n-komm.
Unser IT Partner

Whitepaper

IT-Betrieb auslagern: wann es sich lohnt und was in den Vertrag gehört

Bereiche, Betriebsort, Vertrag und Übergang: ein Leitfaden für Geschäftsführung und IT-Leitung im Mittelstand.



n-komm GmbH · Karlsruhe · Stand November 2026

Auf einen Blick

Bereiche, Betriebsort, Vertrag und Übergang: ein Leitfaden für Geschäftsführung und IT-Leitung im Mittelstand.

- Managed IT Services lohnen sich vor allem dann, wenn IT-Wissen an wenigen Personen hängt, Routinearbeit liegen bleibt oder die Kosten schwer planbar sind. Sie müssen nicht alles abgeben: Co-Managed IT verstärkt ein vorhandenes IT-Team bei klar abgegrenzten Aufgaben.
- Gut eignen sich Bereiche mit wiederkehrender, gut beschreibbarer Arbeit: Überwachung und Updates, Server und Datensicherung, Arbeitsplätze und Microsoft 365, Helpdesk, der Betrieb von Anwendungen wie ELO ECM und der laufende Schutz der IT.
- Beim Betriebsort zählt, dass Sie wissen, wo Ihre Daten liegen und wer sie betreut. Rechenzentren in Deutschland, eine Zertifizierung nach ISO/IEC 27001 und eine Datensicherung mit unveränderbarer Kopie sind belastbare Prüfpunkte.
- Die Service-Vereinbarung entscheidet über den Erfolg: Leistungsumfang, Servicezeiten, Reaktionszeiten, Verantwortlichkeiten, Berichte und der geregelte Ausstieg gehören schriftlich festgehalten, bevor der Betrieb beginnt.
- Der Übergang gelingt in Schritten: Bestandsaufnahme, Startgespräch, geordnete Übernahme mit Dokumentation, Einbindung des Teams und regelmäßige Abstimmung. Bei der n-komm vergehen erfahrungsgemäß 2 bis 8 Wochen bis zum laufenden Betrieb.

Inhalt

1. Wann sich das Auslagern des IT-Betriebs lohnt
2. Welche Bereiche sich für Managed Services eignen
3. Betriebsort und Datenhaltung: Ihre Daten in Deutschland
4. Was in die Service-Vereinbarung gehört
5. Wie der Übergang gelingt
6. Wie die n-komm unterstützt
7. Checkliste: Prüffragen vor dem Auslagern

01

Wann sich das Auslagern des IT-Betriebs lohnt

Bei Managed IT Services übernimmt ein IT-Dienstleister dauerhaft den Betrieb Ihrer IT oder einzelner Bereiche, zu einem planbaren Monatspreis. Er überwacht Server und Arbeitsplätze, spielt Updates ein, sichert Daten und hilft Ihren Beschäftigten im Helpdesk. Ein solcher Dienstleister heißt Managed Service Provider, kurz MSP.

Der Unterschied zum klassischen IT-Service auf Abruf liegt im Zeitpunkt. Beim Support auf Abruf kommt der Dienstleister, wenn etwas kaputt ist, und berechnet den Einsatz. Bei Managed Services kümmert er sich laufend und kann viele Störungen verhindern, bevor sie entstehen. Damit haben Auftraggeber und Dienstleister dasselbe Interesse: eine IT, die stabil läuft.

Ob sich das Auslagern lohnt, entscheidet selten die Technik allein. Häufiger geht es um Personal und Planbarkeit. Wenn das gesamte IT-Wissen an einer oder zwei Personen hängt, werden Urlaub und Krankheit zum Betriebsrisiko. Gleichzeitig wird die Umgebung nicht einfacher: Updates kommen jede Woche, Microsoft 365 und Cloud-Dienste verändern sich laufend, und Fachkräfte für Betrieb und Sicherheit sind schwer zu finden.

Auslagern heißt nicht, die Kontrolle abzugeben. Sie legen fest, was der Dienstleister betreut, in welchem Umfang und nach welchen Regeln. Die strategischen Entscheidungen bleiben bei Ihnen: welche Anwendungen Sie einsetzen, wohin sich die IT entwickelt und wie viel Sie investieren. Was Sie abgeben, ist vor allem die wiederkehrende Betriebsarbeit.

