INCIDENT-PLAYBOOK MAL-01

Virenmeldung oder Sicherheitswarnung

Malware & verdächtiges Verhalten

Auf dem Bildschirm erscheint eine Warnung über einen Virus, eine Bedrohung oder ein Sicherheitsproblem. Unklar ist, ob die Meldung vom installierten Schutzprogramm stammt oder von einer Website, die eine Warnung nur nachbaut.

- Warnfenster im Browser mit Telefonnummer zum Support
- Meldung des Virenscanners über eine blockierte Datei
- Aufforderung, ein Reinigungsprogramm zu installieren
- Dauerhafter Warnton mit Vollbildmeldung

Sofortmaßnahmen

ERSTE 15 MINUTEN

01 Prüfen, wo die Meldung steht. Alles innerhalb eines Browserfensters ist keine Meldung deines Schutzprogramms.

02 Keine Telefonnummer aus der Meldung anrufen und keine angebotene Software installieren.

03 Browserfenster oder Tab schließen. Lässt es sich nicht schließen, den Browser über den Task-Manager beenden.

04 Kommt die Meldung nachweislich vom Schutzprogramm: nichts wegklicken, Screenshot machen und melden.

05 Wurde bereits etwas installiert oder eine Nummer angerufen: Gerät vom Netz trennen und die IT anrufen.

Melden

SOFORT

WEN

IT-Verantwortliche oder IT-Dienstleister. Bei echter Scanner-Meldung zeitnah, bei installierter Fremdsoftware sofort.

WIE

Über den internen Meldeweg aus dem Kontaktblatt. Wurde etwas installiert, telefonisch und von einem anderen Gerät.

WAS BEREITHALTEN

- Wortlaut der Meldung, am besten als Screenshot
- Ob sie im Browser oder ausserhalb erschienen ist
- Welcher Dateiname oder Bedrohungsname genannt wurde
- Was du unmittelbar davor geöffnet hast
- Ob du etwas installiert oder angerufen hast

Nicht tun

HÄUFIGE FEHLER

- × Die angezeigte Support-Nummer anrufen. Sie führt zu den Urhebern der Meldung.
- × Ein empfohlenes Reinigungs- oder Optimierungsprogramm installieren.
- × Eine echte Scanner-Meldung wegklicken und weiterarbeiten, ohne sie zu melden.
- × Die blockierte Datei erneut öffnen oder aus der Quarantäne holen.

Was danach passiert

IT · DATENSCHUTZ · LEITUNG

- → Die IT prüft die Protokolle des Schutzprogramms und ordnet ein, ob es sich um einen Einzelfund oder eine Welle handelt.
- → Bei installierter Fremdsoftware wird das Gerät untersucht und im Zweifel neu aufgesetzt.
- → Häufen sich gefälschte Warnfenster, werden die auslösenden Adressen zentral gesperrt.

Verweise: Incident-Kontaktblatt (PDF) · Rechner verhält sich ungewöhnlich (MAL-02) · Verdächtiger Anruf (PHI-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