



OBERLAND.IT
MIT SICHERHEIT ZUM ERFOLG



5 IT-Fehler

**die dein Unternehmen
finanziell schädigen können!**



Inhaltsverzeichnis

Vorwort	02
IT-Fehler und deren Auswirkungen	03
Warum Sie Ihre IT nicht dem Zufall überlassen sollten.	05
Die 5 größten IT-Fehler und deren Schadenspotential	07
Case-Study aus der Praxis	10
Checkliste - Wie sicher ist Ihre IT wirklich?	15
Fazit und der nächste Schritt.	20



Die **Oberland IT GmbH** mit Sitz in Garmisch-Partenkirchen steht seit vielen Jahren für zuverlässige, transparente und lösungsorientierte IT-Betreuung im oberbayerischen Raum. Unser Fokus liegt auf kleinen und mittleren Unternehmen, die ihre IT nicht dem Zufall überlassen wollen - sondern auf Sicherheit, Stabilität und Zukunftsfähigkeit setzen.

Was uns besonders macht:

Viele unserer Kunden kommen zu uns, obwohl sie bereits einen IT-Anbieter haben. Warum? Weil sie feststellen, dass es einen Unterschied macht, wer sich kümmert. Bei uns gibt es keine versteckten Probleme, keine halbherzigen Lösungen und kein Fachchinesisch. Stattdessen setzen wir auf:

- ✓ **Individuelle Betreuung statt Massenabfertigung**
- ✓ **Transparente Prozesse und klare Empfehlungen**
- ✓ **Langfristige Lösungen statt kurzfristiger Flickschusterei**

Ob es um IT-Sicherheit, Systembetreuung, Cloud-Lösungen oder Mitarbeiterschulung geht – wir handeln proaktiv, nicht erst, wenn's brennt. Unser Ziel: Dass unsere Kunden nachts ruhig schlafen können, weil sie wissen, dass ihre IT funktioniert – zuverlässig, sicher und professionell betreut.

Oberland IT: Persönlich. Klar. Kompetent.

Jetzt IT checken lassen.

IT-Fehler und deren Auswirkungen

Für viele Unternehmen läuft die IT einfach mit – still im Hintergrund, unauffällig, zuverlässig. Zumindest scheinbar. Denn oft zeigt sich erst im Ernstfall, wo die wahren Schwachstellen liegen: Wenn plötzlich keine Datensicherung greift, ein Cyberangriff erfolgreich ist oder der alte Server endgültig den Dienst quittiert. Dann ist der Schaden nicht nur technisch, sondern auch wirtschaftlich enorm.

In der Praxis begegnen wir bei der **Oberland IT** immer wieder denselben grundlegenden Fehlern – auch in Unternehmen, die bereits von einem IT-Dienstleister betreut werden.

Schnellüberblick

1. Fehlende oder unzureichende Datensicherung

Backups, die nicht funktionieren oder nicht vorhanden sind.

2. Kein Schutz durch eine professionelle Firewall

Ein offenes Einfallstor für Angreifer.

3. Ungeprüfte E-Mail-Kommunikation

Einfallstor Nummer eins für Cyberkriminalität.

4. Veralterte Hard- und Software

Insbesondere durch das Support-Ende von Windows 10 ein aktuelles Risiko!

5. Keine Schulung der Mitarbeitenden

Menschliche Fehler bleiben das größte Sicherheitsleck

Diese Punkte allein können ein **Unternehmen empfindlich treffen**. Noch gefährlicher wird es, wenn IT rein reaktiv betrieben wird - also erst dann gehandelt wird, wenn bereits etwas passiert ist.

Deshalb ist **jetzt** der **richtige Zeitpunkt**, einen kritischen Blick auf Ihre IT zu werfen. Dieses E-Book zeigt Ihnen in komprimierter Form, worauf es ankommt - und gibt Ihnen eine **Checkliste zur Selbsteinschätzung**, mit der Sie in nur **15 Minuten** herausfinden, ob Ihr Unternehmen gefährdet ist.

Unser Anspruch: Nach diesem E-Book wissen Sie, wo Ihre IT sicher aufgestellt ist - und wo es konkreten Handlungsbedarf gibt.



