XCUBITOR

CHECKLISTE 2 VON 3

IT-Notfallplan für KMU

Die erste Stunde entscheidet, was ein Angriff kostet. Diese vier Seiten gehören ausgefüllt in die Schublade – mit den Nummern, die Sie brauchen, wenn der Rechner mit den Kontakten gerade verschlüsselt ist.

Checkliste zum Ausdrucken und Ausfüllen · Stand: November 2026 · xcubitor.at

1 Notfallkarte – ausfüllen, ausdrucken, neben den Router hängen

Im Ernstfall ist der Rechner mit den Kontakten oft genau der, der nicht mehr geht. Deshalb auf Papier.

WER	NAME	TELEFON / E-MAIL
IT-Dienstleister / Betreuer		
WKO Cyber-Security-Hotline (Mitglieder, 0–24 Uhr)	Wirtschaftskammer	**0800 888 133**
Hoster / Website-Agentur		
Microsoft-365- / Google-Administrator		
Bank (Notfallnummer, Überweisungen stoppen)		
Cyberversicherung (Polizzennummer)		
Datenschutz-Verantwortliche Person / Rechtsbeistand		
Steuerberatung		
Polizei (Anzeige) · Meldestelle Internetkriminalität	Notruf 133	against-cybercrime@bmi.gv.at
Datenschutzbehörde (Meldung binnen 72 h)	dsb.gv.at	Online-Meldeformular
Wo liegen die Backups? Wer kann sie zurückspielen?		
Wo liegt dieser Plan? (Ordner, Schublade, zweiter Ausdruck zu Hause)		

2 Die ersten 60 Minuten

- [ ] Ruhe bewahren, nichts löschen, nichts neu installieren
  Erpressernachricht, verdächtige Mails und Fehlermeldungen mit dem Handy fotografieren
- [ ] Betroffene Geräte vom Netzwerk trennen: Netzwerkkabel ziehen, WLAN aus – aber nicht ausschalten, solange nichts verschlüsselt wird
  Läuft eine Verschlüsselung sichtbar, Rechner ausschalten (Empfehlung der WKO-Hotline)
- [ ] Backups sofort abstecken oder vom Netz nehmen, damit sie nicht mitverschlüsselt werden
- [ ] Hilfe holen: IT-Dienstleister, danach die WKO-Hotline 0800 888 133
  Zeitpunkt und Gesprächspartner notieren (Protokoll auf Seite 3)
- [ ] Passwörter ändern – nur von einem sauberen Gerät aus: zuerst E-Mail und Admin-Konten, dann Bank, Hosting, Microsoft 365/Google
- [ ] Aktive Sitzungen beenden und Weiterleitungsregeln in E-Mail-Konten prüfen
  Angreifer legen oft eine stille Weiterleitung an
- [ ] Bank anrufen, wenn Zahlungen oder Rechnungsdaten betroffen sein könnten
- [ ] Team informieren: Was ist passiert, was darf gerade nicht benutzt werden, wer ist Ansprechperson
  Kommunikation über einen Kanal, der nicht betroffen ist (Telefon, Signal, privates Handy)

3 Die fünf häufigsten Fälle – und die ersten drei Schritte

Ransomware / Dateien verschlüsselt

1. Geräte vom Netz, Backups abstecken, Fotos machen.
2. IT-Dienstleister und WKO-Hotline; Versicherung informieren.
3. Kein Lösegeld ohne Experten und Versicherung – Zahlung garantiert weder Schlüssel noch Schweigen.

E-Mail-Konto übernommen

1. Passwort ändern, alle Sitzungen beenden, 2FA einschalten.
2. Weiterleitungs- und Postfachregeln löschen, gesendete Mails prüfen.
3. Kontakte warnen (Telefon!): „In unserem Namen können gefälschte Rechnungen unterwegs sein.“

Website gehackt / Google-Warnung

1. Hoster oder Agentur: Website offline oder in Wartung schalten.
2. Alle WordPress-, Hosting- und FTP-Passwörter ändern; unbekannte Admins löschen.
3. Bereinigung mit Ursachenklärung, danach Google-Überprüfung beantragen. Notfallhilfe: xcubitor.at/website-gehackt/

Gefälschte Rechnung / CEO-Fraud

1. Bereits überwiesen? Sofort Bank anrufen – Rückruf ist in den ersten Stunden möglich.
2. Absender prüfen: Wurde unser Konto oder das des Lieferanten übernommen?
3. Anzeige bei der Polizei; Beleg und Mail-Header sichern.

