IT-Notfallplan

Sofortmaßnahmen, Checklisten und Vorlagen – für Privat, Handwerk und kleine Unternehmen

Autor	CEIS-IT.de
Thema	IT-Notfall
Stichwörter	IT-Sicherheit, IT-Notfallplan, CEIS-IT

Notfallkontakt

CEIS-IT Notfallkontakt	
Telefon:	02984 918 98 67
Mobil / WhatsApp:	0175 800 50 54
E-Mail (nicht anklickbar):	mail@ceis-it.de
Adresse:	Langelohstraße 4, 35108 Allendorf (Eder) – Ortsteil Bromskirchen
Website:	Web: CEIS-IT.de

Ihre Daten (ausfüllen)	
Kundennummer (falls vorhanden):	_____
Standort / Adresse (falls abweichend):	_____
Internet/Router Zugang:	Ort: _____ Nutzer: _____ Passwort: _____

Tipp: Speichern Sie dieses Dokument auch auf Ihrem Handy, damit Sie es im Ausfallfall (z. B. PC defekt) griffbereit haben.

1. Die ersten 10 Minuten (Priorität: Stoppen, Sichern, Notieren)

In Notfällen gewinnt nicht, wer am schnellsten klickt – sondern wer systematisch vorgeht.

Goldene Regel: Wenn Sie nicht sicher sind, ob eine Aktion Daten zerstört: lieber stoppen, getrennt lassen, notieren und Hilfe holen.

1. 1) Stoppen Sie die Ausbreitung: Betroffene Geräte sofort vom Netzwerk trennen (LAN-Kabel ziehen, WLAN aus, VPN trennen).
2. 2) Nichts übereilt neu installieren: Keine „Reinigungs-Tools“ aus Popups installieren – und nicht „einfach Windows neu machen“ ohne Backup-Plan.
3. 3) Beweise sichern: Screenshot von Fehlermeldungen, Lösegeldforderung oder auffälligen E-Mails. Uhrzeit notieren.
4. 4) Konten absichern: Wenn ein Konto betroffen sein könnte: Passwort sofort ändern (von einem sauberen Gerät) und 2FA aktivieren.
5. 5) Backups schützen: Externe Festplatten/Backuplaufwerke abziehen, damit sie nicht mitverschlüsselt werden.
6. 6) Lage einschätzen: Was ist betroffen? (1 PC, mehrere PCs, Server, E-Mail, Internet, Telefon, Kassensystem).

Notizfeld: Was ist passiert / seit wann / welche Meldung?

Zeitpunkt entdeckt:	_____	**Wer hat es entdeckt:**	_____
Betroffene Systeme:	_____		
Was genau zu sehen ist (Meldung/ Verhalten):	_____		
Letzte Aktion davor (Download, Update, USB, E-Mail-Anhang):	_____		

2. Schnelle Einordnung (Was ist das Problem?)

Kreuzen Sie an, was am besten passt. Danach springen Sie zur passenden Checkliste.

Symptom	Woran erkennen Sie es?	Nächster Schritt
Ransomware / Verschlüsselung	Dateien haben neue Endungen, lassen sich nicht öffnen oder es erscheint eine Lösegeldforderung.	Kapitel 3
Phishing / Konto übernommen	Fremde Logins, Mails wurden ohne Sie versendet oder das Passwort funktioniert nicht mehr.	Kapitel 4
Malware / Popups / Umleitungen	Der Browser zeigt dauernd Werbung, Startseite ändert sich oder Programme starten von selbst.	Kapitel 5
PC startet nicht / Bluescreen	Kein Bild, Piepen, Bluescreen-Code, Endlosschleife.	Kapitel 6
Internet/WLAN Ausfall	Kein Internet, WLAN bricht ab oder nur einzelne Geräte sind betroffen.	Kapitel 7
Drucker/Office Störung	Drucker offline, Outlook sendet nicht, Teams/Office spinnt.	Kapitel 8
Daten gelöscht / Laufwerk defekt	Ordner sind weg, Festplatte klickt oder das Laufwerk fehlt.	Kapitel 9

Wenn Sie unsicher sind: Behandeln Sie es wie einen Sicherheitsvorfall (Kapitel 3–5) und trennen Sie das Netzwerk.

3. Ransomware / Verschlüsselung

Ziel: Ausbreitung stoppen, Backups schützen, Wiederherstellung vorbereiten.

Bitte nicht: Keine Lösegeldzahlung ohne Beratung. Keine Tools aus dubiosen Webseiten. Nicht „einfach alles löschen“, bevor klar ist, was gerettet werden kann.

