UKNS IT-Premium Services

IT-Notfallplan für Unternehmen

Checkliste für Cyberangriff, Serverausfall, E-Mail-Konto-Missbrauch und Datenverlust in kleinen und mittelständischen Unternehmen.

Kostenlose Praxisvorlage für Leipziger Unternehmen

Wenn kritische IT-Systeme ausfallen, zählt ein klarer Ablauf. Diese Checkliste hilft Geschäftsführung, Office-Management und IT-Verantwortlichen, die ersten Minuten strukturiert zu überbrücken, Schäden zu begrenzen und den Wiederanlauf vorzubereiten.

Notfallkontakt UKNS: 0341 24820174 | https://ukns.eu/it-notfallplan-unternehmen-leipzig/

1. Die ersten 15 Minuten

Ziel: Kontrolle gewinnen, Schaden begrenzen, Beweise sichern und Kommunikation bündeln.

- [ ] Ereignis protokollieren: Uhrzeit, betroffene Systeme, Symptome und erste Beobachtungen notieren.
- [ ] Nicht hektisch neu starten: Bei Angriff, Ransomware oder Datenverlust können Neustarts Spuren zerstören.
- [ ] Betroffene Geräte isolieren: Netzwerk trennen, WLAN deaktivieren, aber Geräte möglichst eingeschaltet lassen.
- [ ] Koordination festlegen: Eine Person entscheidet, eine dokumentiert, eine kommuniziert.
- [ ] Externe IT informieren: Screenshots, Fehlermeldungen und betroffene Nutzer bereithalten.

2. Rollen und Kontakte

Rolle	Name / Kontakt	Aufgabe
Geschäftsführung		Entscheidet über Betriebsunterbrechung, Kommunikation, Budget und Meldewege.
IT-Koordination		Steuert Dienstleister, interne IT und Wiederanlauf der Systeme.
Datenschutz		Prüft personenbezogene Daten, Dokumentation und mögliche Meldepflichten.
Kommunikation		Informiert Mitarbeitende, Kunden und Lieferanten abgestimmt und einheitlich.
Externer IT-Partner	UKNS: 0341 24820174	Analyse, Eindämmung, Wiederherstellung und technische Dokumentation.

3. Checkliste nach Szenario

Szenario	Sofortmaßnahmen
Cyberangriff oder Ransomware	[ ] Rechner vom Netzwerk trennen, nicht ausschalten [ ] Keine Lösegeldkommunikation ohne Beratung starten [ ] Passwörter betroffener Konten zurücksetzen, MFA prüfen [ ] Weiterleitungen und unbekannte Admin-Konten kontrollieren [ ] Backup-Status prüfen, bevor Wiederherstellungen starten
Server- oder Netzwerkausfall	[ ] Betroffene Standorte, Dienste und Nutzergruppen notieren [ ] Strom, Internet, Firewall, Switches und Serverstatus dokumentieren [ ] Keine Mehrfach-Neustarts ohne Diagnose durchführen [ ] Priorisierte Dienste festlegen: Telefonie, E-Mail, ERP, Dateien
Datenverlust	[ ] Nicht weiter auf betroffene Datenträger schreiben [ ] Gelöschte Ordner, Zeitpunkt und Nutzer festhalten [ ] Cloud-Papierkorb, Versionierung und Backup-Snapshots prüfen [ ] Keine Reparaturtools auf Originaldatenträgern ausführen
E-Mail-Konto kompromittiert	[ ] Konto sperren oder Passwort sofort ändern [ ] MFA zurücksetzen und neue Geräte prüfen [ ] Weiterleitungsregeln, App-Passwörter und OAuth-Freigaben entfernen [ ] Team vor Folge-Mails und Zahlungsbetrug warnen

4. Vorbereitung vor dem Ernstfall

- [ ] Aktuelle Systemliste mit Servern, Cloud-Diensten, Netzwerkgeräten und kritischen Anwendungen pflegen.
- [ ] Backup-Konzept mit Wiederherstellungstest, Aufbewahrungsfristen und Offline- oder Immutable-Kopie dokumentieren.
- [ ] Admin-Konten mit MFA, Notfallzugängen und sauberer Rechtevergabe absichern.
- [ ] Kontaktliste für Geschäftsführung, IT, Datenschutz, Versicherung, Hosting, Telefonie und Schlüsselpersonen aktuell halten.
- [ ] Kommunikationsvorlagen für Mitarbeitende, Kunden und Lieferanten vorbereiten.
- [ ] Festlegen, welche Systeme innerhalb von 4, 24 und 72 Stunden wieder verfügbar sein müssen.

5. Wiederanlauf priorisieren

Priorität	System / Prozess	Max. Ausfallzeit	Verantwortlich
1			
2			
3			
4			

UKNS unterstützt Unternehmen in Leipzig bei Backup-Prüfung, Sicherheitscheck, Microsoft-365-Absicherung, Notfallhandbuch und Wiederanlaufplanung.

Kontakt: 0341 24820174 | https://ukns.eu/kontakt/