Notfall Taschenkarte für Privatanwender

Schadsoftwareanzeichen erkennen:

- Plötzliche Verschlüsselung von Daten
- Bekannte Daten haben unbekannte Dateiendungen z.B. .lock oder .0x0
- Lösegeldhinweise in deinen Dateiordnern
- Starke Systemverlangsamung, Pop-ups, unbekannte Prozesse
- Unerklärliche Konto-/Passwortwarnungen

Sofortmaßnahmen einleiten:

- Gerät sofort vom Netzwerk trennen (WLAN/LAN/Bluetooth).
- Nicht ausschalten, wenn Forensik/Analyse nötig sein könnte; sonst geordnet herunterfahren.
- Keine Zahlungen, keine Kontaktaufnahme mit Erpressern.
- Keine Selbstreinigung mit Tools aus unbekannter Quelle.
- Externe Datenträger abziehen.

Zugangsdaten erneuern:

- Passwörter nur von einem sauberem Gerät aus ändern (Kompromittierten Dienst / E-Mail zuerst, dann weitere Dienste).
- Wo/Wenn möglich 2FA aktivieren.
- Bank/Provider/Dienstanbieter bei Verdacht informieren.

Wiederherstellung durchführen:

- System neu aufsetzen (Clean Install).
- Updates/Patches vollständig einspielen.
- Aktuelle Backups prüfen, Integrität verifizieren (offline/immutable für die Wiederherstellung bevorzugen).
- Daten nur aus sauberen Backups zurückspielen!

Fall aufarbeiten

- Infektionsweg identifizieren (Mail, Download, USB).
- Backup-Strategie verbessern (z.B. 3-2-1 Konzept, Offline-Kopie).
- Basis-Härtung durchführen: Standardnutzer mit wenig Rechten verwenden, Makros aus, nur Software aus vertrauenswürdigen Quellen installieren.