WHITE PAPER

IT-Risiken im Mittelstand

Risiken, Lösungen und Best Practices

2026 - CETOS Services AG

Gesamtschaden dt. Wirtschaft 2024
267 Mrd. €

IT-Sicherheitsausgaben in DE 2024
11,2 Mrd. €

1. Executive Summary

Der deutsche Mittelstand ist das Rückgrat der Volkswirtschaft – und steht gleichzeitig im Zentrum einer wachsenden Bedrohungslandschaft. Cyberangriffe, Datenverlust und ein anhaltender Fachkräftemangel setzen IT-Abteilungen unter enormen Druck. Während Großkonzerne über dedizierte Security-Teams und erhebliche IT-Budgets verfügen, müssen mittelständische Unternehmen mit 50 bis 500 Mitarbeitenden oft deutlich mehr mit weniger erreichen.

Dieses White Paper analysiert die drei zentralen Risikobereiche im IT-Support des Mittelstands – Cyberbedrohungen, Fachkräftemangel und Compliance-Anforderungen – und leitet daraus praxiserprobte Lösungsansätze und konkrete Best Practices ab. Die zugrunde liegenden Zahlen und Fakten stammen ausschließlich aus verifizierten Quellen des Bundesamts für Sicherheit in der Informationstechnik (BSI) sowie des Digitalverbands Bitkom.

> *Reaktiver IT-Support kostet mittelständische Unternehmen nachweislich mehr als ein proaktiv aufgestellter IT-Betrieb – sowohl in direkten Kosten als auch in Produktivitätsverlusten und Reputationsschäden. IT-Sicherheit ist kein Kostenfaktor, sondern eine strategische Investition in die Zukunftsfähigkeit des Unternehmens.*

2. Ausgangslage: IT-Risiken im Mittelstand heute

Die Cybersicherheitslage in Deutschland ist nach Einschätzung des BSI angespannt und besorgniserregend. Der BSI-Lagebericht 2024 (Berichtszeitraum Juli 2023 bis Juni 2024) zeichnet ein klares Bild: Cyberangriffe nehmen zu, werden professioneller – und treffen zunehmend auch kleine und mittlere Unternehmen.

309.000	**81 %**	**267 Mrd. €**
neue Schadprogramme täglich, weltweit (BSI-Lagebericht 2024)	der deutschen Unternehmen betroffen (Bitkom: Wirtschaftsschutz 2024)	Gesamtschaden dt. Wirtschaft durch Cyberkriminalität 2024 (Bitkom: Wirtschaftsschutz 2024)

Quellen: BSI – Die Lage der IT-Sicherheit in Deutschland 2024; Bitkom – Wirtschaftsschutz 2024 (n=1.003 Unternehmen)

Besonders aufschlussreich ist die Entwicklung der letzten Jahre: Laut Bitkom-Wirtschaftsschutzstudie 2024 waren 81 Prozent aller befragten deutschen Unternehmen in den vorangegangenen zwölf Monaten von Datendiebstahl, Industriespionage oder Sabotage betroffen – ein Anstieg von 9 Prozentpunkten gegenüber dem Vorjahr. Der dadurch verursachte Gesamtschaden stieg um 29 Prozent auf den Rekordwert von 266,6 Milliarden Euro, wovon 178,6 Milliarden Euro direkt auf Cyberkriminalität entfallen.

Der BSI-Lagebericht 2024 hebt hervor, dass kleine und mittlere Unternehmen (KMU) meist nicht gezielt, sondern als Teil groß angelegter und automatisierter Angriffskampagnen getroffen werden. Dies macht sie nicht zu einem kleineren Ziel – im Gegenteil: Die Schutzlücken sind häufig größer als bei großen Unternehmen, da es an Budget, Personal und Expertise fehlt.

3. Die größten Risiken im IT-Support des Mittelstands

3.1 Cyberangriffe und Ransomware

Ransomware – also Schadsoftware, die Systeme verschlüsselt und Lösegeld erpresst – bleibt laut BSI und Bitkom die gravierendste Einzelbedrohung für Unternehmen jeder Größe. Das Geschäftsmodell hat sich professionalisiert: Unter dem Begriff Ransomware as a Service (RaaS) stellen kriminelle Gruppen ihre Infrastruktur gegen Provision anderen Angreifern zur Verfügung, was die Einstiegshürde drastisch senkt.

