AEDIAEVUM LEITFADENREIHE

Erpressungssoftware (Ransomware)

Schutz für Privatpersonen

Für alle privaten Internetnutzerinnen und -nutzer

Herausgegeben von der aediaevum Stiftung · Mühltal · Juni 2026

Ein Klick auf einen falschen Anhang — und plötzlich sind alle Fotos und Dokumente verschlüsselt. Eine Lösegeldforderung erscheint. Das ist Ransomware, und sie trifft längst nicht mehr nur Unternehmen.

---

1. Was Ransomware eigentlich ist

Ransomware ist Schadsoftware, die Dateien verschlüsselt und unbrauchbar macht. Für die Entschlüsselung verlangen die Täter Lösegeld — meist in Kryptowährung. Moderne Varianten drohen zusätzlich mit der Veröffentlichung privater Daten (doppelte Erpressung).

Wie gelangt Ransomware auf ein Gerät?

- E-Mail-Anhänge, getarnt als Rechnung, Bewerbung oder Mahnung
- Infizierte Links in E-Mails, SMS oder Messenger
- Gefälschte Software-Updates von unseriösen Webseiten
- Präparierte USB-Sticks

2. Die fünf wichtigsten Schutzmaßnahmen

Regelmäßige Backups

Die wichtigste Maßnahme: 3-2-1-Regel — 3 Kopien, 2 Medien, 1 Kopie getrennt vom Hauptgerät aufbewahrt.

Software aktuell halten

Automatische Updates für Betriebssystem und Programme aktivieren.

Keine unbekannten Anhänge

Auch bei seriös wirkenden Absendern misstrauisch bleiben.

Aktueller Virenschutz

Erkennt viele bekannte Schadprogramme, bevor sie aktiv werden.

Makros deaktiviert lassen

Office-Makros niemals aktivieren, wenn ein Dokument dazu auffordert.

3. Was im Ernstfall zu tun ist

1. Gerät sofort vom Netzwerk trennen (WLAN aus, Kabel ziehen).
2. Gerät nicht ausschalten, sofern möglich.
3. Kein Lösegeld zahlen — keine Garantie auf Wiederherstellung.
4. Anzeige bei der Polizei erstatten.
5. Professionelle Hilfe einholen, bevor Sie selbst etwas versuchen.

> **Wichtiger Hinweis**
>
> • Bevor Sie zahlen, prüfen Sie nomoreransom.org — ein Projekt von Europol und IT-Sicherheitsfirmen mit kostenlosen Entschlüsselungs-Werkzeugen für viele bekannte Ransomware-Varianten.

4. Vendor-Lock-In vermeiden

Nutzen Sie offene Dateiformate, verteilen Sie Backups auf mindestens zwei unabhängige Anbieter, und prüfen Sie regelmäßig, ob Sie Ihre Daten vollständig exportieren können. So bleiben Sie handlungsfähig, auch wenn ein einzelner Dienst ausfällt.

5. Ihre Ransomware-Schutz-Checkliste

■	Ich habe ein aktuelles Backup meiner wichtigen Daten.
■	Mindestens eine Kopie ist physisch getrennt aufbewahrt.
■	Automatische Updates sind aktiviert.
■	Ich öffne keine unerwarteten Anhänge.
■	Mein Virenschutz ist aktuell.
■	Ich weiß, dass ich im Ernstfall sofort das Netzwerk trenne.

aediaevum Stiftung · In der Röde 5 · 64367 Mühltal · Gemeinnützige Stiftung zur Förderung der Kriminalprävention
Stiftungsaufsicht: Regierungspräsidium Darmstadt · Stand: 21.06.2026 · Dieses Dokument darf kostenlos ausgedruckt und weitergegeben werden.