NOTFALL · CHECKLISTE

Ransomware entdeckt.
Was jetzt zählt – und was schadet.

Die ersten Entscheidungen bestimmen, wie teuer der Vorfall wird. Diese Checkliste ordnet sie nach Zeit: sofort, in den ersten Stunden, in den ersten Tagen. Ausdrucken und in den Notfallordner legen.

WER TRIFFT ES	WAS ES KOSTET	WAS ZUERST ZÄHLT
Rund 80 % der Ransomware-Fälle treffen kleine und mittlere Firmen	Ø rund 1,2 Mio. € Wiederherstellung je Vorfall in Deutschland	Nicht ausschalten – isolieren. Beweise gehen sonst verloren

0–15 MIN	15–60 MIN	1–4 STD	BIS 24 STD	AB TAG 2
Bestätigen, alarmieren, isolieren	Ausmaß eingrenzen, Backups schützen	Beweise sichern, Einbruchsweg suchen	Melden, kommunizieren	Sauber wiederanlaufen, härten

Schritt 1 Sofort – die ersten 15 Minuten

ERLEDIGT?

- ☐ **Fund bestätigen:** Lösegeldforderung, umbenannte Dateien oder Alarm gegengeprüft
- ☐ **Betroffene Systeme vom Netz trennen** – Kabel ziehen, WLAN aus, Ports sperren
- ☐ **Backups sofort schützen**: Verbindung trennen, Aufbewahrung sperren, Löschrechte entziehen
- ☐ **Krisenstab alarmieren** und Erreichbarkeit über einen **alternativen Kanal** sicherstellen (nicht über die betroffene Umgebung)
- ☐ **Systeme eingeschaltet lassen.** Ausschalten vernichtet flüchtige Spuren im Arbeitsspeicher
- ☐ **Privilegierte Konten sichern**: Passwörter der Admin- und Dienstkonten ändern, Sitzungen beenden

DIESE FÜNF FEHLER KOSTEN AM MEISTEN

- ✕ Betroffene Rechner **neu starten oder ausschalten** – Speicherspuren und Schlüssel gehen verloren
- ✕ Verschlüsselte Dateien **löschen** oder blind Entschlüsselungs-Tools starten
- ✕ Nach außen kommunizieren, **bevor Umfang und Datenabfluss geklärt** sind
- ✕ Sich mit **Domänen-Admin-Konten** an infizierten Systemen anmelden
- ✕ **Ohne Rechtsbeistand** Kontakt zu den Erpressern aufnehmen

Bildmotiv: KI-generiertes Symbolbild

Schritt 2 Erste Stunden – Ausmaß und Beweise

ABGEHAKT?

- [ ] **Umfang bestimmen:** welche Systeme, Standorte, Konten und Daten sind betroffen
- [ ] **Ransomware-Familie identifizieren** – manche Varianten haben freie Entschlüsselungswerkzeuge
- [ ] **Datenabfluss prüfen** – doppelte Erpressung ist der Regelfall, nicht die Ausnahme
- [ ] **Forensische Sicherung** vor Wiederherstellung: Arbeitsspeicher, Datenträger-Images, Logdateien
- [ ] **Einbruchsweg suchen**: exponierte Fernzugänge, Phishing, ungepatchte Schwachstelle, Dienstleister
- [ ] **Lückenlos protokollieren**: wer hat wann was entschieden und getan (zählt später vor Behörde und Versicherer)

Schritt 3 Melden – Fristen laufen ab Kenntnis

ABGEHAKT?

- [ ] **BSI: Erstmeldung binnen 24 Stunden**, Detailbericht binnen 72 Stunden (sofern NIS2 greift)
- [ ] **Polizei / Zentrale Ansprechstelle Cybercrime** des Landes einschalten
- [ ] **Kunden, Partner und Belegschaft** nach abgestimmtem Sprachregelungs-Entwurf informieren
- [ ] **Datenschutzbehörde: binnen 72 Stunden**, wenn personenbezogene Daten betroffen sind
- [ ] **Cyber-Versicherung** unverzüglich informieren – Obliegenheiten prüfen, bevor Kosten entstehen
- [ ] **KRITIS-Betreiber:** erhebliche Störungen zusätzlich unverzüglich nach BSIG melden

Schritt 4 Wiederanlauf – aber sauber

ABGEHAKT?

- [ ] **Wiederherstellung erst in eine bereinigte Umgebung** – sonst folgt die zweite Verschlüsselung
- [ ] **Einbruchsweg geschlossen**, bevor Systeme wieder ans Netz gehen
- [ ] **Zugangsdaten flächendeckend erneuert**, inklusive Dienst- und Schnittstellenkonten
- [ ] **Reihenfolge nach Geschäftskritikalität**, nicht nach technischer Bequemlichkeit
- [ ] **Erhöhte Überwachung** für mindestens 30 Tage nach Wiederanlauf
- [ ] **Lessons Learned** dokumentiert und in den Incident-Response-Plan zurückgespielt

Zur Lösegeldfrage: Eine Zahlung ist die letzte Option und niemals eine Garantie. Bei Bedarf koordiniert Argos Verhandlungen und Transfer über zwei spezialisierte Partner – mit Sanktionslisten-Prüfung und rechtlicher Begleitung. Die Entscheidung bleibt immer bei Ihnen.

Im Ernstfall zählt jede Minute.

Unsere Notfall-Hotline ist rund um die Uhr besetzt, 365 Tage im Jahr. Triage, Eindämmung, Forensik und Recovery kommen aus einer Hand – mit bis zu 20 Spezialistinnen und Spezialisten. Wer den Incident-Response-Retainer hat, überspringt die Suche nach Hilfe komplett.

Notfall-Hotline **+49 89 45 24 24-112** · 24/7/365 · **kontakt@argos.security**

argos.security/notfall

Quellen der Kennzahlen: BSI (Anteil betroffener kleiner und mittlerer Unternehmen), Sophos (durchschnittliche Wiederherstellungskosten in Deutschland). Diese Checkliste ist eine Orientierungshilfe und ersetzt keine Rechtsberatung. **Stand: 07/2026.**