**Prüfen Sie wie es um Ihre IT steht!
Machen Sie den Selbsttest auf Seite 11.**



Warum Sie Ihre IT nicht dem Zufall überlassen sollten.

IT ist längst kein Nebenschauplatz mehr - sie ist das Rückgrat jedes modernen Unternehmens. Sobald Server, Netzwerke oder Software stillstehen, steht oft das gesamte Unternehmen mit ihnen still. Und das passiert leider häufiger, als man denkt.



Ein paar Zahlen, die zum Nachdenken anregen:

- Ein durchschnittlicher IT-Ausfall kostet deutsche Unternehmen rund **5.000 Euro pro Stunde** - bei produktionsnahen Betrieben oder Online-Handel deutlich mehr.
- Laut Bitkom benötigen betroffene Unternehmen im Schnitt **3 bis 5 Tage**, um sich nach einem IT-Sicherheitsvorfall wieder voll funktionsfähig aufzustellen.
- Über **70% der erfolgreichen Cyberangriffe** auf KMUs beginnen mit einer einfachen E-Mail - Phishing, infizierte Anhänge oder gefälschte Absender.
- **40% der Unternehmen**, die einen schweren Datenverlust erleiden, **erholen sich nie vollständig** davon - weil Kunden abspringen, Strafen drohen oder Vertrauen dauerhaft verloren geht.

Was vielen Unternehmern nicht bewusst ist: **Die größte Bedrohung liegt nicht in hochkomplexen Angriffen, sondern in einfachen Versäumnissen.** Kein Backup, keine Firewall, veraltete Software - das reicht aus, um ein Unternehmen komplett lahmzulegen.

Ob Handwerksbetrieb, Steuerkanzlei oder Einzelhändler: Die Risiken sind überall dieselben. Und sie lassen sich vermeiden - wenn man die IT aktiv und professionell gestaltet, anstatt erst im Notfall zu reagieren.



Im nächsten Kapitel stellen wir Ihnen die **fünf gravierendsten IT-Fehler** vor, die wir in kleinen und mittelständischen Unternehmen regelmäßig sehen. Und wir zeigen auf, welches finanzielle Schadenspotenzial tatsächlich dahinter steckt.

Von unbrauchbaren Backups über veraltete Systeme bis hin zu fehlender Mitarbeitersensibilisierung.

Lassen Sie Ihre IT prüfen!

Die 5 größten IT-Fehler und deren Schadenspotential

Wir thematisieren nun die fünf häufigsten IT-Fehler, die Unternehmen zum Verhängnis werden können. Unabhängig davon, ob bereits ein IT-Dienstleister im Einsatz ist oder nicht. Dabei zeigen wir Ihnen, was in der Praxis passiert, wenn diese Schwachstellen **nicht erkannt oder ignoriert werden**, und welches **finanzielle Schadens-potenzial** dahintersteckt.



1. Fehlende oder unzureichende Datensicherung

Ein funktionierendes Backup ist wie eine Versicherung - man merkt erst, wie wichtig es ist, wenn es zu spät ist. In der Praxis sehen wir häufig Sicherungslösungen, die nie getestet wurden, veraltet sind oder im Ernstfall gar nicht funktionieren.

Besonders kritisch wird es, wenn wichtige Kundendaten, Auftragsinformationen oder ganze Buchhaltungssysteme betroffen sind. Der Datenverlust kann nicht nur den Betriebsablauf stoppen, sondern auch rechtliche und steuerliche Probleme nach sich ziehen.

Die Wiederherstellung (sofern überhaupt möglich) kostet Zeit, Nerven und bares Geld.

Finanzielles Risiko: 10.000 – 100.000 € je nach Ausmaß des Datenverlusts.

