben wie Updates, Monitoring etc. durch externen Dienstleister. Key-User kann einfache physische Eingriffe (z. B. Neustart, Austausch) vor Ort übernehmen.
Microsoft 365 & Software-Admin	Extern	Verwaltung der Cloud-Umgebung und Lizenzierung durch MSP. Effizient durch zentrale Tools und Know-how. Intern ggf. Basissupport durch Key-User (Passwörter, Neuanlage).
IT-Sicherheit (Security)	Extern (überwiegend)	Hoher Spezialisierungsgrad, laufende Bedrohungslage. MSP sorgt für Monitoring, Firewall, Patching. Intern: Schulung, Policy-Umsetzung.
Cloud-Services	Extern	Know-how extern erforderlich. Planung, Skalierung und Betrieb durch erfahrenen Partner.
Backup & Disaster Recovery	Extern (ggf. Hybrid)	Technisch anspruchsvolle Umsetzung durch MSP. Intern: Kontrolle von Logs, Meldung von Fehlern.
IT-Projekte & Migrationen	Extern mit internem Koordinator	Externe Expertise verhindert Projektfehler. Interner Projektverantwortlicher sorgt für Anforderungsmanagement und Einbindung der Fachabteilungen.
IT-Strategie & -Planung	Intern (mit externer Beratung)	Strategische Verantwortung liegt intern. Externe Beratung bringt Markt- und Technologiewissen ein.

Legende: „Hybrid“ = Aufgabenteilung zwischen internem Ansprechpartner (Key-User, ggf. technischer IT-Mitarbeiter) und externem Dienstleister.

Diese Zuweisungen haben Empfehlungscharakter und können je nach Unternehmen variieren. Wichtig ist, die **Grenzen der Machbarkeit realistisch abzuschätzen** – etwa ob ein interner Mitarbeiter neben Support auch komplexe Security-Themen stemmen kann (meist nicht der Fall). Die Tabelle zeigt einen generellen Leitfaden: **einfache und reaktive Aufgaben beim Kunden, Spezialwissen und strukturierte Betriebsverantwortung beim Dienstleister**, mit klar definierten Übergabepunkten.

5. Praxisbeispiele: Lerneffekte aus typischen Szenarien

Um die Konsequenzen der Aufgabenteilung greifbarer zu machen, betrachten wir zwei typische Szenarien aus dem Mittelstand:

Beispiel 1: Ausfall des einzigen IT-Admins

Die Mustermann GmbH (50 PC-Arbeitsplätze) hat einen IT-Administrator, der seit Jahren alles alleine managt – vom Passwortreset bis zur Serverwartung. Eines Tages fällt dieser Administrator plötzlich für mehrere Wochen aus (Krankheit). **Die Folgen:** Zunächst merkt man wenig, doch bald bleiben **Support-Anfragen liegen**, da niemand außer ihm Passwörter für bestimmte Systeme kennt. Ein geplanter Upgrade der Buchhaltungssoftware muss verschoben werden. Als dann auch noch der E-Mail-Server Probleme macht, gerät die Firma in Stress: **externe Notfallhilfe** muss ad-hoc organisiert werden, was teuer und zeitaufwändig ist. Dieses Szenario ist leider häufig: Ein Reddit-Nutzer und Admin kommentierte dazu treffend: *„Einfach mal 2 Wochen krank sein und zuschauen, **wie der Laden brennt**…“* 🔥 – sprich, erst wenn der einzige IT-Verantwortliche ausfällt, erkennen viele Unternehmen ihre Abhängigkeit. **Lessons Learned:** Die Geschäftsführung richtet danach eine **vertretungsfähige Struktur** ein. Mustermann GmbH entscheidet sich, einen **externen Dienstleister als Partner** zu engagieren. Der externe Dienstleister sorgt künftig dafür, dass **Dokumentation gepflegt** wird (Passwörter, Netzwerkpläne, laufende Projekte) und steht im Urlaubs- oder Krankheitsfall als **Backup bereit**. Gleichzeitig bleibt der wieder genesene Admin als **interner Koordinator** an Bord. Dieses Hybrid-Modell stellt sicher, dass **kein Einzelpunkt mehr das gesamte Risiko trägt** – Ausfallzeiten können überbrückt werden und **das Wissen ist geteilt**, nicht mehr nur im Kopf einer Person.

Beispiel 2: Migration in die Cloud mit externem Partner

Ein mittelständischer Fertigungsbetrieb plant, seine alte on-premise Exchange E-Mail-Infrastruktur auf **Microsoft 365 (Cloud)** umzustellen, inklusive der Einführung von Teams und OneDrive. Der interne IT-Referent hat so etwas noch nie gemacht, liest Blogs und versucht sich an einem Migrationsplan. Schnell zeigt sich: **die Tücke steckt in vielen Details** (Benutzer synchronisieren, Daten migrieren, Ausfallfenster minimieren, DNS-Umstellungen etc.). Ohne Routine passieren Fehler – im Testlauf gehen einige Kalenderdaten verloren und die Ausfallzeit zieht sich länger als gedacht. Daraufhin wird entschieden, einen **externen IT-Dienstleister hinzuzuziehen**, der auf Microsoft-Cloud-Projekte spezialisiert ist. Dieser bringt **umfassende Erfahrung aus vielen Migrationen** mit, hat bewährte Checklisten und Tools. Gemeinsam mit dem internen IT-Referenten plant man den Umstieg neu. Die externe Crew übernimmt die technische Durchführung an einem Wochenende, während der interne IT-Referent als Ansprechpartner für die Geschäftsführung fungiert und die Mitarbeiterkommunikation übernimmt. **Das Ergebnis:** Die Migration verläuft reibungslos in der vorgesehenen Downtime, keine Daten gehen verloren, und am Montag läuft alles in der Cloud. Gleichzeitig hat der interne IT-Verantwortliche viel gelernt (Know-how-Transfer), sodass er zukünftige Cloud-Administrationsaufgaben größtenteils selbst stemmen kann. **Lessons Learned:** Bei einmaligen Großprojekten oder komplexen technischen Veränderungen lohnt es sich nahezu immer, **externe Expertise einzukaufen**, um **Fehler, Verzögerungen und Risiko zu minimieren**. Die interne IT sollte dennoch beteiligt sein, um Wissen aufzubauen und sicherzustellen, dass die Lösung zum Unternehmen passt. Dieses Beispiel zeigt, **wie externe Dienstleister in kritischen Phasen eine enorme Hilfe sind**, ohne die interne IT zu ersetzen – vielmehr ergänzen sie diese optimal.

