INCIDENT-PLAYBOOK MAL-04

Lösegeldforderung am Bildschirm

Malware & verdächtiges Verhalten

Auf dem Bildschirm steht eine Forderung nach Zahlung, damit Dateien wieder zugänglich werden oder angeblich gestohlene Daten nicht veröffentlicht werden. Oft nennt sie eine Frist und einen Kontaktweg für die Verhandlung.

- Vollbildmeldung mit Countdown und Zahlungsadresse
- Textdatei in jedem Ordner mit Zahlungsanweisung
- Mail mit der Drohung, Daten zu veröffentlichen
- Dateien tragen plötzlich eine fremde Endung

Sofortmaßnahmen

ERSTE 15 MINUTEN

01 Gerät sofort vom Netzwerk und WLAN trennen, damit die Verschlüsselung nicht auf Netzlaufwerke weiterläuft.

02 Gerät eingeschaltet lassen und nicht neu starten.

03 Geschäftsführung und IT unverzüglich telefonisch verständigen. Das ist ein Führungsthema, kein IT-Detail.

04 Foto oder Screenshot der Forderung samt Frist und Kontaktweg sichern, am besten mit dem Handy.

05 Auf nichts antworten und nichts anklicken, auch nicht auf den angebotenen Entschlüsselungstest.

Melden

SOFORT

WEN

Geschäftsführung und IT-Verantwortliche sofort, gemeinsam. Die Entscheidung über das weitere Vorgehen liegt bei der Leitung.

WIE

Telefonisch über den Notfallkontakt aus dem Kontaktblatt. Nicht über Mail oder Chat, die möglicherweise mitgelesen werden.

WAS BEREITHALTEN

- Wortlaut der Forderung und genannte Frist
- Welche Laufwerke und Ordner betroffen sind
- Seit wann die Dateien nicht mehr lesbar sind
- Ob weitere Geräte im Haus Auffälligkeiten zeigen
- Ob das Gerät noch am Netz hing, als es bemerkt wurde

Nicht tun

HÄUFIGE FEHLER

- × Auf die Forderung antworten oder in Verhandlungen treten. Das entscheidet ausschließlich die Geschäftsführung.
- × Zahlen. Es gibt keine Zusicherung, dass Daten zurückkommen oder unveröffentlicht bleiben.
- × Betroffene Dateien löschen oder mit Wiederherstellungsprogrammen experimentieren.
- × Eine Sicherung einspielen, bevor geklärt ist, ob der Zugang der Täter noch besteht.

Was danach passiert

IT · DATENSCHUTZ · LEITUNG

- → Die Geschäftsführung entscheidet über Anzeige, Einbindung der Versicherung und externe Unterstützung bei der Aufarbeitung.
- → Sind personenbezogene Daten betroffen, läuft parallel die Frist für die Meldung an die Datenschutzbehörde.
- → Fällt das Unternehmen unter NIS2, prüft die Leitung die Meldepflicht nach dem NISG 2026: Frühwarnung binnen 24 Stunden.

Verweise: Incident-Kontaktblatt (PDF) · Verdacht auf Ransomware (MAL-03) · Verdacht auf Datenschutzverletzung (DAT-05) · 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