Zwei Modelle haben sich bewährt. Bei der Komplettbetreuung übernimmt der Dienstleister die Rolle der IT-Abteilung, etwa wenn es keine eigene gibt. Bei Co-Managed IT verstärkt er ein vorhandenes Team bei festgelegten Aufgaben, zum Beispiel bei Überwachung und Patch-Management, also dem geplanten Einspielen von Updates, oder bei der Datensicherung. Beide Modelle lassen sich später anpassen.

Es gibt auch Gründe, Aufgaben im Haus zu behalten. Wer ein eingespieltes IT-Team mit ausreichender Vertretung hat, gewinnt durch Auslagern oft wenig. Sehr spezielle Systeme, die nur wenige Fachleute kennen, brauchen einen Dienstleister mit genau dieser Erfahrung, sonst verlagert sich das Risiko nur. Und manche Aufgaben, etwa die Abstimmung mit den Fachabteilungen oder die Auswahl neuer Anwendungen, gehören ohnehin ins eigene Haus. Eine ehrliche Bestandsaufnahme zeigt, wo die Grenze für Ihr Unternehmen verläuft.

Auch die Kosten sollten Sie vollständig betrachten. Support auf Abruf wirkt auf den ersten Blick günstiger, weil nur gezahlt wird, wenn etwas passiert. Ausfälle, Notfalleinsätze, stillstehende Arbeitsplätze und Sicherheitsvorfälle tauchen in dieser Rechnung aber selten auf. Ein planbarer Monatsbetrag, je nach Leistung pro Arbeitsplatz oder pro Server, macht die IT-Kosten kalkulierbar und lässt sich direkt mit dem Aufwand für eigenes Personal vergleichen.

- Das IT-Wissen hängt an einer oder zwei Personen, Vertretungen sind nicht geregelt.
- Updates und Datensicherungen laufen, werden aber nicht regelmäßig geprüft.

- Bei Störungen warten Beschäftigte, bis jemand Zeit hat, besonders im Homeoffice.
- Die IT-Kosten schwanken von Monat zu Monat, Investitionen erfolgen spontan.
- Für Sicherheit, Dokumentation und Planung bleibt im Tagesgeschäft keine Zeit.
- Ihr IT-Team kommt vor lauter Routineanfragen nicht zu seinen Projekten.

Kurz erklärt: Co-Managed IT

Bei Co-Managed IT verstärkt ein Dienstleister Ihre eigene IT-Abteilung. Er übernimmt festgelegte Aufgaben, etwa den First-Level-Support, die Überwachung oder die Datensicherung. Ihr Team behält die Verantwortung für den Rest, gewinnt Zeit für Projekte und hat bei Urlaub oder Krankheit eine Vertretung. Entscheidend ist eine genaue Abgrenzung, wer was übernimmt.

02

Welche Bereiche sich für Managed Services eignen

Gut geeignet sind Aufgaben, die regelmäßig anfallen, sich klar beschreiben lassen und von Erfahrung mit vielen Umgebungen profitieren. Viele Unternehmen starten mit einem Bereich und erweitern später. Wichtig ist, dass die Bausteine ineinandergreifen und nicht jeder Bereich bei einem anderen Dienstleister liegt, sonst entstehen genau an den Schnittstellen die Lücken.

IT-Infrastruktur umfasst Server, Speicher, Netzwerk und Arbeitsplätze, also alles, was Ihre Anwendungen zum Laufen brauchen. In vielen Unternehmen ist sie gewachsen, nicht geplant. Ein Dienstleister kann hier zweierlei leisten: einen Gesamtplan mit Prioritäten und Zeitplan für Investitionen und danach den laufenden Betrieb. Bei Problemen gibt es dann keinen Streit darüber, wer zuständig ist.

Server, Cloud und Datensicherung gehören zu den wichtigsten Kandidaten. Auf den Servern laufen ERP-System, Dateiablage, Dokumentenmanagement und E-Mail. Der Betrieb umfasst Überwachung von Speicher, Leistung und Diensten, geplante Updates und Virtualisierung. Ebenso wichtig ist die Datensicherung: Sie ist nur so gut wie ihre Wiederherstellung, und genau die wird im Alltag selten geprüft.