Weitere typische Szenarien im Mittelstand könnten ähnlich aussehen: Sei es der **Aufbau eines zweiten Standorts**, wo ein MSP die neue Netzwerk-Infrastruktur bereitstellt, oder eine **Cyberattacke**, bei der ein externes Security-Team bei der Analyse und Wiederherstellung unterstützt. Auch bei **alltäglichen Problemen** (z. B. ein Hardware-Defekt am Server) zahlt sich ein externer Wartungsvertrag aus: Ersatzgerät und Techniker stehen schneller parat, als es intern möglich wäre. Die **Praxis zeigt**: Mittelständler, die **vorausschauend interne und externe Ressourcen kombinieren**, sind resilienter und handlungsfähiger, wenn besondere Situationen eintreten.

6. Fazit und Empfehlungen für KMU

Für kleine und mittelständische Unternehmen (KMU) mit 30–100 PCs gibt es keine Einheitslösung nach dem Motto „alles intern“ oder „alles extern“. Die optimale IT-Aufgabenteilung ist individuell und sollte sich an den **Bedürfnissen, Ressourcen und Zielen** Ihres Unternehmens orientieren. Trotzdem lassen sich einige zentrale Empfehlungen ableiten:

- **Setzen Sie auf einen hybriden Ansatz, wenn möglich:** Für diese Unternehmensgröße bewährt sich häufig eine Kombination aus **Key-User-Modell für einfache Aufgaben** und **externer Betreuung für Spezialthemen**. Ergänzen Sie dies – bei entsprechendem IT-Reifegrad – durch **einen technischen Ansprechpartner im Haus**, der strategische Entscheidungen begleitet.
- **Definieren Sie klare Zuständigkeiten:** Dokumentieren Sie, wer welche Aufgaben übernimmt. Sorgen Sie für saubere Übergabepunkte und vermeiden Sie Zuständigkeitslücken – zum Beispiel durch ein einfaches **Service-Konzept oder internes IT-Rollenblatt**.
- **Bewerten Sie IT-Kosten vollständig und realistisch:** Stellen Sie **interne Kosten für Personal, Weiterbildung, Vertretung und Infrastruktur** den **klar definierten externen Leistungspaketen** gegenüber. Rechnen Sie auch mit Opportunitätskosten – z. B. wenn interne IT-Kräfte durch Alltagsbetrieb von strategischen Aufgaben abgehalten werden.
- **Nutzen Sie externe Ressourcen zur Kompensation von Fachkräftemangel:** Besonders spezialisierte Rollen (Security, Cloud, Architektur) lassen sich wirtschaftlich kaum intern besetzen. Ein externer Partner bietet sofort verfügbares Know-how – und entlastet die internen Kräfte.
- **Planen Sie zukunftsorientiert:** Ihre IT-Aufstellung sollte nicht nur heute funktionieren, sondern auch in drei Jahren noch tragfähig sein. Digitalisierung, wachsender Remote-Anteil und steigende Cyberrisiken erfordern **laufende Weiterentwicklung** – intern wie extern.
- **Holen Sie regelmäßig externe Impulse:** Ein Blick von außen auf Ihre IT-Struktur hilft, blinde Flecken zu erkennen. Lassen Sie Ihre IT-Strategie gelegentlich durch externe Fachleute reflektieren – z. B. durch einen CIO-as-a-Service oder eine unabhängige Systemprüfung.
- **Notfallplanung und Dokumentation nicht vergessen:** Ohne dokumentierte Passwörter, Netzwerkpläne und Zuständigkeiten ist Ihr Unternehmen im Ernstfall nicht handlungsfähig. Sorgen Sie dafür, dass **Wissen nicht an einzelne Personen gebunden** ist – weder intern noch extern.

- **Überprüfen Sie regelmäßig die Aufgabenteilung:** Wächst das Unternehmen? Verändert sich die Technik? Hat sich die interne Kompetenz weiterentwickelt? Überprüfen Sie Ihre IT-Aufteilung **mindestens jährlich**, um auf Veränderungen schnell reagieren zu können.

Fazit: Eine abgestimmte IT-Aufgabenteilung verschafft mittelständischen Unternehmen Stabilität, Effizienz und Handlungssicherheit. Mit der richtigen Balance aus Eigenleistung und externer Unterstützung wird IT vom Kostenfaktor zur strategischen Stärke – und schafft Raum für Innovation, Sicherheit und Zukunftsfähigkeit.