Bedrohungsindikator	Quelle
309.000 neue Malware-Varianten täglich (+26 % zum Vorjahr)	*BSI Lagebericht 2024*
Ransomware ist häufigste Ursache für Cyberschäden (31 % aller Fälle)	*Bitkom Wirtschaftsschutz 2024*
1,1 Milliarden USD Lösegeld weltweit im Berichtszeitraum erpresst	*BSI Lagebericht 2024*
80 % der angezeigten Cyberangriffe richten sich gegen KMU	*BSI Lagebericht 2024*
65 % der Unternehmen fühlen sich durch Cyberangriffe existenziell bedroht	*Bitkom Wirtschaftsschutz 2024*

Quellen: BSI – Die Lage der IT-Sicherheit in Deutschland 2024; Bitkom – Wirtschaftsschutz 2024

Ein besonders besorgniserregender Trend ist die zunehmende Nutzung von Zero-Day-Schwachstellen durch gut finanzierte Angreifergruppen. Da für diese Sicherheitslücken noch keine Patches existieren, bleibt mittelständischen Unternehmen oft keine Reaktionszeit. Täglich wurden im Berichtszeitraum 78 neue Schwachstellen in Softwareprodukten bekannt – ein Anstieg von 14 Prozent gegenüber dem Vorjahr (BSI 2024).

3.2 Fachkräftemangel

Der Mangel an qualifizierten IT-Fachkräften ist ein systemisches Problem der deutschen Wirtschaft, das sich unabhängig von Konjunkturzyklen verschärft. Aktuell fehlen in deutschen Unternehmen rund 109.000 IT-Fachkräfte (Bitkom, August 2025). Auf dem Hochpunkt 2023 waren es sogar 149.000 unbesetzte Stellen – fünf Jahre zuvor lag die Zahl noch bei 82.000.

IT-Stellen bleiben in deutschen Unternehmen im Schnitt 7,7 Monate unbesetzt, und 70 Prozent der Unternehmen beklagen einen spürbaren Mangel an IT-Fachkräften auf dem Arbeitsmarkt. Besonders ernüchternd: Nur 2 Prozent halten das aktuelle Angebot für ausreichend (Bitkom 2023). Der Blick nach vorne stimmt kaum optimistischer – 79 Prozent der Unternehmen erwarten eine weitere Verschlechterung der Lage in den kommenden Jahren (Bitkom 2025).

Quellen: Bitkom – Arbeitsmarkt für IT-Fachkräfte 2023 und 2025 (je n>850 Unternehmen)

Für den Mittelstand bedeutet dies eine strukturelle Herausforderung: Offene IT-Stellen können nicht zeitnah besetzt werden, vorhandene Mitarbeitende werden überlastet, und die Abhängigkeit von einzelnen Schlüsselpersonen steigt. Das sogenannte Key-Person-Risk – der Ausfall einer einzigen zentralen IT-Person durch Krankheit, Urlaub oder Kündigung – kann ganze IT-Abteilungen lähmen.

3.3 Compliance und regulatorische Anforderungen

Die regulatorischen Anforderungen an IT-Sicherheit nehmen zu. Mit der europäischen NIS-2-Richtlinie (Network and Information Security Directive 2) werden deutlich mehr Unternehmen als bisher zu konkreten IT-Sicherheitsmaßnahmen verpflichtet. Neben NIS-2 gelten weiterhin die DSGVO (Datenschutz-Grundverordnung) sowie branchenspezifische Regularien.

NIS-2: Erweiterte Meldepflichten bei Sicherheitsvorfällen, Haftung der Geschäftsführung
DSGVO: Technisch-organisatorische Maßnahmen zum Schutz personenbezogener Daten
Branchenspezifisch: KRITIS-Verordnung, branchenspezifische Sicherheitsstandards (B3S)

Die NIS-2-Richtlinie erweitert den Kreis der betroffenen Unternehmen erheblich. Auch mittelständische Unternehmen in sogenannten "wichtigen" und "besonders wichtigen" Einrichtungen sind jetzt explizit erfasst. Geschäftsführer haften persönlich für die Umsetzung der geforderten Sicherheitsmaßnahmen.