2. Kein Schutz durch eine professionelle Firewall

Ohne eine moderne Firewall gleicht das Firmennetzwerk einem unverschlossenen Haus - jeder kann rein, keiner kontrolliert. Angreifer scannen gezielt kleine Unternehmen nach offenen Zugängen ab. Sind diese vorhanden, kann Schadsoftware unbemerkt ins System gelangen und dort Daten verschlüsseln oder ausspähen. Besonders gefährlich: Oft bleibt ein solcher Angriff unentdeckt, bis der Schaden bereits angerichtet ist. Die Folge können Betriebsstillstand, Erpressung oder sogar Bußgelder wegen Datenschutzverstößen sein.

Finanzielles Risiko: 20.000 – 150.000 €, inkl. möglicher DSGVO-Strafen.

3. Ungeprüfte E-Mail-Kommunikation

E-Mails gehören zum Alltag - und genau das macht sie so gefährlich. Cyberkriminelle nutzen gezielte Phishing-Mails, um Schadsoftware einzuschleusen oder Zugangsdaten abzugreifen. Ohne eine automatische E-Mail-Filterung oder Mitarbeitersensibilisierung genügt ein falscher Klick, und der Schaden ist angerichtet. Ein infiziertes System kann in Minuten lahmgelegt werden, während die IT tagelang mit der Schadensbegrenzung beschäftigt ist.

Hinzu kommen Imageschäden und mögliche Haftungsfragen, wenn Kundendaten betroffen sind.

Finanzielles Risiko: 5.000 – 75.000 €, je nach Vorfall und Folgeschäden.

4. Veraltete Hard- und Software

Viele Unternehmen arbeiten noch mit Windows 10 - obwohl der Support für Sicherheitsupdates demnächst endet. Veraltete Systeme sind ein ideales Ziel für automatisierte Angriffe, da bekannte Schwachstellen nicht mehr geschlossen werden. Gleiches gilt für Server, Drucker oder branchenspezifische Software, die nicht regelmäßig aktualisiert wird. Sicherheitslücken, Systemabstürze und Inkompatibilitäten häufen sich - mit direkten Auswirkungen auf Produktivität und Sicherheit.

Finanzielles Risiko: 10.000 – 80.000 €, durch Ausfälle, Mehraufwand und Sicherheitsvorfälle.

5. Keine Schulung der Mitarbeitenden

Die größte Sicherheitslücke sitzt oft vor dem Bildschirm. Ohne regelmäßige Schulungen wissen viele Mitarbeitende nicht, wie sie mit verdächtigen E-Mails umgehen, sichere Passwörter erstellen oder sensible Daten schützen sollen. Dabei sind menschliche Fehler der häufigste Auslöser für Sicherheitsvorfälle - nicht die Technik. Ein falscher Klick, eine unbedachte Weitergabe von Informationen oder das Nutzen unsicherer USB-Sticks kann schwerwiegende Folgen haben. Prävention ist hier deutlich günstiger als Schadensbehebung.

Finanzielles Risiko: 2.000 – 50.000 €, abhängig vom Auslöser und betroffenen Daten.



LAUBENDERARCHITEKTUR

Case Study aus der Praxis.

Das Laubender Architekturbüro mit rund 15 Mitarbeitenden stand vor einer kritischen Schwelle: Die bestehende IT-Infrastruktur war im Laufe der Jahre nicht in der gleichen Geschwindigkeit gewachsen wie der das Unternehmen, manche sicherheitsrelevante IT-Systeme blieben dabei auf der Strecke.

Die IT-Landschaft bestand aus einem Mini-PC als „Server“, vereinzelt Anti-Viren-Lösungen und einer zwar zentral verwalteten, aber nicht abgesicherten Microsoft 365 Umgebung.

Der Zugang zum Firmennetzwerk erfolgte teilweise unverschlüsselt oder ohne Mehrfaktor-Authentifizierung - ein typisches Bild in vielen gewachsenen Organisationen.

Lösungsansatz:

Ziel war es, die bestehenden Schwachstellen systematisch zu beheben und die IT nachhaltig sicher, effizient und zukunftsfähig aufzustellen. Nach einer Bestandsaufnahme entschied sich das Architekturbüro für eine ganzheitliche Erneuerung und Absicherung - umgesetzt durch die Oberland IT GmbH. Im Fokus standen Zukunftssicherheit, Ausfallschutz und Verteidigung gegen Cyberangriffe.