Checkliste

- Betroffene Geräte sofort offline (LAN raus, WLAN aus).
- Alle Backups/USB-Platten/Netzlaufwerke trennen.
- Nicht neu starten, wenn gerade Verschlüsselung läuft (erst trennen, dann dokumentieren).
- Screenshots der Forderung und Dateiendungen machen.
- Aus einem sauberen Gerät: Passwörter der wichtigsten Konten ändern (E-Mail, Microsoft, Google, Banking, Fernzugriff).
- CEIS-IT kontaktieren und Notizen bereithalten (Kapitel 1 Notizfeld).

4. Phishing / Konto übernommen (E-Mail, Microsoft, Google)

Ziel: Zugriff zurückholen, weitere Schäden verhindern, betroffene Partner informieren.

Bitte nicht: Nicht auf „Support“-Links aus der Phishing-Mail klicken. Keine Daten in angeblichen Login-Seiten eingeben.

Checkliste

- Von einem sauberen Gerät: Passwort ändern und 2FA aktivieren.
- Alle aktiven Sitzungen abmelden (Microsoft/Google: „Sitzungen“ bzw. „Geräte“ prüfen).
- Postausgang, Weiterleitungen und Regeln prüfen (oft verstecken Angreifer Regeln).
- Wenn Firmenkonto: Admin informieren, ggf. Konto sperren und weitere Konten prüfen.
- Betroffene Kontakte warnen (kurze Vorlage in Kapitel 10).
- Wenn Zahlung/Bank betroffen: Bank sofort anrufen (Sperrhotline).

5. Malware / Popups / Browser leitet um

Ziel: Schadsoftware entfernen, Browser wieder sauber, Passwörter schützen.

Bitte nicht: Keine „Cleaner“ aus Werbebannern installieren. Keine Registry-Tools verwenden, wenn Sie nicht genau wissen, was sie ändern.

Checkliste

- Internet trennen, wenn starke Anzeichen da sind (Popups, Umleitungen, seltsame Installationen).
- Unbekannte Programme deinstallieren (Windows: Apps).

- Browser-Add-ons prüfen und Unbekanntes entfernen.
- Browser zurücksetzen (Startseite/Suchmaschine).
- Vollständigen Virenscan starten (Windows-Sicherheit) und Ergebnis notieren.
- Wenn Sie Logins eingegeben haben: Passwörter ändern (von einem sauberen Gerät).
- Wenn es bleibt: CEIS-IT kontaktieren – oft ist eine saubere Analyse schneller als stundenlanges Probieren.

Schnelltests (5 Minuten)

- Task-Manager: Unbekannte Prozesse? Sehr hohe CPU/Datenträger? (Screenshot machen).
- Autostart: Unbekannte Einträge deaktivieren (nicht löschen, erst dokumentieren).
- Windows-Sicherheit: Schutzverlauf öffnen und Warnungen notieren.
- Browser: Startseite/Suchmaschine und Erweiterungen prüfen.
- Wenn Sie Business nutzen: Prüfen Sie, ob weitere Geräte im Netzwerk Auffälligkeiten zeigen.

Notizen:

_____
_____
_____

6. PC startet nicht / Bluescreen

Ziel: Schaden begrenzen und Daten retten, bevor irgendetwas „repariert“ wird.

Bitte nicht: Nicht mehrfach „hart aus“ drücken, wenn die Festplatte auffällig klingt (klicken/schleifen). Das kann Datenrettung erschweren.

Checkliste

- Notieren Sie: Was genau passiert (Piepen, bleibt schwarz, Bluescreen-Code).
- Alle USB-Geräte abziehen (bis auf Tastatur/Maus).
- Strom komplett trennen (PC: Netzschalter am Netzteil, Laptop: Netzteil ab, 20 Sekunden Power-Taste halten).
- Wenn BitLocker-Abfrage kommt: Wiederherstellungsschlüssel bereithalten.
- Wenn wichtige Daten drauf sind: keine Neuinstallation, bevor geklärt ist, wie Backup/Datensicherung erfolgt.

7. Internet/WLAN Ausfall

Ziel: Eingrenzen, ob Provider, Router oder Gerät die Ursache ist.

Bitte nicht: Router nicht mehrfach schnell an/aus schalten. Das kann die Synchronisation verlängern.

Checkliste

- Prüfen Sie: Betrifft es alle Geräte oder nur eins?
- Router: Strom 30 Sekunden raus, dann 3–5 Minuten warten (vollständiger Neustart).
- Wenn nur ein Gerät: WLAN vergessen und neu verbinden; ggf. Flugmodus an/aus.
- Status-LEDs am Router notieren (DSL/Internet/Online).
- Wenn Firmenbetrieb: Gast-WLAN testweise nutzen, um die Leitung zu prüfen (falls vorhanden).

8. Office/Drucker/Outlook Störung

Ziel: Standardfehler schnell beheben, bevor große Änderungen gemacht werden.

