

Checkliste:

IT-Notfall-Check für den Mittelstand

30 Fragen, die zeigen, ob Ihr Unternehmen nach einem IT-Ausfall oder Cyberangriff schnell wieder arbeitsfähig wäre.

Ein Cyberangriff oder ein schwerer IT-Ausfall trifft Unternehmen meist unerwartet. Innerhalb weniger Stunden können Server, Arbeitsplätze und wichtige Geschäftsprozesse stillstehen. Die eigentliche Herausforderung beginnt jedoch oft erst danach: Wie schnell lässt sich der Geschäftsbetrieb wiederherstellen?

Mit diesem IT-Notfall-Check erkennen Sie in wenigen Minuten, wie gut Ihr Unternehmen auf einen IT-Ausfall oder Cyberangriff vorbereitet ist. Kreuzen Sie einfach alle Aussagen an, die bereits auf Ihr Unternehmen zutreffen. Jedes leere Kästchen weist auf einen Bereich hin, in dem Sie Ihre Ausfallsicherheit weiter verbessern sollten.

1. Datensicherung & Wiederherstellung

- ☐ Werden Ihre Backups täglich automatisch erstellt?
- ☐ Werden die Sicherungen regelmäßig auf Fehler geprüft?
- ☐ Wurde innerhalb der letzten zwölf Monate eine vollständige Wiederherstellung getestet?
- ☐ Gibt es mindestens eine Datensicherung außerhalb Ihres Unternehmens (Offline oder Cloud)?
- ☐ Sind auch Microsoft 365, E-Mails und Cloud-Daten Bestandteil Ihrer Datensicherung?

2. Schutz der IT-Systeme

- ☐ Werden Sicherheitsupdates zeitnah installiert?
- ☐ Sind Server und Arbeitsplätze mit aktueller Schutzsoftware ausgestattet?
- ☐ Ist eine Firewall professionell eingerichtet und aktuell?
- ☐ Nutzen alle Mitarbeitenden eine Multi-Faktor-Authentifizierung für wichtige Zugänge?
- ☐ Werden ungewöhnliche Aktivitäten im Netzwerk automatisch erkannt?

3. Benutzer & Zugriffsrechte

- ☐ Haben Mitarbeitende nur die Berechtigungen, die sie wirklich benötigen?
- ☐ Werden ehemalige Benutzerkonten sofort deaktiviert?
- ☐ Werden Administratorrechte nur an wenige Personen vergeben?
- ☐ Werden Passwortrichtlinien regelmäßig überprüft?
- ☐ Gibt es ein Verfahren für den sicheren Umgang mit mobilen Geräten?

4. Organisation im Notfall

- ☐ Gibt es einen dokumentierten IT-Notfallplan?
- ☐ Sind Verantwortlichkeiten eindeutig festgelegt?
- ☐ Wissen Mitarbeitende, wen sie im Ernstfall informieren müssen?
- ☐ Sind wichtige Ansprechpartner auch außerhalb der Geschäftszeiten erreichbar?
- ☐ Liegen wichtige Zugangsdaten sicher und dokumentiert vor?

5. Betrieb & Überwachung

- ☐ Werden Server und zentrale Systeme permanent überwacht?
- ☐ Werden Ausfälle automatisch gemeldet?
- ☐ Gibt es definierte Reaktionszeiten bei Störungen?
- ☐ Werden Protokolle regelmäßig ausgewertet?
- ☐ Werden kritische Systeme regelmäßig überprüft?

6. Cyberangriff & Krisenmanagement

- ☐ Wissen Sie, welche Systeme im Ernstfall zuerst wiederhergestellt werden müssen?
- ☐ Gibt es einen Ansprechpartner für IT-Forensik oder Cyberversicherung?
- ☐ Wissen Mitarbeitende, wie sie sich bei einem Verdacht auf Schadsoftware verhalten sollen?
- ☐ Wurde bereits einmal ein IT-Notfall durchgespielt?
- ☐ Haben Sie einen externen IT-Partner, der Sie im Krisenfall kurzfristig unterstützen kann?

Ihre Auswertung

Angekreuzte Aussagen	Einschätzung
26–30	Sehr gute Vorbereitung. Ihre IT verfügt über eine stabile Grundlage und ist auch für kritische Situationen gut aufgestellt.
18–25	Gute Basis. Einzelne Schwachstellen sollten überprüft werden, um Risiken weiter zu reduzieren.
10–17	Erhöhter Handlungsbedarf. Mehrere Schwächen könnten im Ernstfall zu längeren Ausfällen führen.
0–9	Akuter Handlungsbedarf. Ihre Organisation wäre auf einen größeren IT-Ausfall oder Cyberangriff vermutlich nur unzureichend vorbereitet.

Nächster Schritt

Wissen Sie wirklich, wie schnell Ihr Unternehmen nach einem IT-Ausfall oder Cyberangriff wieder arbeitsfähig wäre?

Diese Checkliste liefert Ihnen eine erste Einschätzung Ihrer aktuellen Situation. Sie kann jedoch eine individuelle Analyse Ihrer IT-Umgebung nicht ersetzen.

SystemFAKTOR unterstützt mittelständische Unternehmen dabei, ihre IT so aufzustellen, dass Ausfälle minimiert und Geschäftsprozesse auch im Ernstfall schnell wiederhergestellt werden können. Gemeinsam analysieren wir Ihre Backup-Strategie, Wiederherstellungsfähigkeit, Sicherheitsmaßnahmen und organisatorischen Abläufe und zeigen Ihnen konkret, wo Handlungsbedarf besteht und welche Maßnahmen die größte Wirkung erzielen.

Nehmen Sie jetzt Kontakt auf:

Tel.: 02173 26482-0

E-Mail: info@systemfaktor.de