

CHECKLISTE · NOTFALLPLAN

IT-Notfallplan: Die Minimalversion für KMU

Rollen, Erstmaßnahmen, Meldewege und Wiederanlauf – kompakt genug, um im Ernstfall wirklich genutzt zu werden.

DAS ERHALTEN SIE

- Einseitige Notfallkarte zum Ausdrucken
- Schweregrade, Rollen und Kommunikationskette
- Meldefristen: DSGVO und NIS2 im Überblick
- Wiederanlauf-Reihenfolge, Test-Intervalle, Checkliste

AUF EINEN BLICK

Für	**Geschäftsleitung und IT-Verantwortliche**
Zeitbedarf	**ca. 2 Stunden Erstellung, 1 Stunde Übung**
Stand	**16. November 2026**
Version	**2.0**

Unverbindliche Praxishilfe – keine Rechtsberatung, kein Audit

1 Grundsätze

> Im Notfall zählt Klarheit: Wer entscheidet, wen man erreicht, welche Systeme zuerst wiederhergestellt werden und wie Informationen verlässlich geteilt werden.

- **Kurz und offline**: Der Plan muss ohne E-Mail, Dateiablage und Anmeldedienste verfügbar sein – ausgedruckt und an einem zweiten Ort.
- **Rollen statt Personen**: Jede Rolle hat eine Vertretung.
- **Geübt**: Ein nie geübter Plan funktioniert im Ernstfall selten.
- **Anschlussfähig**: Für ein vollständiges Notfallmanagement bietet der BSI-Standard 200-4 (Business Continuity Management) die Methodik; diese Minimalversion ist ein Einstieg.

Schweregrade

Stufe	Beispiel	Reaktion
1 – Störung	Einzelner Arbeitsplatz oder Dienst gestört, Umgehung möglich	Regulärer Support
2 – Schwerer Vorfall	Wichtiger Dienst ausgefallen oder Verdacht auf Kompromittierung eines Kontos	Incident Lead informieren, Lagebewertung innerhalb einer Stunde
3 – Notfall	Kritische Prozesse stehen; Ransomware; Datenabfluss wahrscheinlich	Krisenstab, Geschäftsleitung sofort, externe Unterstützung, Meldepflichten prüfen

Notfallkarte – zum Ausdrucken

Bei Verdacht auf einen IT-Sicherheitsvorfall

- **Ruhe bewahren** – nichts löschen, nichts neu installieren, keine Lösegeldkommunikation.
- **Betroffenes Gerät vom Netzwerk trennen** (Kabel ziehen, WLAN aus) – **nicht ausschalten**, sofern nicht anders angewiesen.
- **Sofort melden** an die unten genannte Stelle: Was ist passiert? Wann? Welches Gerät? Was wurde schon getan?
- **Notizen machen** mit Uhrzeit; Fotos von Bildschirmmeldungen.
- Keine Zugangsdaten herausgeben; Kommunikation über Telefon statt über möglicherweise betroffene Systeme.

Incident Lead (Name, Telefon) _____

Vertretung (Name, Telefon) _____

IT-Dienstleister / Notfallnummer _____

Geschäftsleitung (Telefon) _____

Datenschutzbeauftragte/r _____

Cyber-Versicherung (Policen-Nr., Hotline) _____

Polizei: Zentrale Ansprechstelle Cybercrime (ZAC) des Landes _____

Treffpunkt / Ersatzkommunikation _____

Bewahren Sie eine ausgedruckte Fassung dieses Dokuments außerhalb der IT-Systeme auf.

2 Rollen und Kommunikationskette

Rolle	Aufgabe	Name / Vertretung
Incident Lead	Koordiniert, bewertet, dokumentiert, eskaliert	_____ / _____
Geschäftsleitung	Entscheidet über Abschaltungen, externe Hilfe, Kommunikation, Meldungen	_____ / _____
Technik	Eindämmung, Beweissicherung, Wiederherstellung	_____ / _____
Datenschutz	Bewertet Personenbezug und Meldepflicht	_____ / _____
Kommunikation	Mitarbeitende, Kunden, Lieferanten, ggf. Presse	_____ / _____

Wer wird informiert?

Intern	Extern	Behörden & Stellen
Geschäftsleitung, betroffene Abteilungen, alle Mitarbeitenden (über Ersatzkanal)	IT-Dienstleister, Cloud-/Softwareanbieter, Cyber-Versicherung, ggf. Kunden und Lieferanten	Datenschutzaufsicht, ggf. BSI (NIS2), Polizei (ZAC)

3 Meldefristen im Überblick

Regelung	Wann	Frist
DSGVO Art. 33	Verletzung des Schutzes personenbezogener Daten, sofern ein Risiko für Betroffene nicht unwahrscheinlich ist	Meldung an die Aufsichtsbehörde unverzüglich, möglichst **binnen 72 Stunden** nach Bekanntwerden
DSGVO Art. 34	Voraussichtlich hohes Risiko für Betroffene	Benachrichtigung der Betroffenen unverzüglich
NIS2 / BSIG (nur betroffene Einrichtungen)	Erheblicher Sicherheitsvorfall	Frühwarnung **binnen 24 Stunden**, Meldung binnen 72 Stunden, Abschlussbericht in der Regel binnen eines Monats an das BSI
Verträge & Versicherung	Je nach Vertrag mit Kunden, Dienstleistern und Versicherer	Fristen und Obliegenheiten vorab heraussuchen und hier notieren

Rechtliche Bewertung

Ob eine Meldepflicht besteht, ist eine Einzelfallentscheidung. Binden Sie Datenschutzbeauftragte und rechtliche Beratung früh ein. Bei Erpressung oder möglicher Straftat: Polizei einschalten; die Zentralen Ansprechstellen Cybercrime (ZAC) der Länder sind auf Unternehmen ausgerichtet.

