

IT-NOTFALLPLAN



REGEL NR. 1

Ruhe bewahren. Keine Panik.

1 Nicht herunterfahren

2 Nichts löschen

3 Karte unten befolgen

1 RANSOMWARE

Lösegeldforderung oder Sperrbildschirm

- 1 **Netzwerkkabel ziehen** und WLAN abschalten
- 2 **Gerät anlassen**, Bildschirm fotografieren
- 3 **IT und Geschäftsführung** sofort informieren
- 4 **Andere warnen**: keine Datei vom Server öffnen
- 5 **Polizei verständigen**, Ansprechstelle Cybercrime

NIEMALS zahlen, antworten oder herunterfahren

2 SERVERAUSFALL

Server oder Software reagiert nicht

- 1 **Prüfen**: nur mein Gerät oder alle betroffen?
- 2 **Offene Arbeit** lokal sichern, solange möglich
- 3 **Uhrzeit und Symptome** notieren
- 4 **IT informieren**, Ausfall genau beschreiben
- 5 **Ersatzablauf** nutzen, Papier oder Telefon

NIEMALS Server selbst neu starten oder abschalten

3 DATENVERLUST

Dateien fehlen oder sind gelöscht

- 1 **Arbeit einstellen** am betroffenen Gerät
- 2 **Papierkorb** und Versionsverlauf prüfen
- 3 **Cloud prüfen**: Papierkorb in OneDrive oder SharePoint
- 4 **Notieren**: Dateiname, Ordner, letzte Änderung
- 5 **IT informieren** für die Rücksicherung

NIEMALS eigene Rettungsprogramme starten

4 NETZWERK

Internet oder Netzwerk ausgefallen

- 1 **Prüfen**: nur mein Gerät oder alle betroffen?
- 2 **Statusleuchten** an Router und Switch prüfen
- 3 **WLAN trennen** und neu verbinden
- 4 **Störung prüfen** beim Provider, Nummer unten
- 5 **Länger als 15 Minuten?** IT informieren

NIEMALS Netzwerkgeräte umstecken oder zurücksetzen

5 PHISHING

Verdächtige E-Mail oder verdächtiger Anruf

- 1 **Nicht klicken**: keine Links, keine Anhänge
- 2 **Schon geklickt?** Kabel ziehen und IT anrufen
- 3 **Angeblicher IT-Anruf?** Auflegen und selbst zurückrufen
- 4 **Passwort ändern**, überall wo es gleich lautet
- 5 **Weiterleiten**: E-Mail als Anhang an die IT

NIEMALS Zugangsdaten per E-Mail oder Telefon nennen

6 MALWARE

PC langsam, Pop-ups, fremde Programme

- 1 **Netzwerkkabel ziehen** und WLAN abschalten
- 2 **Gerät anlassen**, Spuren bleiben erhalten
- 3 **Notieren**: seit wann? was zuletzt installiert?
- 4 **IT informieren**, Symptome genau beschreiben
- 5 **USB-Sticks** am Gerät liegen lassen, nicht weitergeben

NIEMALS selbst deinstallieren oder Virencans starten

NOTFALLKONTAKTE

bitte ausfüllen und aktuell halten

FUNKTION	NAME ODER FIRMA	TELEFON	E-MAIL ODER WEB
IT-Notfallhilfe	Lisser IT-Systemhaus	04408 999 99 99	notfall@lisser-it.de
Geschäftsführung			
IT-Ansprechpartner			
Internetprovider			
Cyberversicherung			
Polizei ZAC	ZAC Niedersachsen, LKA	0511 9873 6230	lka.polizei-nds.de
BSI Hotline	Bundesamt für Sicherheit	0800 274 1000	bsi.bund.de

NIEMAND ERREICHBAR?



Scannen: Notfallhilfe anrufen,
per WhatsApp melden oder
Nummer speichern.

IMMER GILT

- Verdächtige E-Mails und Links niemals öffnen
- Unbekannte USB-Sticks nicht anschließen
- Passwörter nie am Bildschirm notieren
- Zugangsdaten auch offline hinterlegen
- Unsicher? Erst fragen, dann klicken

NACH DEM VORFALL

- Vorfall dokumentieren: was, wann, wer
- Im Team besprechen und Ablauf verbessern
- **Daten betroffen?** 72 Stunden Meldefrist beachten
- Diesen Aushang aktualisieren

VORFALL NOTIEREN

Datum und Uhrzeit _____
Was ist passiert _____

Gerät _____
Bemerkt von _____

Stand _____ Verantwortlich _____ Nächste Prüfung _____