Ransomware-Sofortmaßnahmen

NOTFALLKARTE · ISU 17
AUSDRUCKEN & IN DEN NOTFALLORDNER

Für den Ernstfall. Bewusst offline nutzbar, denn im Vorfall ist Ihr Intranet womöglich selbst verschlüsselt. Ruhe bewahren, Reihenfolge halten.

DIE ERSTEN 60 MINUTEN

1. **Isolieren, nicht ausschalten.** Netzwerk trennen, System aber anlassen, damit Spuren im Speicher bleiben.
2. **Spuren sichern.** Speicherabbild und Protokolle ziehen, bevor Sie etwas verändern.
3. **Zugänge sperren.** Kompromittierte und verdächtige Konten sofort deaktivieren.
4. **Backups trennen.** Datensicherung vom Netz nehmen, bevor die Verschlüsselung sie erreicht.
5. **Krisenstab rufen.** Kleiner Kreis, Sprecher und Protokollführer benennen, auf Papier mitschreiben.
6. **Kommunikation umstellen.** Auf einen Weg wechseln, der ohne Ihre Mailserver funktioniert.
7. **Meldeuhr starten.** Uhrzeit des Bekanntwerdens notieren, 72-Stunden-Frist beginnt jetzt.

WICHTIGE BEFEHLE

Netzwerk trennen ohne Ausschalten

```
Disable-NetAdapter -Name "Ethernet" -Confirm:$false
```

Konto sofort deaktivieren

```
Disable-ADAccount -Identity "vorname.nachname"
```

Angemeldete Sitzungen prüfen

```
query user
```

Bei Domänenverdacht: krbtgt zweimal zurücksetzen (offizielles Skript)

Merksatz: Erst isolieren und sichern, dann sperren, dann bewerten. Wer sofort aufräumt, vernichtet die Beweise, die über Meldung und Versicherung entscheiden.

AUF KEINEN FALL

- ✗ Betroffene Server hektisch **herunterfahren**, das löscht Spuren.
- ✗ Aus einem **unklaren Backup** wiederherstellen, der Angreifer kann darin sitzen.
- ✗ Vorschnell **Lösegeld zahlen**, keine Garantie, rechtlich heikel, finanziert den nächsten Angriff.
- ✗ Ohne Sicherung der Spuren **bereinigen** oder neu installieren.
- ✗ Allein entscheiden, immer **im Krisenstab** abstimmen.

MELDEPFLICHT

72 Stunden

Art. 33 DSGVO Meldung an die Aufsichtsbehörde, sobald personenbezogene Daten betroffen sein könnten. Frist ab Bekanntwerden, nicht ab Analyseende. Erstmeldung mit Nachmeldung ist zulässig.

Art. 34 DSGVO Bei hohem Risiko zusätzlich die Betroffenen informieren.

TELEFONKETTE & KONTAKTE

Krisenstab-Leitung	
IT-Leitung	
Datenschutzbeauftragte(r)	
IT-Dienstleister / IR	
Cyberversicherung / Hotline	
Aufsichtsbehörde	
Geschäftsführung	