Checkliste

- Drucker: Prüfen, ob „offline“ aktiv ist, Warteschlange leeren, Drucker neu starten.
- Outlook: Online/Offline prüfen, Konto testen, Passwortabfrage ernst nehmen (Phishing ausschließen).
- Windows: Neustart (kein Standby), Updates prüfen.
- Wenn es nach einem Update begann: Zeitpunkt notieren (hilft bei Rückgängig/Repair).

9. Daten gelöscht / Laufwerk defekt

Ziel: Keine weiteren Schreibvorgänge, damit Datenrettung/Restore möglich bleibt.

Bitte nicht: Keine Datenrettungssoftware auf das betroffene Laufwerk installieren – das überschreibt oft genau die Dateien, die Sie retten möchten.

Checkliste

- Sofort stoppen: nichts installieren, keine großen Kopiervorgänge.
- Wenn externes Laufwerk: abziehen und nicht weiter testen.
- Wenn Daten in der Cloud (OneDrive/Google): Papierkorb/Versionen prüfen.
- Backup prüfen (letztes Datum notieren).
- CEIS-IT kontaktieren, wenn es kritisch ist (schnell handeln lohnt sich).

Restore-Plan (kurz)

1. 1) Backup-Quelle festlegen (USB/NAS/Cloud) und Datum notieren.
2. 2) Erst Ursache klären (Virus/Malware) – sonst verschlüsseln Sie nach dem Restore erneut.
3. 3) Wiederherstellung in dieser Reihenfolge: (a) E-Mail/Accounts, (b) zentrale Daten, (c) Programme/Clients.
4. 4) Nach Restore: Updates einspielen, Passwörter ändern, 2FA aktivieren.

Backup-Quelle	Letztes Backup-Datum	OK?
_____	_____	____
_____	_____	____

10. Kommunikationsvorlagen (kurz und nützlich)

Im Notfall ist Kommunikation schwierig. Nutzen Sie diese Vorlagen und passen Sie nur das Nötigste an.

A) Interne Info (Mitarbeitende)

Betreff: IT-Störung – bitte vorerst nichts ändern

Text: Wir haben aktuell eine IT-Störung. Bitte lassen Sie alle betroffenen Geräte eingeschaltet, trennen Sie sie aber vom Netzwerk (LAN ziehen/WLAN aus). Installieren Sie keine Programme und öffnen Sie keine unbekannten E-Mails. Wir melden uns, sobald es weitergeht.

B) Warnung an Kontakte (wenn ein E-Mail-Konto kompromittiert sein könnte)

Text: Bitte ignorieren Sie E-Mails/Links, die heute von unserer Adresse kamen und ungewöhnlich wirken. Wir prüfen aktuell einen möglichen Sicherheitsvorfall. Wenn Sie etwas angeklickt oder Daten eingegeben haben, ändern Sie vorsichtshalber Ihre Passwörter.

C) Telefon-Skript (Provider/Hotline)

Kundennr./Vertrag:	_____	**Anschlussadresse:**	_____ _____
Fehler seit:	_____	Status-LEDs Router:	_____ _____
Was bereits getan wurde:	Router Neustart / Kabel geprüft / anderes Gerät getestet / Störungskarte geprüft		

11. Vorbereitung (30–60 Minuten, die Ihnen Tage sparen)

Dieser Teil ist für „ruhige Zeiten“. Wenn Sie ihn erledigen, ist der Ernstfall halb so schlimm.

- Backups: Mindestens 1 Offline-Backup (USB-Platte nur für Backup, danach abziehen) oder eine 3-2-1 Strategie.
- Passwortmanager: Ein zentraler Passwortmanager und 2FA für E-Mail und Microsoft/Google.
- Admin-Zugriffe: Router-Zugang, Windows-Admin, Cloud-Admin an einem sicheren Ort dokumentieren.
- Inventar: Liste der wichtigsten Geräte (PCs, Laptops, Router, NAS) und Seriennummern.
- Notfallkontakte: Provider, Bank, Softwareanbieter, Schlüsselpersonen.
- Wiederherstellungsmedien: Windows-Wiederherstellungs-USB, BitLocker-Schlüssel.
- Mini-Training: 10 Minuten Phishing-Beispiele im Team anschauen.

Inventarliste (ausfüllen)

Gerät	Name/Standort	Wichtiges Konto/Passwort-Ort	Bemerkung
Router/Firewall	_____	_____	_____
Haupt-PC	_____	_____	_____
Laptop	_____	_____	_____
NAS/Backup	_____	_____	_____
Drucker	_____	_____	_____

Wenn Sie möchten, kann CEIS-IT diesen Notfallplan mit Ihnen in 30–60 Minuten gemeinsam fertig einrichten (Backup-Check, Kontosicherheit, Router-Absicherung).