1. Server-Modernisierung auf leistungsfähige Hardware

Der bisherige Mini-PC wurde durch einen professionellen Server mit unterbrechungsfreier Stromversorgung (USV), RAID-Speicher und Remote-Verwaltung ersetzt. Der neue Server garantiert:

- Hohe Performance für lokale Anwendungen und Dienste
- Skalierbarkeit für zukünftige Anforderungen
- Sicherem Betrieb auch bei Stromausfällen

Mögliche wirtschaftliche Schäden:

- Systemausfall durch Hardwaredefekt mit bis zu 5 Tagen Ausfallzeit
- Geschätzter wirtschaftlicher Schaden: **ca. 30.000€** durch Geschäftsunterbrechung und Verzögerungen bei Kundenprojekten

2. Zentrales Patchmanagement mit integriertem Virenschutz

Alle Arbeitsplatzrechner wurden in ein zentrales Patchmanagement überführt. Sicherheitsupdates und Patches werden automatisiert installiert. Zudem schützt eine einheitliche Virenschutzlösung alle Geräte zuverlässig vor Schadsoftware.

Ergebnisse:

- Minimale Angriffsfläche durch aktuelle Systeme
- Kein manuelles Nachpflegen oder Vergessen von Updates
- Transparenz für IT-Verantwortliche

Mögliche wirtschaftliche Schäden:

- Infektion durch Schadsoftware (z.B. Verschlüsselungstrojaner) über bekannte Sicherheitslücken
- Schaden durch Datenverlust oder Betriebsunterbrechung: **bis zu 150.000 €** (inkl. IT-Forensik und Wiederherstellung)

3. Firewall und VPN mit Zwei-Faktor-Authentifizierung

Die VPN-Zugänge für das Homeoffice wurden mit einer modernen Next-Generation-Firewall abgesichert. Jede Verbindung ist durch Zwei-Faktor-Authentifizierung geschützt. Die Firewall filtert zudem schädlichen Datenverkehr und isoliert Netzbereiche.

Sicherheitseffekte:

- Deutlich reduzierte Angriffsfläche
- Schutz vor unautorisiertem Fernzugriff
- Mehr Sichtbarkeit über die Netzwerknutzung

Mögliche wirtschaftliche Schäden:

- Kompromittierung von Zugangsdaten und unbefugter Zugriff auf Unternehmensdaten
- Möglicher Schaden: **50.000€** durch Datenverlust, Datenschutzverstöße oder Betriebsstörung

4. Immutable Server-Backup in die Cloud

Ein besonderes Augenmerk galt der Datensicherung: Es wurde eine professionelle Backup-Lösung eingerichtet, die tägliche Sicherungen des Servers in eine Cloudumgebung erstellt – mit Immutable-Technologie. Das bedeutet: Einmal gespeicherte Daten sind nicht mehr veränderbar – selbst bei erfolgreichem Ransomware-Angriff.

Nutzen:

- Schutz vor Datenmanipulation oder -verschlüsselung
- Schnelle Wiederherstellung im Notfall
- Revisions sichere Sicherungen mit geografischer Trennung

Mögliche wirtschaftliche Schäden:

- Totalausfall im Falle eines Ransomware-Angriffs ohne Möglichkeit zur Datenwiederherstellung
- Schaden: **300.000€ oder mehr** durch vollständigen Datenverlust, Betriebsunterbrechung und Imageschäden. Etwaige Insolvenz.

5. Erweiterter Schutz der Microsoft 365 Umgebung

Die Microsoft 365 Umgebung wurde durch eine spezialisierte Cloud-Sicherheitslösung abgesichert (u. a. Anti-Spam, Phishing-Filter, Anomalie-Erkennung, E-Mail-Archivierung). Damit werden gezielte Angriffe (z. B. CEO-Fraud, Passwort-Phishing) zuverlässig erkannt und verhindert.