4. Analyse und Trends

4.1 Die wirtschaftliche Dimension von IT-Ausfällen

Die finanziellen Folgen von Cyberangriffen und IT-Ausfällen werden häufig unterschätzt. Neben direkten Kosten durch Lösegeldforderungen, Wiederherstellung und Forensik entstehen erhebliche indirekte Schäden durch Produktionsausfälle, Reputationsschäden und den Verlust von Kundendaten oder geistigem Eigentum.

267 Mrd. €	**+29 %**	**11,2 Mrd. €**
Gesamtschaden dt. Wirtschaft 2024 (Bitkom)	Schadensanstieg gegenüber 2023 (Bitkom)	IT-Sicherheitsausgaben in DE 2024 (BSI)

Quellen: Bitkom – Wirtschaftsschutz 2024; BSI – Lagebericht 2024

Die Diskrepanz zwischen dem Gesamtschaden (267 Milliarden Euro) und den IT-Sicherheitsausgaben (11,2 Milliarden Euro) verdeutlicht das wirtschaftliche Argument für präventive IT-Sicherheitsinvestitionen. Der Return on Security Investment (ROSI) fällt bei konsequenter Prävention nachweislich positiv aus.

4.2 Aktuelle Bedrohungstrends

Der BSI-Lagebericht 2024 und die Bitkom-Wirtschaftsschutzstudie 2024 identifizieren mehrere Entwicklungen, die besondere Aufmerksamkeit erfordern:

- **RaaS:** Ransomware as a Service (RaaS): Professionelle Hackergruppen vermieten ihre Infrastruktur, was die Zahl potenzieller Angreifer dramatisch erhöht.
- **KI-Angriffe:** KI-gestützte Angriffe: Künstliche Intelligenz wird zunehmend für überzeugenderes Phishing, automatisierte Schwachstellensuche und Social Engineering genutzt.
- **Lieferkette:** Supply-Chain-Attacken: 13 % der Unternehmen berichten von Angriffen über Zulieferer und IT-Dienstleister (Bitkom 2024).
- **Double Extortion:** Datenlecks als Druckmittel: Neben der Verschlüsselung werden gestohlene Daten zunehmend als zweite Erpressungsebene eingesetzt.

Besonders alarmierend: Laut Bitkom 2024 berichten 80 Prozent der Unternehmen von einer Zunahme an Cyberattacken in den vergangenen zwölf Monaten – und nur 53 Prozent sind der Meinung, ihr Unternehmen sei sehr gut auf Cyberangriffe vorbereitet.

5. Lösungsansätze für den Mittelstand

Es gibt keine Einheitslösung für den IT-Support im Mittelstand. Entscheidend ist die Passgenauigkeit zum eigenen Unternehmen: Größe, Branche, Digitalisierungsgrad und vorhandene IT-Kompetenz bestimmen, welches Modell den größten Mehrwert bietet.

5.1 Endpoint-Management

Zentralisiertes Endpoint-Management ist die Grundlage eines strukturierten IT-Betriebs. Es ermöglicht die einheitliche Verwaltung, Überwachung und Absicherung aller Endgeräte – von Laptops über Smartphones bis zu Servern.

Ein automatisiertes Patch-Management sorgt dafür, dass Sicherheitsupdates zeitnah und flächendeckend eingespielt werden – ohne manuellen Aufwand. Die zentrale Softwareverteilung standardisiert die Softwareumgebungen und reduziert damit sowohl Angriffsflächen als auch Supportaufwand. Mobile Geräte werden über Mobile Device Management (MDM) in die Sicherheitsstrategie einbezogen, und eine vollständige Asset-Inventarisierung bildet die Grundlage für alle weiteren Security-Analysen.

5.2 Backup & Recovery

Funktionierende Backups sind die effektivste Versicherung gegen Ransomware und Datenverlust. Die bewährte 3-2-1-Strategie bildet den Goldstandard: drei Kopien der Daten, auf zwei verschiedenen Medien, davon eine Kopie außerhalb des Unternehmens (offsite oder Cloud).

Die Umsetzung erfordert automatisierte, regelmäßige Backups ohne manuelle Eingriffe sowie den Einsatz von Offline- oder Immutable-Backups, die auch bei einem aktiven Ransomware-Angriff nicht verschlüsselt werden können. Ebenso wichtig ist die Definition klarer Recovery-Ziele: Recovery Time Objective (RTO) und Recovery Point Objective (RPO) müssen festgelegt, dokumentiert und den relevanten Personen bekannt sein. Abgerundet wird das Konzept durch einen getesteten Wiederherstellungsplan, der im Ernstfall handlungsfähig macht.