Beim Arbeitsplatz und Microsoft 365 geht es um Notebooks und PCs, Benutzerkonten, Lizenzen und sichere Einstellungen. Ein Dienstleister richtet neue Geräte ein, verwaltet sie zentral, zum Beispiel mit Microsoft Intune, und hält Windows und Programme aktuell. Neue Beschäftigte finden am ersten Tag einen fertigen Arbeitsplatz vor, und wer das Unternehmen verlässt, verliert seine Zugänge ohne Verzug.

Der Helpdesk ist die Anlaufstelle für alle IT-Fragen Ihrer Beschäftigten, per Telefon, E-Mail oder Ticket. Der Vorteil gegenüber dem Dienstleister auf Abruf: Der Helpdesk kennt Ihre Umgebung, und niemand muss bei jedem Anruf neu erklären, wie sie aussieht. Wiederkehrende Probleme werden sichtbar und lassen sich an der Ursache beheben.

Auch Fachanwendungen lassen sich betreiben. Ein Beispiel ist ein Dokumentenmanagement wie ELO ECM: Updates wollen auf einem Testsystem geprüft, Schnittstellen zu ERP oder DATEV gepflegt und Berechtigungen aktuell gehalten werden. Die Softwarepflege des Herstellers stellt neue Versionen bereit, spielt sie aber nicht ein und testet nicht Ihre Anpassungen. Diese Lücke schließt der Betrieb als Managed Service.

Managed Security schließlich ist der laufende Schutz der IT. Dazu gehören Endpoint-Schutz, also die Absicherung jedes Notebooks, PCs und Servers, der Betrieb der Firewall, eine Überwachung mit SIEM, regelmäßige Schwachstellenprüfungen und Schulungen der Beschäftigten. Ein SIEM sammelt die Meldungen aus Ihren Systemen an einer Stelle und erkennt Muster, die einzeln unauffällig wären. Einmalige Projekte wie ein Penetrationstest ergänzen den laufenden Schutz, ersetzen ihn aber nicht.

Bereich	Typische laufende Aufgaben	Vorab klären
Infrastruktur	Planung, Erneuerung, Netzwerkbetrieb	Gesamtplan und Investitionszeitplan
Server, Cloud, Backup	Überwachung, Updates, Sicherung	Betriebsort, Wiederherstellungstests
Workplace, Microsoft 365	Geräte, Benutzer, Lizenzen, Updates	Bestandsgeräte, Lizenzmodell
Helpdesk	Anfragen annehmen, lösen, dokumentieren	Servicezeiten, Kanäle, Eskalation
Anwendungen (z. B. ELO ECM)	Updates, Schnittstellen, Rechte	Testsystem, Zuständigkeit Hersteller
Managed Security	Schutz, Überwachung, Schwachstellen	Überwachungszeiten, Vorgehen im Ernstfall

03

Betriebsort und Datenhaltung: Ihre Daten in Deutschland

Wer den Betrieb auslagert, muss nicht zwingend die Server auslagern. Grundsätzlich gibt es drei Varianten, die sich auch kombinieren lassen. Die Server bleiben in Ihrem Haus, und der Dienstleister betreibt sie aus der Ferne. Oder sie laufen im Rechenzentrum des Dienstleisters oder eines Partners. Oder Sie nutzen Dienste großer Cloud-Anbieter, etwa für Microsoft 365.

Der Betrieb im eigenen Haus eignet sich, wenn Daten das Gebäude nicht verlassen sollen oder Anwendungen kurze Wege brauchen. Sie benötigen dann aber weiter einen geeigneten Serverraum, eigene Hardware und deren Erneuerung. Ein Rechenzentrum des Dienstleisters nimmt Ihnen genau das ab: kein eigener Serverraum, keine eigene Serverhardware, dafür ein planbarer Monatsbetrag. Häufig ist ein Mix sinnvoll, etwa Server vor Ort und Datensicherung im Rechenzentrum.

