BEDROHUNGS-BIBLIOTHEK

JULITH GmbH
Awareness-as-a-Service

Ransomware - wenn die ganze Firma still steht

Ransomware-Angriffe legen Unternehmen tagelang lahm und kosten im Schnitt sechsstellig - auch ohne Lösegeldzahlung. Wir zeigen, welche Einfallstore am häufigsten sind und warum Backups allein nicht reichen.

min Lesezeit: 9 min **Aktualisiert:** 14. März 2026 **Risiko:** Sehr hohes Risiko
Quelle: awareness-as-a-service.com/de/resources/threats/ransomware

Was ist Ransomware?

Ransomware ist Schadsoftware, die Dateien oder ganze Systeme verschlüsselt und erst nach Zahlung eines Lösegelds (englisch: ransom) wieder freigeben soll. In der Praxis ist das Bild komplexer: Moderne Ransomware-Gruppen betreiben sogenannte **Double Extortion** - sie exfiltrieren Daten, bevor sie verschlüsseln, und drohen mit Veröffentlichung, selbst wenn das Lösegeld bezahlt wird.

Ransomware-Angriffe sind kein Zufallsprodukt. Hinter den meisten großen Kampagnen stehen professionelle kriminelle Organisationen, die Zugang zu Unternehmensnetzwerken kaufen (Initial Access Brokers), Schwachstellen systematisch ausnutzen und sich wochenlang unentdeckt in Netzwerken bewegen, bevor sie zuschlagen. Die eigentliche Verschlüsselung ist oft das letzte Glied einer langen Kette.

Die Folgekosten übersteigen das Lösegeld regelmäßig um ein Vielfaches: Betriebsausfälle, Forensik, Systemwiederherstellung, Reputationsschäden, Regulierungsfolgen. Das BSI schätzt, dass Unternehmen nach einem schweren Ransomware-Angriff im Schnitt mehrere Wochen benötigen, um den Betrieb vollständig wiederherzustellen.

Auf einen Blick

01

Wochen, nicht Stunden

Die durchschnittliche Wiederherstellungszeit nach einem vollständigen Ransomware-Angriff beträgt mehrere Wochen - Backups allein reichen selten für eine schnelle Rückkehr zum Normalbetrieb.

02

Double Extortion ist Standard

Daten werden exfiltriert, bevor sie verschlüsselt werden. Selbst nach Zahlung des Lösegelds besteht das Risiko einer Veröffentlichung.

03

Phishing ist häufigster Einstieg

Kompromittierte Zugangsdaten und Phishing-Mails, die Malware nachladen, sind die häufigsten initialen Zugangswege - vor ungepatchten Schwachstellen und RDP-Brute-Force.

Woran erkennen Sie Ransomware?

Ransomware kündigt sich selten direkt an - die Vorbereitungsphase ist für Nutzer kaum sichtbar. Diese Signale können auf einen aktiven oder bevorstehenden Angriff hinweisen:

Ungewöhnliche Dateioperationen
Massenhafte Umbenennung oder Verschlüsselung von Dateien durch einen unbekannten Prozess - oft erkennbar an neuen Dateiendungen (.locked, .encrypted, zufällige Zeichen).

Fremde Admin-Accounts
Neue lokale Administrator-Accounts oder unbekannte Konten in Active Directory sind ein starkes Signal für laufende Kompromittierung.

RDP-Brute-Force-Versuche
Massenhafte fehlgeschlagene RDP-Anmeldeversuche in den Logs deuten auf Zugangsversuche hin, die Ransomware-Deployment vorbereiten können.

Datenbank oder Fileserver plötzlich offline
Systeme, die ohne erkennbaren Grund offline gehen oder nicht mehr erreichbar sind, können auf laufende Verschlüsselung hindeuten.

Sicherheitslösung deaktiviert
Wenn Antivirus, EDR oder Firewall-Logs verstummen oder Dienste gestoppt werden, kann das ein Zeichen sein, dass ein Angreifer Werkzeuge entfernt.

Unerwarteter Netzwerktraffic
Große Datenmengen, die nachts oder am Wochenende in Richtung externer IP-Adressen fließen, können Exfiltration ankündigen.

So schützen Sie sich

Für Mitarbeitende

- **Phishing-Links und Anhänge nicht öffnen** - Ransomware landet häufig über eine Phishing-Mail im Netzwerk.
- **Keine privaten USB-Sticks oder Speichermedien** an Unternehmensrechnern verwenden.
- **Ungewöhnliches Systemverhalten sofort melden:** Prozesse, die unerwartet starten, plötzlich langsames System, unbekannte Dateiendungen.
- **Keine Umgehung von Sicherheitswarnungen:** Wenn ein Browser oder Betriebssystem vor einer Website oder Datei warnt, diese Warnung ernst nehmen.

