INCIDENT-PLAYBOOK MAL-03

Verdacht auf Ransomware

Malware & verdächtiges Verhalten

Dateien lassen sich nicht mehr öffnen, tragen plötzlich fremde Endungen oder es erscheint eine Erpressungsnachricht. Jede Minute zählt, weil die Verschlüsselung weiterläuft, solange das Gerät im Netzwerk hängt.

- Dateinamen mit unbekannter Endung versehen
- Textdatei mit Lösegeldforderung in jedem Ordner
- Office-Dateien lassen sich nicht mehr öffnen
- Netzlaufwerke verändern sich vor den Augen

Sofortmaßnahmen

ERSTE 15 MINUTEN

01 Gerät sofort vom Netzwerk trennen: Netzwerkkabel ziehen und WLAN ausschalten. Das stoppt die Ausbreitung auf Server und Kolleginnen.

02 Gerät eingeschaltet lassen und nicht neu starten. Im Arbeitsspeicher liegen Spuren, die für die Aufklärung und manchmal für die Entschlüsselung entscheidend sind.

03 Angeschlossene Datenträger und Backup-Festplatten physisch abstecken.

04 Foto der Erpressungsnachricht mit dem Handy machen, bevor irgendetwas verändert wird.

05 Sofort telefonisch melden. Nicht per Mail vom betroffenen Gerät.

Melden

SOFORT

WEN

IT-Verantwortliche oder IT-Dienstleister sofort, parallel die Geschäftsführung. Bei laufender Ausbreitung gilt das als Notfall zu jeder Tageszeit.

WIE

Telefonisch über den Notfallkontakt aus dem Kontaktblatt. Wenn niemand erreichbar ist, die nächste Eskalationsstufe anrufen.

WAS BEREITHALTEN

- Welches Gerät betroffen ist und wo es steht
- Woran du es bemerkt hast und wann
- Ob Netzlaufwerke oder Cloud-Ordner betroffen sind
- Was auf der Erpressungsnachricht steht
- Was du zuletzt geöffnet oder installiert hast

Nicht tun

HÄUFIGE FEHLER

- × Das Gerät herunterfahren oder neu starten, solange die IT nichts anderes sagt.
- × Auf eigene Faust ein Entschlüsselungswerkzeug aus dem Internet herunterladen und ausführen.
- × Kontakt zu den Erpressern aufnehmen oder zahlen. Beides entscheidet ausschließlich die Geschäftsführung.
- × Dateien aus einem Backup zurückspielen, bevor klar ist, dass das Netzwerk sauber ist.

Was danach passiert

IT · DATENSCHUTZ · LEITUNG

- → Die IT isoliert betroffene Systeme, sucht nach weiteren befallenen Geräten und sichert Spuren für die Aufklärung.
- → Die Geschäftsführung entscheidet über Krisenkommunikation, Anzeige bei der Polizei und Einbindung der Cyber-Versicherung.
- → Sind personenbezogene Daten betroffen, läuft parallel die Bewertung nach Art. 33 DSGVO mit der 72-Stunden-Frist.
- → Wesentliche und wichtige Einrichtungen nach NISG 2026 prüfen zusätzlich die Berichtspflichten nach § 34: Frühwarnung binnen 24 Stunden, Meldung binnen 72 Stunden an das zuständige Computer-Notfallteam.

Verweise: Incident-Kontaktblatt (PDF) · Verdacht auf Datenschutzverletzung (DAT-05) · Bin ich von NIS2 betroffen? · Interne Kontakte siehe Incident-Kontaktblatt

Playbooks sind der Anfang. Der Prozess dahinter ist Führungsarbeit.

Alle Playbooks, Kontaktblatt und Hintergründe online — kostenfrei und ohne Anmeldung.

wermescher.com/tools/it-notfallplan