Ransomware: erste Schritte

Eine druckbare Arbeitsvorlage für Schweizer KMU · Oktober 2026

Grundsatz: Erst dokumentieren. Dann entscheiden.

Keine voreiligen Neustarts, Löschungen, Neuinstallationen oder unkoordinierten Passwortwechsel. Solche Schritte können die Lage und wichtige Hinweise verändern.

0–15 Minuten: Lage sichern

- ☐ Zeitpunkt, sichtbare Symptome, betroffene Systeme und Konten notieren.
- ☐ Eine verantwortliche Kontaktperson bestimmen; bei sichtbarer Ausbreitung IT einbeziehen.
- ☐ Betroffene Systeme nicht neu starten, zurücksetzen oder neu installieren.
- ☐ Erpressungsnotizen, Fehlermeldungen und verdächtige E-Mails nicht löschen.

15–60 Minuten: Ausbreitung begrenzen

- ☐ Geschäftskritische Prozesse, Fernzugriffe und Cloud-Abhängigkeiten vor Eingriffen prüfen.
- ☐ Systeme, Benutzerkonten und Freigaben in einer Zeitlinie erfassen.
- ☐ Krisenorganisation aktivieren: Geschäftsleitung, IT und Kommunikation.
- ☐ Kommunikationsweg und Entscheidungsrollen festlegen.

1–4 Stunden: Optionen vorbereiten

- ☐ Backups schützen, Zustand prüfen; keine unkoordinierte Rücksicherung.
- ☐ Technische Quellen, Beobachtungen und bisherige Schritte festhalten.
- ☐ Privilegierte Konten und Zugänge koordiniert absichern.
- ☐ Versicherung, Datenschutz und weitere Fachstellen nach eigenem Ablauf einbeziehen.

Vor dem Wiederanlauf

- ☐ Umfang, Eintrittsweg und priorisierte Geschäftsprozesse eingrenzen.
- ☐ Integrität und Wiederherstellbarkeit der ausgewählten Backups prüfen.
- ☐ Passwortwechsel, Mehrfaktorauthentisierung, Patches und Monitoring planen.
- ☐ Wiederanlauf, Beobachtung und Nachbereitung dokumentieren.

Nicht tun

Nicht überstürzt bezahlen, Systeme pauschal abschalten, Hinweise löschen oder Zugangsdaten über ungesicherte Kanäle versenden. Eine Zahlung garantiert keine Wiederherstellung.

Fallnotizen

Zeitpunkt: ..... Verantwortliche Person: .....

Betroffene Systeme/Konten: .....

Nächster Schritt

Akut-Check für Ihren konkreten Vorfall anfragen: it-forensik.ch/akut-check-it-vorfall/ · +41 41 562 70 30

Diese Vorlage unterstützt die technische Ersteinschätzung und ersetzt keine Einzelfall-, Rechts- oder Versicherungsberatung. Grundlage: BACS, Notfallkonzept für Schweizer KMU (2026).

Copyright by Dr. René Bäder (PhDs) · V1.2