Für die Auswahl zählen Rechenleistung, Verfügbarkeit, Wachstum, Datenschutz und das gewünschte Betriebskonzept. Beim Datenschutz ist die wichtigste Frage einfach: Wissen Sie, wo Ihre Daten liegen und wer sie betreut? Rechenzentren in Deutschland, betrieben von Unternehmen, die Sie kennen, machen diese Frage leicht zu beantworten.

Belastbare Nachweise helfen bei der Bewertung. Eine Zertifizierung nach ISO/IEC 27001 zeigt, dass ein Betreiber ein Managementsystem für Informationssicherheit eingeführt hat und es regelmäßig von unabhängiger Stelle prüfen lässt. Fragen Sie nach dem Geltungsbereich: Umfasst das Zertifikat auch das Rechenzentrum, in dem Ihre Systeme laufen?

Ebenso wichtig ist das Sicherungskonzept. Bewährt hat sich die Regel, mehrere Kopien auf unterschiedlichen Medien zu halten, mindestens eine davon an einem anderen Ort. Gegen Ransomware, also Schadsoftware, die Daten und gezielt auch Datensicherungen verschlüsselt, schützt eine Kopie, die sich nicht verändern oder löschen lässt. Legen Sie außerdem fest, welche Systeme im Ernstfall zuerst wieder laufen müssen und wie viele Daten Sie höchstens verlieren dürfen. Daraus entstehen Sicherungsrhythmus und Notfallplan.

Ein häufiges Missverständnis betrifft Cloud-Dienste wie Microsoft 365. Der Anbieter sorgt dafür, dass der Dienst läuft, aber nicht automatisch dafür, dass Sie gelöschte oder verschlüsselte Inhalte beliebig lange zurückholen können. Prüfen Sie deshalb, ob Postfächer, OneDrive und SharePoint zusätzlich und unabhängig gesichert werden sollen. Diese Frage gehört in jedes Sicherungskonzept, gleich wo die übrigen Systeme laufen.

Planen Sie den Betriebsort nicht als Entscheidung für immer. Anforderungen ändern sich, und ein guter Dienstleister ermöglicht später den Wechsel zwischen den Varianten, etwa von Servern im eigenen Haus in ein Rechenzentrum. Viele Unternehmen beginnen mit der Datensicherung im Rechenzentrum und verlagern danach einzelne Server, Schritt für Schritt und ohne den laufenden Betrieb zu unterbrechen.

Kurz erklärt: unveränderbare Datensicherung

Bei einer unveränderbaren Datensicherung, Fachleute sprechen von Immutable Backup, wird eine Kopie so gespeichert, dass sie für einen festgelegten Zeitraum weder verändert noch gelöscht werden kann, auch nicht mit Administratorrechten. Verschlüsseln Angreifer Ihre Systeme, bleibt diese Kopie für die Wiederherstellung erhalten. Sie ersetzt keine regelmäßigen Wiederherstellungstests, sondern ergänzt sie.

04

Was in die Service-Vereinbarung gehört

Managed Services stehen und fallen mit der Service-Vereinbarung, oft SLA genannt (Service Level Agreement). Sie hält fest, was der Dienstleister leistet, wann er erreichbar ist und wie schnell er reagiert. Je genauer sie formuliert ist, desto weniger Diskussion gibt es im Alltag und im Ernstfall.

Am Anfang steht der Leistungsumfang. Welche Systeme, Standorte, Arbeitsplätze und Anwendungen betreut der Dienstleister, und was ist ausdrücklich nicht enthalten? Wie werden Leistungen außerhalb des Umfangs abgerechnet, etwa Projekte oder Weiterentwicklungen? Halten Sie auch fest, wie Sie den Umfang anpassen, wenn Ihr Unternehmen wächst oder neue Anwendungen dazukommen.

Servicezeiten und Reaktionszeiten sind zwei verschiedene Dinge. Die Servicezeit regelt, wann Ihre Beschäftigten den Helpdesk erreichen. Die Reaktionszeit regelt, wie schnell der Dienstleister auf eine Meldung reagiert, meist abgestuft nach Dringlichkeit: Steht ein Arbeitsplatz still oder sind viele betroffen, hat das Vorrang. Prüfen Sie, ob Sie eine Bereitschaft außerhalb der Servicezeiten brauchen, und vereinbaren Sie sie dann ausdrücklich. Verlassen Sie sich nur auf Zeiten, die im Vertrag stehen.