Mögliche wirtschaftliche Schäden:

- CEO-Fraud oder erfolgreiche Phishing-Angriffe auf Mitarbeitende
- Potenzieller finanzieller Schaden: **5.000 € bis 100.000 €** je nach Vorfall (z. B. durch gefälschte Zahlungsaufforderungen)

Ergebnis: Sicherer, stabiler und skalierbarer IT-Betrieb

Innerhalb weniger Wochen wurde die gesamte IT-Umgebung modernisiert. Das Laubender Architekturbüro profitiert seither von:

- Zuverlässiger Systemverfügbarkeit
- Spürbar höherer Sicherheit im täglichen Betrieb
- Entlastung interner Ressourcen durch Automatisierung
- Deutlich reduzierter Angriffsfläche für Cyberbedrohungen

Die Oberland IT GmbH bleibt weiterhin strategischer Partner und überwacht die Systeme im Rahmen eines kontinuierlichen Servicevertrags.

Jetzt 30 Minuten kostenloses Beratungsgespräch vereinbaren.

Checkliste - Wie sicher ist Ihre IT wirklich?

Mit dieser Checkliste finden Sie es in wenigen Minuten heraus.

Beantworten Sie die folgenden Fragen ehrlich – und erhalten Sie eine erste Einschätzung, ob akuter Handlungsbedarf besteht oder Ihre IT bereits auf einem soliden Fundament steht.

1. Datensicherung

1. Gibt es ein automatisiertes Backup Ihrer geschäftskritischen Daten (Server, Arbeitsplätze, Cloud-Dienste)?

- Ja (0 Punkte)
- Teilweise (2 Punkte)
- Nein (5 Punkte)

2. Wird das Backup regelmäßig geprüft und testweise wiederhergestellt?

- Ja (0 Punkte)
- Gelegentlich (2 Punkte)
- Nie / Weiß ich nicht (4 Punkte)

3. Werden Ihre Backups an einem getrennten, sicheren Ort gespeichert (z. B. extern oder Cloud)?

- Ja (0 Punkte)
- Lokal aber getrennt (1 Punkt)
- Nur am gleichen Standort (3 Punkte)

2. Firewall & Netzwerksicherheit

1. Verfügt Ihr Unternehmen über eine professionelle, zentral verwaltete Firewall?

- Ja (0 Punkte)
- Veraltet / keine zentrale Verwaltung (3 Punkte)
- Keine Ahnung / Nein (6 Punkte)

2. Gibt es eine Trennung zwischen internen Netzwerken und Gast-/IoT-Zugängen?

- Ja (0 Punkte)
- Teilweise (1 Punkt)
- Nein (2 Punkte)

3. Wird der Netzwerkverkehr regelmäßig überwacht oder protokolliert (z. B. durch ein IT-Systemhaus)?

- Ja (0 Punkte)
- Teilweise (1 Punkt)
- Nein / Keine Ahnung (3 Punkte)

3. E-Mail-Sicherheit

1. Gibt es einen aktiven Spam- und Virenfiler für eingehende E-Mails?

- Ja (0 Punkte)
- Nicht sicher (2 Punkte)
- Nein (4 Punkte)

2. Erkennen Mitarbeitende Phishing- oder Fake-Mails zuverlässig?

- Ja (0 Punkte)
- Unsicher (2 Punkte)
- Nein (5 Punkte)

3. Ist eine E-Mail-Verschlüsselung für sensible Kommunikation im Einsatz?

- Ja (0 Punkte)
- Nur bei Bedarf (2 Punkte)
- Nein (3 Punkte)

4. Systemaktualität (Windows 10 / Altgeräte)

1. Nutzen Sie noch Arbeitsplätze mit Windows 10 (Support-Ende Oktober 2025)?

- Nein (0 Punkte)
- Teilweise (5 Punkte)
- Überwiegend (15 Punkte)

2. Sind Server, Arbeitsplätze und mobile Geräte auf aktuellem Softwarestand (Updates)?

- Ja (0 Punkte)
- Teilweise (2 Punkte)
- Nein / unklar (4 Punkte)

3. Gibt es einen konkreten Plan zur Umstellung auf Windows 11 oder ein alternatives System?

- Ja (0 Punkte)
- In Vorbereitung (2 Punkte)
- Nein (4 Punkte)