> *Praxishinweis: Ein Backup, das nicht regelmäßig auf Wiederherstellbarkeit getestet wird, ist kein echtes Backup. Die Wiederherstellungsfähigkeit (Recovery Testing) sollte mindestens quartalsweise nachgewiesen werden.*

5.3 Passwort-Tresor und Identitätsmanagement

Angriffe auf Passwörter waren für 24 Prozent der Cyberschäden verantwortlich (Bitkom 2024). Ein professionelles Identitäts- und Zugriffsmanagement (IAM) reduziert dieses Risiko erheblich.

Unternehmensweite Passwort-Manager ermöglichen die zentrale Verwaltung sicherer, einzigartiger Passwörter für alle Dienste. Multi-Faktor-Authentifizierung (MFA) ergänzt den Passwortschutz als zweiter Schutzfaktor bei allen externen Zugängen, VPNs und privilegierten Konten. Das Least-Privilege-Prinzip stellt sicher, dass Mitarbeitende nur auf die Systeme und Daten zugreifen können, die sie für ihre Aufgaben tatsächlich benötigen. Nicht mehr benötigte Accounts sollten regelmäßig überprüft und zeitnah deaktiviert werden.

5.4 24/7-Monitoring und Incident Response

Ohne kontinuierliches Monitoring bleiben Angriffe oft wochenlang unentdeckt. Der durchschnittliche Zeitraum zwischen Einbruch und Entdeckung (Mean Time to Detect, MTTD) liegt bei Mittelstandsunternehmen häufig bei mehreren Wochen – genug Zeit für Angreifer, tief ins Netzwerk einzudringen.

Ein Security Information and Event Management (SIEM) bündelt alle Sicherheitsereignisse zentral und ermöglicht ihre Auswertung in Echtzeit. Für Unternehmen ohne eigenes Sicherheitsteam ist Managed Detection & Response (MDR) eine kostengünstige Alternative: Spezialisierte Dienstleister übernehmen das 24/7-Monitoring extern. Parallel dazu benötigt jedes Unternehmen einen dokumentierten Incident Response Plan mit klar geregelten Prozessen und Verantwortlichkeiten für den Ernstfall. Regelmäßige Penetrationstests – also simulierte Angriffe durch Sicherheitsexperten – helfen dabei, Schwachstellen zu finden, bevor echte Angreifer sie ausnutzen.

6. Best Practices

Die folgenden Maßnahmen haben sich in der Praxis als besonders wirkungsvoll erwiesen und können unabhängig vom gewählten IT-Support-Modell umgesetzt werden. Sie sind nach Priorität sortiert und bilden einen strukturierten Fahrplan für den Aufbau einer resilienten IT-Infrastruktur.

Bereich	Maßnahme	Priorität
Sicherheit	Multi-Faktor-Authentifizierung (MFA) für alle externen Zugänge einführen	**Hoch**
Backup	3-2-1-Backup-Strategie implementieren und regelmäßig testen	**Hoch**
Monitoring	Proaktives System-Monitoring mit automatischen Alerts einrichten	**Hoch**
Dokumentation	IT-Systemlandschaft und Konfigurationen laufend dokumentieren	**Mittel**
Schulung	Mindestens jährliche Security-Awareness-Schulungen für alle Mitarbeitenden	**Mittel**
SLAs	Klare Reaktions- und Lösungszeiten für IT-Anfragen definieren	**Mittel**
Notfallplan	Business Continuity Plan (BCP) und IT-Notfallplan erstellen und üben	**Empfohlen**
Compliance	NIS-2-Betroffenheit prüfen und ggf. Maßnahmenplan aufsetzen	**Empfohlen**

Prioritätseinstufung basiert auf BSI IT-Grundschutz und BSI-Empfehlungen für KMU (www.bsi.bund.de)

7. Handlungsempfehlungen

7.1 IT-Risikoanalyse durchführen

Der erste Schritt ist eine ehrliche Bestandsaufnahme. Eine strukturierte IT-Risikoanalyse deckt blinde Flecken auf und priorisiert Handlungsbedarfe. Das BSI bietet mit dem Cyber-Risiko-Check (basierend auf DIN SPEC 27076) einen niedrigschwelligen Einstieg speziell für KMU an.