Ein häufiger Konfliktpunkt sind ungeklärte Verantwortlichkeiten. Wer entscheidet über Änderungen, wer gibt Updates frei, wer spricht mit den Herstellern Ihrer Fachanwendungen? Beim Co-Managed-Modell ist diese Abgrenzung besonders wichtig, weil zwei Teams an derselben Umgebung arbeiten. Eine einfache Tabelle mit Aufgaben und Zuständigkeiten verhindert, dass Aufgaben doppelt oder gar nicht erledigt werden.

Berichte und Abstimmungstermine machen die Leistung sichtbar. Vereinbaren Sie, welche Kennzahlen Sie regelmäßig erhalten, etwa zu Anfragen, Sicherungen und Systemzustand, und wie oft Sie den Zustand Ihrer IT gemeinsam besprechen. Verarbeitet der Dienstleister personenbezogene Daten in Ihrem Auftrag, gehört in der Regel ein Vertrag zur Auftragsverarbeitung nach der DSGVO dazu. Regeln Sie außerdem, wann und wie der Dienstleister auf Geräte Ihrer Beschäftigten zugreift, und binden Sie, falls vorhanden, den Betriebsrat ein.

Oft vergessen wird der Ausstieg, im Fachjargon Exit. Er ist kein Zeichen von Misstrauen, sondern sichert Ihre Handlungsfähigkeit. Klären Sie Laufzeit und Kündigungsfristen, die Übergabe der Dokumentation, aller Zugangsdaten und Konfigurationen, die Herausgabe Ihrer Daten in einem nutzbaren Format und die Mitwirkung des Dienstleisters bei der Übergabe an einen Nachfolger. Wer das zu Beginn regelt, muss es im Streitfall nicht verhandeln.

Schließlich lohnt ein Blick auf das Vorgehen im Ernstfall. Was passiert, wenn ein Angriff erkannt wird oder ein zentrales System ausfällt? Wer wird informiert, wer darf Geräte vom Netz nehmen,

und wer unterstützt bei Meldungen an Behörden? Diese Fragen sind schnell beantwortet, solange alles läuft, und schwer, wenn es darauf ankommt.

Vertragsbestandteil	Was geregelt sein sollte
Leistungsumfang	Betreute Systeme, Ausschlüsse, Abrechnung von Zusatzleistungen
Servicezeiten	Erreichbarkeit des Helpdesks, Kanäle, Bereitschaft nach Bedarf
Reaktionszeiten	Abgestuft nach Dringlichkeit, schriftlich im Vertrag
Verantwortlichkeiten	Freigaben, Änderungen, Herstellerkontakt, Eskalation
Berichte und Datenschutz	Kennzahlen, Abstimmungstermine, Auftragsverarbeitung
Exit	Laufzeit, Kündigung, Übergabe von Daten und Dokumentation

05

Wie der Übergang gelingt

Die meisten Sorgen vor dem Auslagern betreffen nicht den späteren Betrieb, sondern den Wechsel. Läuft während der Übernahme alles weiter? Geht Wissen verloren? Ein geordnetes Vorgehen in wenigen Schritten beantwortet diese Fragen. Wie lange die Übernahme dauert, hängt von Größe, Komplexität und Dokumentationsstand der Umgebung ab. Bei der n-komm vergehen erfahrungsgemäß 2 bis 8 Wochen von der Bestandsaufnahme bis zum laufenden Betrieb.

Am Anfang steht die Bestandsaufnahme: Welche Arbeitsplätze, Server, Netzwerke und Anwendungen gibt es, wer betreut sie heute, und wo hakt es? Sie zeigt Risiken, etwa veraltete Systeme oder ungetestete Datensicherungen, und ist die Grundlage für jedes belastbare Angebot. Gleichzeitig klären Sie Ihre Ziele: planbare Kosten, weniger Ausfälle, mehr Sicherheit oder Entlastung des eigenen Teams.

