INCIDENT-PLAYBOOK PHI-03

Verdächtigen Anhang geöffnet

Phishing & Social Engineering

Du hast einen Anhang geöffnet und danach stimmt etwas nicht. Das Dokument verlangt, den Bearbeitungsschutz aufzuheben oder Inhalte zu aktivieren, es öffnet ein Fenster, das nach Zugangsdaten fragt, oder es bleibt leer, obwohl eine Rechnung angekündigt war.

- Word- oder Excel-Datei bittet, Inhalte zu aktivieren
- Angebliche Rechnung öffnet eine Anmeldemaske
- ZIP-Archiv mit einer Datei, die wie ein Dokument aussieht
- Dokument ist leer oder unleserlich

Sofortmaßnahmen

ERSTE 15 MINUTEN

01 Datei und Programm schließen. Hast du Inhalte oder Makros aktiviert, das Gerät sofort vom Netzwerk und WLAN trennen.

02 Gerät eingeschaltet lassen. Ein Neustart kann Spuren vernichten, die für die Aufklärung gebraucht werden.

03 Die IT anrufen, nicht mailen. Bei aktivierten Makros gilt das Gerät bis zur Prüfung als nicht vertrauenswürdig.

04 Hast du in einem Fenster Zugangsdaten eingegeben: Passwort von einem anderen Gerät aus ändern.

05 Die Ursprungsnachricht samt Absender und Dateiname festhalten, ohne sie weiterzuleiten.

Melden

SOFORT

WEN

IT-Verantwortliche oder IT-Dienstleister, unverzüglich. Bei Dateien aus dem Rechnungsumlauf zusätzlich die Buchhaltung.

WIE

Telefonisch über den Notfallkontakt aus dem Kontaktblatt, weil das betroffene Gerät für die Meldung nicht genutzt werden soll.

WAS BEREITHALTEN

- Dateiname und Dateityp des Anhangs
- Ob du Inhalte, Makros oder den Bearbeitungsschutz freigegeben hast
- Was nach dem Öffnen auf dem Bildschirm passiert ist
- Absender und Betreff der Nachricht
- Ob das Gerät noch am Netz hängt

Nicht tun

HÄUFIGE FEHLER

- × Den Rechner neu starten oder herunterfahren, bevor die IT den Fall aufgenommen hat.
- × Die Datei zur Prüfung an jemanden weiterleiten. Der nächste Empfänger öffnet sie im Zweifel ebenfalls.
- × Selbst einen Virenscan starten und das Ergebnis abwarten, statt zu melden.
- × Weiterarbeiten, weil scheinbar nichts passiert ist. Schadsoftware arbeitet in der Regel unauffällig.

Was danach passiert

IT · DATENSCHUTZ · LEITUNG

- → Die IT untersucht das Gerät, prüft Netzwerkverbindungen und offene Prozesse und entscheidet über Bereinigung oder Neuaufsetzen.
- → Erreichbare Netzlaufwerke und Cloud-Ordner werden auf Veränderungen und Verschlüsselung geprüft.
- → Dieselbe Datei wird in allen Postfächern gesucht und dort zentral entfernt.

Verweise: Incident-Kontaktblatt (PDF) · Verdacht auf Ransomware (MAL-03) · Phishing-Link angeklickt (PHI-02) · Interne Kontakte siehe Incident-Kontaktblatt