ErsteHilfePC Kempten

IT-Service, Forensik & Cyber-Sicherheit im Allgäu

IT-NOTFALL-HOTLINE ALLGÄU
0831 5206664

BSI-Orientierte Notfall-Checkliste & IT-Schutzmaßnahmen

Verhalten bei Hackerangriffen, Virenverdacht & Fernwartungsbetrug — Empfehlungen für Unternehmen und Privatpersonen im Allgäu.

TEIL 1: SOFORTMASSNAHMEN BEI AKUTEM VERDACHT / ANGRIFF

- [ ] **1. Netzwerkverbindung sofort trennen** SOFORT
  Ziehen Sie unverzüglich das LAN-Kabel ab und schalten Sie das WLAN am Gerät aus. Stoppen Sie damit die weitere Kommunikation der Angreifer oder das Abfließen von Daten. *Gerät nicht sofort herunterfahren, falls IT-Forensik benötigt wird!*

- [ ] **2. Fernwartungs-Sitzungen sofort beenden** SOFORT
  Schließen Sie Programme wie AnyDesk, TeamViewer oder RustDesk sofort über den Task-Manager, falls Unbefugte Zugriff haben. Unterbrechen Sie die Verbindung zwingend.

- [ ] **3. Online-Banking & Konten sperren** WICHTIG
  Wurden Bankdaten oder Zugänge eingegeben? Rufen Sie sofort den **Sperr-Notruf 116 116** an oder kontaktieren Sie Ihre Hausbank direkt, um Überweisungen zu stoppen.

- [ ] **4. Passwörter über SAUBERES Zweitgerät ändern** WICHTIG
  Ändern Sie Zugangsdaten für E-Mail, Cloud, Social Media und Firmennetzwerke **ausschließlich über ein zweites, unbeflecktes Gerät** (z. B. Ihr Smartphone über Mobilfunk).

- [ ] **5. Kein Lösegeld zahlen & Beweise sichern** RECHT
  Bei Ransomware (Erpresser-Software) niemals zahlen! Machen Sie Fotos vom Bildschirm, sichern Sie Logfiles und erstatten Sie Anzeige bei der Polizeiinspektion Kempten / Kripo Schwaben Süd/West.

TEIL 2: DIE 5 WICHTIGSTEN PRÄVENTIONSSCHRITTE (BSI-GRUNDSCHUTZ)

- [ ] **6. Multi-Faktor-Authentifizierung (MFA / 2FA) aktivieren** EMPFOHLEN
  Schützen Sie alle Konten (E-Mail, Banking, Microsoft 365) mit einem zweiten Faktor (z. B. Authenticator-App). Passwort-Diebstahl allein reicht Angreifern dann nicht mehr aus.

- [ ] **7. 3-2-1 Backup-Strategie konsequent umsetzen** EMPFOHLEN
  Mindestens 3 Kopien aller wichtigen Daten auf 2 unterschiedlichen Medien, davon 1 Backup **offline/getrennt** vom Netzwerk aufbewahren (Schutz vor Erpressungstrojanern).

- [ ] **8. Patch-Management & Automatische Updates** EMPFOHLEN
  Halten Sie Betriebssysteme (Windows/macOS/Linux), Webbrowser, Router (FritzBox) und Software-Anwendungen stets tagesaktuell, um Sicherheitslücken zu schließen.

- [ ] **9. Sicheres Passwort-Management nutzen** EMPFOHLEN
  Nutzen Sie pro Dienst ein eigenes, komplexes Passwort (mind. 12–16 Zeichen). Verwenden Sie einen lokalen oder verschlüsselten Passwort-Manager (z. B. Bitwarden, KeePass).

- [ ] **10. Rechteeinschränkung & Phishing-Sensibilisierung** EMPFOHLEN
  Arbeiten Sie im Alltag nie mit Administrator-Konten. Seien Sie skepisch bei unerwarteten E-Mails, Dateianhängen oder Zahlungsaufforderungen.

Sie benötigen professionelle Hilfe bei der Bereinigung oder Vorbeugung?

ErsteHilfePC Kempten prüft Ihre Systeme vor Ort oder per gesicherter Diagnose, entfernt Schadsoftware rückstandslos, stellt verlorene Daten wieder her und sichert Ihr Netzwerk zuverlässig ab.

Jetzt anrufen:
0831 5206664