ZUFLUCHTMODUS

KRISEN-PLAYBOOK

Cyberangriff

Wenn Systeme ausfallen, Konten gehackt oder Daten verschlüsselt werden

Aktuelle Online-Version

08:05 · HOME OFFICE, HAMBURG Ihr Laptop zeigt eine rote Meldung: „Ihre Dateien wurden verschlüsselt." Ein Zähler läuft, 72 Stunden. Auf dem Handy hat Ihre Bank eine Nachricht geschickt: „Ungewöhnliche Aktivität." Dann fällt das Internet aus. **Panik nützt dem Angreifer. Ein ruhiger Plan nützt Ihnen.**

Zuerst

1. **Gerät vom Netz trennen** (WLAN aus, Netzwerkkabel ziehen), nicht ausschalten, wenn Beweise wichtig sind.
2. **Passwörter ändern** von einem sicheren Gerät: E-Mail zuerst, dann Banking, Shops, Soziale Medien. **2-Faktor** aktivieren.
3. **Bank** informieren und Karten sperren (116 116 für Sperr-Notruf), Kontoauszüge prüfen.
4. **Kein Lösegeld zahlen**, nichts anklicken. Beweise sichern (Screenshots).
5. **Anzeige** bei der Polizei, Meldung beim BSI und bei der Verbraucherzentrale. Bei Datenverlust Datenschutzbehörde.

1 Sofort

ERSTE 30 MINUTEN

- [ ] **Betroffene Geräte sofort vom Internet trennen (WLAN aus, LAN-Kabel ab). Nicht weiter benutzen.**
- [ ] Nichts bezahlen, nicht mit den Erpressern kommunizieren. Bildschirm fotografieren.
- [ ] **Von einem sauberen Gerät: Passwörter ändern (E-Mail zuerst), Zwei-Faktor-Authentifizierung aktivieren, bestehende Sitzungen abmelden.**
- [ ] Bank und Kreditkartenanbieter anrufen. Bei unbekannten Buchungen: Karte sperren (116 116).
- [ ] Familie, Kollegen und Kontakte warnen, falls von Ihrem Konto Nachrichten verschickt wurden.

2 Schaden eingrenzen

ERSTE STUNDEN BIS TAGE

- [ ] Backups prüfen: Sind sie unverschlüsselt und offline? Nicht an das infizierte System anschließen.
- [ ] Gerät professionell bereinigen lassen oder neu aufsetzen. Daten nur aus sauberen Backups wiederherstellen.
- [ ] Anzeige bei der Polizei (online über die Onlinewache) und Meldung an das BSI. Betroffene Plattformen und Provider informieren.
- [ ] Bei gestohlenen Daten: Schufa und Kreditkonten beobachten, Identitätsmissbrauch melden.
- [ ] **Bei Datenpanne in einer Firma oder Organisation: DSGVO-Meldepflicht innerhalb von 72 Stunden beachten.**

3 Wenn Dienste großflächig ausfallen

BEI AUSFALL VON BANK, MOBILFUNK, INTERNET

- [ ] Bargeld, Papier und Radio nutzen. Informationen kommen über Rundfunk und Behörden.
- [ ] Wichtige Nummern und Adressen auf Papier. Treffpunkte mit Familie vereinbaren.
- [ ] Das Handy sparsam einsetzen. Bei Mobilfunkausfall Polizei- oder Feuerwachen aufsuchen.
- [ ] Auf Falschinformationen achten: nur amtliche Quellen nutzen (Radio, NINA, Behördenseiten).

NICHT tun

- ✕ Lösegeld zahlen: Es garantiert nichts und finanziert Kriminelle.
- ✕ Das infizierte Gerät weiter benutzen oder Backups anschließen.
- ✕ Unbekannte Anhänge oder Links öffnen, auch nicht von bekannten Absendern ohne Rückfrage.
- ✕ Dasselbe Passwort für mehrere Dienste nutzen.
- ✕ Dem „Support-Anrufer“ Fernzugriff gewähren.
- ✕ Überstürzt Geld überweisen.

Wichtige Nummern

Deutschland	**112**
Österreich	**112**
Schweiz	**112**

Meine Kontakte: _____

Treffpunkt: _____

Das sollten Sie griffbereit haben

Basis

- [ ] Passwort-Manager und 2-Faktor-Authentifizierung
- [ ] Regelmäßige Backups auf externer Festplatte (offline)
- [ ] Bargeld und Papierliste mit Nummern (Bank, Sperr-Notruf 116 116)
- [ ] Radio als Informationsquelle
- [ ] Software und Betriebssystem aktuell halten

Fortgeschritten

- [ ] FIDO2-Sicherheitsschlüssel für wichtige Konten
- [ ] Verschlüsselter USB-Stick für Dokumente
- [ ] Zweite SIM-Karte eines anderen Netzbetreibers oder Notfall-Hotspot
- [ ] Netzwerkgeräte mit USV schützen

Danach

- [ ] Alle Konten prüfen, Passwort-Manager und 2FA einrichten.
- [ ] Geräte und Software aktualisieren, Virenscanner prüfen.
- [ ] Backup-Strategie umsetzen (3-2-1: 3 Kopien, 2 Medien, 1 extern).
- [ ] Familie schulen: Phishing, Fake-Shops, Anrufbetrug.

zufluchtmodus.de/notfall/cyberangriff/ · Überprüft am 24. November 2026

Allgemeine Informationen. Folgen Sie immer den Anweisungen von BBK, Behörden und 112.