INCIDENT-PLAYBOOK PHI-02

Phishing-Link angeklickt

Phishing & Social Engineering

Du hast einen Link aus einer Nachricht geöffnet und erst danach gemerkt, dass etwas nicht stimmt. Die Seite verlangt eine Anmeldung, einen Bestätigungscode oder einen Download. Vielleicht hast du schon etwas eingetippt.

- Anmeldeseite, die der internen Anmeldung nachgebaut ist
- Seite fragt nach dem Code aus der Authenticator-App
- Download startet ohne Zutun
- Adresszeile zeigt eine fremde Domain

Sofortmaßnahmen

ERSTE 15 MINUTEN

01 Seite sofort schließen. Wurde nichts eingegeben, ist in den meisten Fällen nichts abgeflossen.

02 Hast du Zugangsdaten eingegeben: Passwort von einem anderen Gerät aus ändern und alle aktiven Sitzungen abmelden.

03 Hast du einen MFA-Code bestätigt: sofort telefonisch melden. Der Zugriff kann in diesem Moment bereits laufen.

04 Wurde etwas heruntergeladen oder installiert: Gerät vom Netz trennen und die IT anrufen, bevor du weiterarbeitest.

05 Screenshot der Seite und die vollständige Adresse aus der Adresszeile sichern.

Melden

SOFORT

WEN

IT-Verantwortliche oder IT-Dienstleister, unverzüglich. Bei bestätigtem MFA-Code sofort telefonisch.

WIE

Telefonisch über den Notfallkontakt aus dem Kontaktblatt, wenn Zugangsdaten oder ein Code betroffen sind. Sonst über den internen Meldeweg.

WAS BEREITHALTEN

- Welche Adresse in der Adresszeile stand
- Ob du Zugangsdaten eingegeben hast und für welchen Dienst
- Ob du eine MFA-Anfrage bestätigt hast
- Ob ein Download gestartet oder etwas installiert wurde
- Uhrzeit des Klicks, so genau wie möglich

Nicht tun

HÄUFIGE FEHLER

- × Abwarten und beobachten, ob etwas passiert. Bei abgeflossenen Zugangsdaten zählt jede Minute.
- × Das neue Passwort auf demselben Gerät setzen, wenn ein Download gelaufen ist.
- × Die Seite noch einmal öffnen, um nachzusehen, wie sie aussah. Der Screenshot genügt.
- × Den Vorfall verschweigen, weil er unangenehm ist. Gemeldete Fälle sind in Minuten eingedämmt.

Was danach passiert

IT · DATENSCHUTZ · LEITUNG

- → Die IT prüft die Anmeldeprotokolle des betroffenen Kontos auf fremde Zugriffe und setzt die Anmeldedaten neu auf.
- → Bei bestätigtem MFA-Code werden zusätzlich die hinterlegten Geräte und Wiederherstellungsoptionen kontrolliert.
- → Wurde etwas ausgeführt, wird das Gerät untersucht und im Zweifel neu aufgesetzt.

Verweise: Incident-Kontaktblatt (PDF) · Verdacht auf Kontoübernahme (ACC-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