Für Administratoren

- **Offline-Backups (3-2-1-Regel):** Drei Kopien, zwei verschiedene Medientypen, eine offline/air-gapped. Backups regelmäßig auf Wiederherstellbarkeit testen.
- **Netzwerk-Segmentierung:** Kritische Systeme (Produktionssteuerung, Buchhaltung, Backups) in separaten Segmenten mit strengen Firewall-Regeln isolieren.
- **RDP absichern oder deaktivieren:** Kein direkt ins Internet exponierter RDP; zwingend MFA; idealerweise nur über VPN oder Jump-Host.
- **Patch-Management priorisieren:** Bekannte, ausgenutzte Schwachstellen (CISA KEV-Liste) innerhalb von 24–72 Stunden patchen.
- **EDR/XDR einsetzen:** Verhaltensbasierte Erkennung erkennt Ransomware-typische Muster (Masssenverschlüsselung, LSASS-Dump) frühzeitig.

Echte Beispiele

FALL 01 · KLINIK · DE · Q3/2025

Ransomware-Gruppe infiltrierte ein Krankenhaus über eine nicht gepatchte VPN-Schwachstelle. Drei Wochen nach dem initialen Zugang verschlüsselten die Angreifer Patientenakten, Laborsysteme und das PACS. Stationäre Patienten mussten verlegt werden.

Schaden: mehrwöchiger Teilbetrieb, Forensik und Wiederherstellung EUR 1,2 Mio. · **Lösegeld:** nicht bezahlt · **Lehre:** VPN-Appliances sind bevorzugte Einstiegspunkte - Patches müssen innerhalb von Stunden, nicht Wochen folgen.

FALL 02 · SPEDITION · CH · Q4/2025

Phishing-Mail mit gefälschter Zollabrechnung öffnete einen Loader, der wochenlang inaktiv blieb. Erst nach vollständiger Kartierung des Netzwerks wurde LockBit-Ransomware ausgerollt. Disposition, Buchungssysteme und E-Mail-Server lagen drei Tage komplett still.

Schaden: CHF 320.000 Betriebsausfall, Kundenverlust · **Lösegeld:** CHF 180.000 gefordert, nicht bezahlt · **Lehre:** Offline-Backups ermöglichten letztlich die Wiederherstellung - aber der Betriebsausfall war trotzdem erheblich.

Was tun, wenn es passiert ist?

DIE ERSTEN 15 MINUTEN

1. **Betroffene Systeme sofort vom Netz trennen** (Netzwerkkabel ziehen, WLAN deaktivieren) - ohne auszuschalten. Laufende Prozesse können forensisch wertvoll sein.
2. **NICHT zahlen, ohne Beratung einzuholen.** Zahlung garantiert keine Entschlüsselung und finanziert weitere Angriffe. Strafverfolgungsbehörden und Forensiker konsultieren.
3. **Krisenteam aktivieren:** IT-Security, Geschäftsführung, Rechtsabteilung, ggf. Cyber-Versicherung.
4. **Behörden informieren:** In DE Meldung an BSI (kritische Infrastruktur) und Landespolizei; in CH an das NCSC. Meldung schützt vor Vorwürfen der Vertuschung.
5. **Forensische Sicherung:** RAM-Dumps und Log-Sicherung vor der Wiederherstellung - für Strafverfolgung und Versicherungsansprüche.
6. **Kommunikation koordinieren:** Kunden, Lieferanten und Behörden proaktiv informieren - nach juristischer Prüfung. Keine Soforterklärungen via Social Media.

Häufige Fragen

Sollte man Lösegeld zahlen?

Generell nicht. Die Zahlung garantiert keine vollständige Entschlüsselung, kann weitere Forderungen auslösen und finanziert kriminelle Strukturen. Ausnahmen sind nur in extremen Situationen (z.B. Menschenleben in Gefahr) nach Rücksprache mit Behörden denkbar. Versicherungen können ggf. Zahlung decken - das ist aber keine Handlungsempfehlung.

Warum reichen Backups allein nicht aus?

Weil Backups Zeit brauchen - Stunden bis Tage für vollständige Wiederherstellung. Weil Angreifer oft Backups mitlöschen oder verschlüsseln, wenn sie nicht sauber isoliert sind. Und weil Exfiltration unabhängig vom Backup-Zustand ein Problem bleibt.

Was sind Indicators of Compromise (IOC) bei Ransomware?

Neue Admin-Konten, deaktivierte Sicherheitslösungen, ungewöhnlicher Outbound-Traffic, LSASS-Dump-Aktivität, unbekannte Prozesse, Cobalt-Strike-Beacons, laterale Bewegung im Active Directory.

Muss ich einen Ransomware-Angriff melden?

In der EU gelten Meldepflichten unter NIS2 für KRITIS und wichtige Einrichtungen (72 Stunden). In CH gibt es branchenabhängige Pflichten und ab 2025 eine NCSC-Meldepflicht für Betreiber kritischer Infrastruktur. Unabhängig von Pflichten: Frühzeitige Meldung schützt und beschleunigt Hilfe.

Weitere Themen

Ransomware ist häufig das finale Glied einer Kette, die mit Phishing oder kompromittierten Zugangsdaten beginnt. Insider Threats und ungesicherte Cloud-Dienste schaffen die Angriffsfläche, die Ransomware-Gruppen ausnutzen.