Zunächst werden alle IT-Systeme, Daten und Prozesse vollständig inventarisiert. Darauf aufbauend werden relevante Bedrohungsszenarien und Schwachstellen identifiziert. Für jedes Szenario erfolgt eine Bewertung von Schadenspotenzial und Eintrittswahrscheinlichkeit. Auf dieser Grundlage können Maßnahmen nach ihrem Kosten-Nutzen-Verhältnis priorisiert werden. Die Ergebnisse werden dokumentiert und regelmäßig aktualisiert – idealerweise jährlich oder nach wesentlichen Veränderungen der IT-Landschaft.

7.2 Backup-Konzept implementieren

Ein professionelles Backup-Konzept ist die wichtigste Einzelmaßnahme gegen Ransomware und Datenverlust. Es schützt nicht nur vor Cyberangriffen, sondern auch vor Hardware-Ausfällen, menschlichen Fehlern und Naturkatastrophen.

Konkret bedeutet das: Die 3-2-1-Strategie wird implementiert und dokumentiert, tägliche Backups aller kritischen Daten laufen automatisiert. Backup-Kopien werden offline oder in einem Immutable-Storage abgelegt, sodass Ransomware keinen Zugriff erhält. Wiederherstellungstests finden mindestens quartalsweise statt und werden dokumentiert. Recovery Time Objective (RTO) und Recovery Point Objective (RPO) werden definiert und den relevanten Personen kommuniziert.

7.3 Outsourcing kritischer IT-Aufgaben prüfen

Angesichts des anhaltenden Fachkräftemangels – aktuell fehlen in Deutschland rund 109.000 IT-Fachkräfte (Bitkom 2025) – ist die vollständige Inhouse-Abdeckung aller IT-Aufgaben für die meisten mittelständischen Unternehmen weder realistisch noch wirtschaftlich sinnvoll. Ein durchdachtes Hybrid-Modell kombiniert interne IT-Kompetenz mit spezialisierten externen Partnern.

In der Praxis bewähren sich drei externe Modelle: Managed Service Provider (MSP) übernehmen den laufenden IT-Betrieb auf Basis klar definierter SLAs. Wer zusätzlich ein dediziertes Sicherheits-Monitoring benötigt, kann ein Security Operations Center (SOC) beauftragen – externe Sicherheitsexperten, die rund um die Uhr überwachen. Eine Cloud-First-Strategie wiederum verlagert Dienste in zertifizierte Cloud-Umgebungen und reduziert dadurch den eigenen Wartungsaufwand erheblich. Bei allen Modellen gilt: SLAs, Datenschutzvereinbarungen und Exit-Szenarien müssen vertraglich präzise geregelt sein.

8. Fazit

IT-Risiken sind im Mittelstand allgegenwärtig und erfordern besondere Aufmerksamkeit. Die Zahlen von BSI und Bitkom zeigen unmissverständlich: Cyberangriffe nehmen zu, werden professioneller, und 65 Prozent der betroffenen Unternehmen fühlen sich existenziell bedroht.

Gleichzeitig ist die Situation nicht hoffnungslos. Unternehmen, die frühzeitig in strukturierte Prozesse, klare Verantwortlichkeiten und proaktive Sicherheitsmaßnahmen investieren, sind nachweislich resilienter gegenüber Angriffen und können auch im Ernstfall schneller reagieren.

> *Die drei wichtigsten Sofortmaßnahmen: (1) Multi-Faktor-Authentifizierung für alle externen Zugänge aktivieren, (2) Backup-Konzept nach 3-2-1-Prinzip implementieren und testen, (3) Proaktives IT-Monitoring einrichten. Diese drei Maßnahmen haben den größten Hebel bei überschaubarem Aufwand.*

Quellenverzeichnis

BSI – Bundesamt für Sicherheit in der Informationstechnik

Die Lage der IT-Sicherheit in Deutschland 2024. Berichtszeitraum: 1. Juli 2023 bis 30. Juni 2024. Bundesamt für Sicherheit in der Informationstechnik, Bonn 2024. URL: www.bsi.bund.de

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
- 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

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