Laptop oder Handy verloren / gestohlen

1. Gerät aus der Ferne sperren oder löschen (Microsoft 365, Google, Apple).
2. Alle auf dem Gerät gespeicherten Zugänge sperren oder Passwörter ändern.
3. Waren Kundendaten darauf und nicht verschlüsselt: DSGVO-Meldung prüfen.

Vernetzte Technik spielt verrückt

1. Kühlung, Heizung, Alarmanlage: Anlage vor Ort in Handbetrieb nehmen.
2. Installateur anrufen: Fernzugang abschalten, Standardpasswörter ändern.
3. Ware, Temperaturen, Schäden fotografieren und dokumentieren (Versicherung).

4 Wen muss ich wann informieren?

WEN	FRIST	WANN ES GILT
Datenschutzbehörde	72 Stunden ab Kenntnis	Personenbezogene Daten betroffen (Kunden, Mitarbeiter, Lieferanten) und ein Risiko für Betroffene ist nicht ausgeschlossen (Art. 33 DSGVO). Bei hohem Risiko auch die Betroffenen informieren (Art. 34).
Bundesamt für Cybersicherheit	24 h Frühwarnung, 72 h Meldung, 1 Monat Bericht	Nur wenn Ihr Unternehmen unter das NISG 2026 fällt (siehe NIS2-Selbstcheck).
Cyberversicherung	Laut Polizze, meist sofort	Immer – sonst riskieren Sie die Deckung. Viele Versicherer stellen eigene Notfallhilfe.
Kunden und Lieferanten	So früh wie möglich	Wenn in Ihrem Namen Mails verschickt werden könnten oder deren Daten betroffen sind. Vertragliche Meldepflichten prüfen.
Polizei	Zeitnah	Bei Erpressung, Betrug, Geldverlust – auch für Versicherung und Bank nötig. Anzeige nur bei der Polizei, nicht per E-Mail an die Meldestelle.
Mitarbeitende	Sofort	Was ist passiert, was nicht benutzen, an wen wenden – über einen sauberen Kanal.

5 Vorfall-Protokoll

Jede Handlung mit Uhrzeit. Das Protokoll braucht die Versicherung, die Datenschutzbehörde, die Polizei – und Sie selbst, wenn Sie nach drei Tagen ohne Schlaf nicht mehr wissen, was wann war.

DATUM / UHRZEIT	WAS WURDE FESTGESTELLT ODER GETAN	WER

6 Danach: wieder sicher starten

- [ ] Ursache klären lassen: Wie sind die Angreifer hineingekommen?
  Ohne Antwort kommt der nächste Angriff über dieselbe Tür
- [ ] Betroffene Systeme neu aufsetzen statt nur „bereinigen“
- [ ] Daten aus einem Backup von vor dem Angriff zurückspielen und auf Vollständigkeit prüfen
- [ ] Alle Passwörter ändern, 2FA überall aktivieren, Weiterleitungsregeln und unbekannte Benutzer entfernen
- [ ] Meldungen abschließen: Datenschutzbehörde, Versicherung, Kunden, ggf. Bundesamt für Cybersicherheit
- [ ] Kurze Nachbesprechung im Team: Was hat gefehlt? Was ändern wir? Notfallkarte aktualisieren

Lösegeld? Wir raten ab. Eine Zahlung garantiert weder den Schlüssel noch, dass gestohlene Daten nicht trotzdem veröffentlicht werden – und macht Sie zum lohnenden Ziel für das nächste Mal. Entscheiden Sie nie allein, sondern mit Experten und Versicherung.

Quellen: WKO Cyber-Security-Hotline, Bundeskanzleramt (Meldestelle Internetkriminalität), DSGVO Art. 33/34, NISG 2026. Ausführlich: xcubitor.at/ratgeber/gehackt-was-tun-notfallplan/ · Allgemeine Information, keine Rechtsberatung.

Sicherheit, die Ihnen erklärt wird

Xcubitor überwacht Website und Webhosting Ihres Unternehmens rund um die Uhr und warnt Sie in verständlicher Sprache. Zum Start prüfen wir, ob niemand mehr drin ist.

xcubitor.at/preise