5. Schulung & IT-Verhalten der Mitarbeitenden

1. Werden alle Mitarbeitenden regelmäßig zu IT-Sicherheit geschult?

- Ja (0 Punkte)
- Selten / unregelmäßig (2 Punkte)
- Nie (5 Punkte)

2. Gibt es klare IT-Richtlinien zu Passwörtern, Gerätenutzung und Datenschutz?

- Ja (0 Punkte)
- Teilweise / mündlich geregelt (1 Punkt)
- Nein (3 Punkte)

3. Wissen Mitarbeitende, was im Fall eines IT-Vorfalles zu tun ist (z. B. Phishing-Versuch, Ransomware)?

- Ja (0 Punkte)
- Unsicher (2 Punkte)
- Nein (4 Punkte)

Auf der nächsten Seite erfahren Sie, was Ihr Ergebnis bedeutet - und ob in Ihrem Unternehmen akuter Handlungsbedarf besteht. Die Auswertung hilft Ihnen dabei, die Einschätzung Ihrer IT-Situation realistisch einzuordnen und erste Schritte abzuleiten.

**Viele Punkte und Handlungsbedarf?
Dann lassen Sie uns gemeinsam Ihre IT checken.**

0-14 Punkte

Kein akuter Handlungsbedarf

Ihre IT ist gut aufgestellt. Bleiben Sie dennoch wachsam und prüfen Sie regelmäßig Sicherheitsstandards, besonders bei Systemwechseln.

15-35 Punkte

Handlungsbedarf vorhanden

Ihre IT weist Schwachstellen auf, die zu Problemen führen können. Lassen Sie Ihr System professionell prüfen und optimieren Sie gezielt.

36+ Punkte

Dringender Handlungsbedarf

Ihre IT ist in einem kritischen Zustand. Es besteht ein erhebliches Risiko für Ausfälle, Datenverlust oder Sicherheitsvorfälle. Handeln Sie schnell, um wirtschaftliche Schäden zu vermeiden.

Fazit und der nächste Schritt

In diesem E-Book haben wir die häufigsten IT-Fehler beleuchtet, die wir in Unternehmen regelmäßig sehen.

Sie haben erfahren, wie gravierend die Auswirkungen sein können, wenn z. B. Datensicherungen fehlen, Firewalls unzureichend sind oder Mitarbeitende ungeschult bleiben. Mit der Selbst-Checkliste konnten Sie einschätzen, wie gut Ihr Unternehmen aktuell aufgestellt ist. Vielleicht haben Sie dabei festgestellt, dass bereits vieles gut läuft - oder aber, dass in mehreren Bereichen dringender Handlungsbedarf besteht.

Wichtig: Ab Oktober 2025 wird es keine Sicherheits- und Funktionsupdates mehr für Windows 10 geben. Ab dann sind alle Unternehmen, welche Win10 nutzen, enorm gefährdet für Cyberangriffe. Sollten Sie noch mit Windows 10 arbeiten, empfehlen wir DRINGEND, mit uns in Verbindung zu treten!

**Kostenlose
30-minütige
Remote-Analyse
Ihrer IT-Situation**



Wenn Sie beim Selbsttest über 14 Punkte erreicht haben, empfehlen wir Ihnen: Warten Sie nicht, bis ein Fehler zum Problem wird. Nutzen Sie unsere Erfahrung und lassen Sie Ihre IT durch einen unserer Experten unverbindlich und neutral unter die Lupe nehmen - direkt per Remote-Zuschaltung.

Sie erhalten in diesem Termin:

- ✓ Eine fachliche Ersteinschätzung Ihrer individuellen IT-Lage
- ✓ Konkrete Hinweise auf Schwachstellen oder Handlungsbedarf
- ✓ Empfehlungen, wie Sie Ihre IT stabiler und sicherer aufstellen können

Vereinbaren Sie jetzt Ihr kostenfreies Erstgespräch - bevor aus kleinen Lücken große Schäden werden.

 **08821-752 68 68**

 **kontakt@oberland.it**

 **www.oberland.it**



Hier klicken
für einen
IT-Check