Auf das Angebot mit Leistungsumfang und Service-Levels folgt ein Startgespräch. Darin klären beide Seiten Erwartungen, Rollen und Ansprechpartner: Wer meldet Störungen, wer entscheidet über Änderungen, und wie oft stimmen Sie sich ab? Danach übernimmt der Dienstleister die Umgebung Schritt für Schritt. Er richtet Überwachung und Datensicherung ein, dokumentiert die Umgebung und schließt erste Sicherheitslücken.

Die Dokumentation ist dabei mehr als eine Pflichtübung. Sie sorgt dafür, dass das Wissen über Ihre IT nicht mehr an einzelnen Personen hängt, weder bei Ihnen noch beim Dienstleister. Und sie ist die Voraussetzung für einen späteren Wechsel, falls er je nötig wird.

Vergessen Sie nicht Ihre Beschäftigten. Zeigen Sie, wie sie den Helpdesk erreichen und was sich für sie ändert. Arbeitet weiter eine eigene IT mit, vereinbaren Sie genau, wer welche Aufgaben übernimmt. Im laufenden Betrieb sorgen regelmäßige Termine und Kennzahlen dafür, dass Sie nachsteuern können, etwa wenn neue Anforderungen dazukommen oder Hardware erneuert werden muss.

- Bestandsaufnahme: Systeme, Anwendungen, Zuständigkeiten und Risiken erfassen.
- Ziele und Modell festlegen: Komplettbetreuung oder Co-Managed IT.
- Service-Vereinbarung abschließen, einschließlich Exit-Regelung.
- Startgespräch: Rollen, Ansprechpartner und Abstimmungsrhythmus klären.
- Geordnete Übernahme mit Überwachung, Datensicherung und Dokumentation.
- Beschäftigte informieren und den Helpdesk bekannt machen.
- Laufender Betrieb mit Berichten, Kennzahlen und regelmäßigen Terminen.

Aus der Praxis: Wiederherstellung zuerst prüfen

Viele Unternehmen sichern ihre Daten seit Jahren, haben eine Wiederherstellung aber nie ausprobiert. Lassen Sie deshalb früh in der Übernahme prüfen, ob sich Daten und Systeme aus der Sicherung tatsächlich zurückholen lassen, und das Ergebnis dokumentieren. Vereinbaren Sie solche Tests anschließend regelmäßig.

06

Wie die n-komm unterstützt

Die n-komm GmbH aus Karlsruhe betreut IT seit 2000, von Karlsruhe und Hamburg aus für Unternehmen in Deutschland, Österreich und der Schweiz. Wir betreuen mehr als 1.000 Arbeitsplätze und sind nach ISO/IEC 27001 zertifiziert. Wir arbeiten als komplette IT-Abteilung oder als Verstärkung für Ihr eigenes Team (Co-Managed IT). Welches Modell passt, klären wir im Erstgespräch.

Sie wählen die Bausteine, die Sie brauchen: IT-Infrastruktur, Server, Cloud und Backup, Managed Workplace und Microsoft 365, Helpdesk und Support, Managed ELO ECM, Managed IT-Security sowie HCL Notes und Domino. Im Hintergrund überwachen wir Ihre Systeme, spielen Updates geplant ein, sichern Ihre Daten nach festem Plan und dokumentieren Ihre Umgebung. In regelmäßigen Terminen besprechen wir mit Ihnen den Zustand Ihrer IT und anstehende Erneuerungen.

Für den Betrieb Ihrer Server und Anwendungen gibt es die n-komm Cloud. Ihre Systeme laufen in unserem eigenen Rechenzentrum in Karlsruhe, das im Geltungsbereich unserer ISO-27001-Zertifizierung liegt, oder bei unserem Partner Continum AG mit Rechenzentren in Freiburg, Karlsruhe und Mannheim. Continum ist seit mehr als zehn Jahren nach ISO/IEC 27001 und PCI DSS zertifiziert. Alle Rechenzentren stehen in Deutschland. Auf Wunsch betreuen wir Ihre Server auch bei Ihnen im Haus. Mindestens eine Kopie Ihrer Daten speichern wir so, dass sie sich nicht verändern oder löschen lässt, und Wiederherstellungstests vereinbaren wir mit Ihnen.

