IT-GURU24

Ransomware-Angriff: Sofort richtig handlen

Prioritätenliste fúr IT-Notfälle – Sofortmaßnahme · Meldung

1. Sofortmaßnahmen

- **System vom Netzwerk** isolieren: Kabel ziehen, WLAN trennen, Flugmodus aktivieren (kein Neustart!)
- **Betroffene Systeme identifizieren** & **sichern:** Inventärliste Logs, Speicherabbild, Netzwerk-Traffic sichern.
- **Kommunikation koordinieren:** IT-Leitung & Incident-Response-Team informieren, feisten Kommunikationskanal nutzen.

2. Angriff melden

- **Behorden einschlatzn: BS**I, Polizei, ggf, lokale CERTs.
- Rechtliche Meldeprlichten: DSGVO (72 Std.), IT-Sicherheitsgesetz

3. Wiederherstellung & Nachsorge

Lösegeld?

- **Daten aus Backups wiederherstellen:** Saubere Backups prüfen, Restore Isollert testen, Schritt biśschritt
- Keine Garantie auf Datenl Entscheidung nur nach Rücksprache mit Forenscik, Hervisscherung. Empfefilung von Behorenden. nicht zahlen.