IT-NOTFALLPLAN

Für kleine und mittlere Unternehmen

CYBERANGRIFF ODER IT-AUSFALL?
Nicht in Panik geraten. Nicht improvisieren. Erst sichern, dann handeln.

Die 6 Schritte im Notfall

1 STOPP

Arbeit am betroffenen System einstellen. Keine Dateien löschen, keine Neuinstallation.

2 MELDEN

Interne Notfallperson und IT-Dienstleister informieren. Cyberverdacht ausdrücklich nennen.

3 ISOLIEREN

Betroffene Geräte – soweit sinnvoll – vom Netzwerk trennen. WLAN deaktivieren / Kabel ziehen.

4 SICHERN

Zeitpunkte, Fehlermeldungen, E-Mails und Screenshots dokumentieren. Nichts unnötig verändern.

5 ANALYSIEREN

Ursache und Ausmaß durch IT bzw. IT-Sicherheit prüfen lassen.

6 WIEDERHERSTELLEN

Systeme erst nach Prüfung und Freigabe wieder produktiv nutzen.

Sofortmaßnahmen

- **Verdächtige E-Mail geöffnet?** Netzwerkverbindung trennen und IT informieren.
- **Ransomware / verschlüsselte Dateien?** Betroffene Systeme isolieren; nicht selbst bereinigen.
- **Konto übernommen?** Zugang sperren, Sitzungen beenden und Passwörter von einem sauberen Gerät ändern.
- **Server / Internet ausgefallen?** IT-Dienstleister kontaktieren und Notbetrieb organisieren.

Was Sie vermeiden sollten

- Nicht auf Erpresserforderungen reagieren, bevor der Vorfall bewertet wurde.
- Keine Dateien oder Logs löschen.
- Keine Systeme eigenmächtig neu installieren.
- Keine verdächtigen Anhänge oder Links erneut öffnen.
- Keine öffentlichen Aussagen ohne Abstimmung.

Wichtig

Backups nicht blind zurückspielen. Erst prüfen lassen, ob der Angreifer noch Zugriff hat und ob die Sicherungen sauber sind.

Wer entscheidet?

Interne Notfallperson: _____
Stellvertretung: _____
IT-Dienstleister: _____
Notfallnummer: _____

Notfall-Checkliste

Diese Seite kann ausgedruckt und ausgefüllt werden.

1. Was ist passiert?

■ **Technischer Ausfall** Server, Internet, Arbeitsplatz etc.	■ **Verdächtiger Sicherheitsvorfall** Phishing, Malware, ungewöhnliche Anmeldung	■ **Bestätigter Cyberangriff** Ransomware, Datendiebstahl, Kontoübernahme

2. Dokumentieren

Datum / Uhrzeit des Vorfalls:	_____
Betroffene Systeme / Geräte:	_____
Betroffene Benutzer / Konten:	_____
Was wurde beobachtet?	_____
_____	_____

3. Wichtige Kontakte

Geschäftsführung:	_____
IT / Systemhaus:	_____
IT-Sicherheitsdienstleister:	_____
Datenschutz:	_____
Cyber-Versicherung:	_____
Rechtsberatung:	_____

4. Wiederanlauf – erst wenn geprüft

■ Ursache / Angriffspfad bekannt oder eingegrenzt	■ Angreiferzugänge geschlossen
■ Systeme und Backups geprüft	■ Passwörter / privilegierte Zugänge abgesichert
■ Datenschutz / rechtliche Meldepflichten bewertet	■ Wiederherstellung abgestimmt

VORBEREITUNG IST DER BESTE NOTFALLPLAN
Kritische Systeme kennen · Backups testen · Notfallkontakte ausdrucken · Zuständigkeiten festlegen · Notfallplan regelmäßig üben

Wave Security GmbH

IT-Sicherheit muss nicht kompliziert sein – wir machen sie verständlich und effektiv. Wave Security unterstützt KMU unter anderem mit Sicherheitsanalysen und Risiko-Bewertungen, Sicherheitsstrategien, Mitarbeiterschulungen, Penetrationstests und Unterstützung bei Incident-Response-Maßnahmen.