INCIDENT-PLAYBOOK MAL-02

Rechner verhält sich ungewöhnlich

Malware & verdächtiges Verhalten

Das Gerät reagiert anders als sonst. Es wird ohne erkennbaren Grund langsam, der Lüfter läuft dauerhaft, Fenster öffnen sich von selbst, der Mauszeiger bewegt sich eigenständig oder Programme starten und beenden sich ohne Zutun.

- Mauszeiger bewegt sich ohne Zutun
- Dauerhaft hohe Auslastung ohne laufendes Programm
- Unbekannte Programme im Autostart
- Dateien sind umbenannt oder verschwunden

Sofortmaßnahmen

ERSTE 15 MINUTEN

01 Gerät vom Netzwerk und WLAN trennen. Das unterbricht Fernzugriff und den Zugang zu Netzlaufwerken.

02 Gerät eingeschaltet lassen und nicht neu starten. Ein Neustart löscht Spuren, die für die Aufklärung gebraucht werden.

03 Nicht weiterarbeiten und keine Zugangsdaten mehr eintippen. Eingaben können mitgelesen werden.

04 Die IT von einem anderen Gerät oder telefonisch verständigen.

05 Notieren, was genau auffällt und seit wann, solange die Beobachtung frisch ist.

Melden

SOFORT

WEN

IT-Verantwortliche oder IT-Dienstleister, unverzüglich. Bei fremdgesteuertem Mauszeiger sofort telefonisch.

WIE

Telefonisch über den Notfallkontakt aus dem Kontaktblatt, nicht vom betroffenen Gerät aus.

WAS BEREITHALTEN

- Welche Auffälligkeiten konkret auftreten
- Seit wann das Verhalten besteht
- Was du zuletzt geöffnet oder installiert hast
- Ob das Gerät noch am Netz hängt
- Ob auf Netzlaufwerke zugegriffen wurde

Nicht tun

HÄUFIGE FEHLER

- × Neu starten oder herunterfahren in der Hoffnung, dass es sich damit erledigt.
- × Selbst Programme deinstallieren oder Autostart-Einträge löschen, bevor die IT den Stand gesehen hat.
- × Weiterarbeiten und sich in andere Dienste einloggen.
- × Externe Datenträger anstecken, um schnell noch Dateien zu sichern.

Was danach passiert

IT · DATENSCHUTZ · LEITUNG

- → Die IT untersucht laufende Prozesse, Autostart und ausgehende Verbindungen und entscheidet über Bereinigung oder Neuaufsetzen.
- → Erreichbare Netzlaufwerke und Cloud-Ordner werden auf Veränderungen geprüft.
- → Anmeldedaten der auf dem Gerät genutzten Konten werden vorsorglich neu aufgesetzt.

Verweise: Incident-Kontaktblatt (PDF) · Verdacht auf Ransomware (MAL-03) · Verdächtigen Anhang geöffnet (PHI-03) · 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