Ihr Team erreicht unseren Helpdesk montags bis freitags von 8 bis 17 Uhr per Telefon, E-Mail und Ticketportal. Viele Anliegen lösen wir per Fernwartung, wenn nötig kommen wir vor Ort, deutschlandweit. Eine Bereitschaft außerhalb dieser Zeiten vereinbaren wir bei Bedarf gesondert, Reaktionszeiten gelten laut Vertrag. In der Service-Vereinbarung halten wir schriftlich fest, welche Systeme und Anwendungen wir betreuen und wann Sie uns erreichen.

Weil wir auch Spezialisten für Cyber Security und für Dokumentenmanagement mit ELO sind, haben Sie für Betrieb, Sicherheit und Digitalisierung einen Ansprechpartner. Wir haben ELO in über 200 Projekten eingeführt und betreuen ELO-Systeme auch dann, wenn wir sie nicht selbst eingeführt haben. Für IBM i ist in unserer Unternehmensgruppe die WITS zuständig: Sie erbringt die Managed Services für IBM Power i, die n-komm die Managed Services für die allgemeine IT und die IT-Security.

Der Weg zur betreuten IT verläuft bei uns in vier Schritten: Bestandsaufnahme, Angebot mit Leistungsumfang, Service-Levels und monatlichem Preis, geordnete Übernahme und laufender Betrieb. Als Familienunternehmen in zweiter Generation legen wir Wert auf langfristige Zusammenarbeit und feste Ansprechpartner, die Ihre Umgebung kennen.

Die n-komm in Kürze

IT-Betreuung seit 2000 von Karlsruhe und Hamburg aus, mehr als 1.000 betreute Arbeitsplätze, zertifiziert nach ISO/IEC 27001. Betrieb bei Ihnen im Haus, im eigenen Rechenzentrum in Karlsruhe oder bei der Continum AG, alle in Deutschland. Helpdesk montags bis freitags von 8 bis 17 Uhr, Reaktionszeiten laut Vertrag.

Checkliste: Prüffragen vor dem Auslagern

- [ ] Haben wir eine aktuelle Übersicht über Arbeitsplätze, Server, Netzwerk und Anwendungen?
- [ ] Welche Ziele verfolgen wir: planbare Kosten, weniger Ausfälle, mehr Sicherheit oder Entlastung?
- [ ] Passt Komplettbetreuung oder Co-Managed IT besser zu unserem Team?
- [ ] Welche Bereiche geben wir ab, und welche bleiben bewusst bei uns?
- [ ] Wo sollen unsere Systeme und Daten laufen, und welche Nachweise hat der Betreiber?
- [ ] Wann wurde zuletzt eine Wiederherstellung aus der Datensicherung getestet?
- [ ] Sind Leistungsumfang, Servicezeiten und Reaktionszeiten schriftlich im Vertrag festgehalten?
- [ ] Ist geklärt, wer Änderungen freigibt und wer mit Herstellern spricht?
- [ ] Regelt der Vertrag den Ausstieg mit Übergabe von Daten, Zugängen und Dokumentation?
- [ ] Wissen unsere Beschäftigten, wie sie den Helpdesk erreichen?

Wer kümmert sich um Ihre IT, wenn Ihr IT-Kollege im Urlaub ist?

Im kostenlosen Erstgespräch schauen wir gemeinsam auf Ihre IT. Sie erfahren, ob Komplettbetreuung oder Verstärkung besser zu Ihnen passt und welches Betriebsmodell sich für Ihre Systeme eignet. 30 Minuten per Teams oder Telefon, unverbindlich.

Kostenloses Erstgespräch vereinbaren

---

n-komm GmbH · Karlsruhe
Tel. +49 721 35 46 00 · info@n-komm.de
n-komm.de/managed-it-services/

n-komm. Unser IT Partner

Stand November 2026. Dieses Whitepaper gibt einen fachlichen Überblick und ersetzt keine individuelle Beratung. © n-komm GmbH