INCIDENT-PLAYBOOK PHI-05

Verdächtiger Anruf oder Identitätsbetrug

Phishing & Social Engineering

Jemand ruft an und gibt sich als IT-Support, Bank, Behörde, Lieferant oder Kollege aus. Verlangt werden Zugangsdaten, ein Bestätigungscode, eine Fernwartungssitzung oder Auskunft über interne Abläufe. Der Anruf kommt unerwartet und drängt zur Eile.

- Angeblicher Support will per Fernwartung auf den Rechner
- Anrufer fragt nach dem Code aus der Authenticator-App
- Bank meldet einen Sicherheitsvorfall und braucht Daten
- Neuer Kollege fragt nach internen Abläufen

Sofortmaßnahmen

ERSTE 15 MINUTEN

01 Keine Zugangsdaten und keine Codes nennen. Kein seriöser Anrufer fragt danach, auch die eigene IT nicht.

02 Keine Fernwartung zulassen und keine Software installieren, die am Telefon verlangt wird.

03 Gespräch beenden. Du brauchst keine Begründung und schuldest keine Höflichkeit.

04 Läuft bereits eine Fernwartung: Gerät vom Netz trennen und die IT über ein anderes Gerät anrufen.

05 Selbst zurückrufen, über eine Nummer aus dem internen Verzeichnis oder von der offiziellen Website.

Melden

SOFORT

WEN

IT-Verantwortliche oder IT-Dienstleister. Bei angeblichen Bank- oder Behördenanrufen zusätzlich Buchhaltung und Geschäftsführung.

WIE

Über den internen Meldeweg aus dem Kontaktblatt. Lief eine Fernwartung, telefonisch und von einem anderen Gerät.

WAS BEREITHALTEN

- Rufnummer und Zeitpunkt des Anrufs
- Als wer sich die Person ausgegeben hat
- Was konkret verlangt wurde
- Ob du etwas genannt, installiert oder freigegeben hast
- Ob Namen oder interne Details bekannt waren

Nicht tun

HÄUFIGE FEHLER

- × Zur Prüfung eine Nummer zurückrufen, die der Anrufer selbst genannt hat.
- × Aus Höflichkeit im Gespräch bleiben und nur Kleinigkeiten bestätigen. Auch Namen und Abläufe sind verwertbar.
- × Einen Code vorlesen, weil der Anrufer ihn angeblich zur Verifizierung braucht.
- × Den Anruf als erledigt betrachten, weil du nichts verraten hast. Die IT braucht die Info trotzdem.

Was danach passiert

IT · DATENSCHUTZ · LEITUNG

- → Die IT prüft, ob im selben Zeitraum Anmeldeversuche oder MFA-Anfragen auf dein Konto liefen.
- → Wurde eine Fernwartung zugelassen, wird das Gerät untersucht und im Zweifel neu aufgesetzt.
- → Häufen sich Anrufe, wird das Team informiert, welche Rollen und Nummern gerade angesprochen werden.

Verweise: Incident-Kontaktblatt (PDF) · Verdacht auf Kontoübernahme (ACC-03) · CEO-Fraud oder Rechnungsbetrug (PHI-04) · Interne Kontakte siehe Incident-Kontaktblatt