4 Eindämmung und Wiederanlauf

Erste Stunden

- Betroffene Systeme nach festgelegtem Verfahren isolieren; bei weiträumigem Befall Internetverbindung kontrolliert trennen.
- Kompromittierte Konten sperren, Kennwörter und Sitzungen zurücksetzen – zuerst Administrator- und Dienstkonten.
- Beweise sichern: Protokolle, betroffene Systeme (Abbild), Zeitleiste. Keine voreilige Neuinstallation.
- Prüfen, ob Backups unversehrt sind, bevor sie mit dem Netz verbunden werden.

Wiederanlauf-Reihenfolge (Beispiel – an Abhängigkeiten anpassen)

#	System	Ziel-RTO	Abhängig von
1	Netzwerk, Firewall, Internet	_____	—
2	Identität (Domäne / Entra ID), DNS, DHCP	_____	1
3	Kernserver und Speicher	_____	1, 2
4	Geschäftskritische Anwendungen (ERP, Buchhaltung)	_____	2, 3
5	E-Mail und Zusammenarbeit	_____	2
6	Arbeitsplätze (sauber neu aufgesetzt)	_____	2–5

Vor dem Wiederanschluss

Ursache verstanden und beseitigt? Zugangsdaten erneuert? Systeme aus vertrauenswürdigen Quellen wiederhergestellt? Überwachung aktiv?

5 Übung, Pflege und Checkliste

Aktivität	Intervall (Empfehlung)
Kontaktliste prüfen	vierteljährlich und bei Personalwechsel
Tabletop-Übung (Planspiel, z. B. Ransomware-Szenario)	jährlich
Wiederherstellung kritischer Systeme testen	mindestens jährlich
Plan überprüfen und Version aktualisieren	jährlich und nach jedem Vorfall
Ausgedruckte Exemplare austauschen	nach jeder Änderung

	Prüfpunkt	Verantwortlich	Termin / Nachweis
VORBEREITUNG			
☐	Kritische Prozesse und Systeme sind priorisiert.	_____	_____
☐	RTO/RPO und Wiederanlauf-Reihenfolge sind vereinbart.	_____	_____
☐	Incident Lead und Vertretung sind benannt.	_____	_____
☐	Notfallkarte ist ausgefüllt, ausgedruckt und verteilt.	_____	_____
☐	Meldefristen und Ansprechpartner sind notiert.	_____	_____
FÄHIGKEIT			
☐	Isolierungs- und Beweissicherungsverfahren sind dokumentiert.	_____	_____
☐	Backups und Wiederherstellungsmedien sind erreichbar und getestet.	_____	_____
☐	Ersatzkommunikation (Telefonliste, Messenger, Treffpunkt) ist festgelegt.	_____	_____
PFLEGE			
☐	Plan wurde mit Mitarbeitenden geübt.	_____	_____
☐	Nachbereitung und nächste Überprüfung sind terminiert.	_____	_____

Quellen & weiterführende Referenzen

- BSI-Standard 200-4 „Business Continuity Management“ (Nachfolger des BSI-Standards 100-4), bsi.bund.de
- BSI: Maßnahmenkatalog „Ransomware“ und IT-Notfallkarte „Verhalten bei IT-Notfällen“, bsi.bund.de
- Verordnung (EU) 2016/679 (DSGVO), Art. 33 und 34
- Richtlinie (EU) 2022/2555 (NIS2) und deutsches NIS2-Umsetzungsgesetz (BSIG) – Meldepflichten für betroffene Einrichtungen
- Polizei: Zentrale Ansprechstellen Cybercrime (ZAC) der Länder, polizei.de
- KONTORIT Wissen: „Backup-Strategie 3-2-1“ und „IT-Grundschutz für KMU“ (kontorit.de/whitepaper)

Unterstützung gewünscht? KONTORIT begleitet kleine und mittlere Unternehmen in Hamburg bei Bestandsaufnahme, Umsetzung und Betrieb. Anfrage: **kontorit.de/kontakt** · E-Mail: **support@kontorit.de**

Dieses Dokument ist eine allgemeine, unverbindliche Orientierungshilfe. Es ersetzt keine individuelle Beratung, kein Sicherheitsaudit, keine Rechts- oder Steuerberatung und keinen Zertifizierungsnachweis. Produktfunktionen, Lizenzen und rechtliche Anforderungen ändern sich; prüfen Sie den aktuellen Stand anhand der genannten Quellen und Ihrer konkreten Umgebung. Genannte Marken gehören ihren jeweiligen Inhabern. © 2026 KONTORIT · Stand 16. November 2026 · Version 2.0