INCIDENT-PLAYBOOK PHI-06

Verdächtiger QR-Code oder SMS-Link

Phishing & Social Engineering

Ein QR-Code oder eine SMS führt auf eine Seite, die Zugangsdaten, eine Zahlung oder eine App-Installation verlangt. Beide Wege umgehen den Mail-Schutz des Unternehmens, weil sie am Handy und außerhalb des Postfachs ankommen.

- QR-Code-Aufkleber über dem Original am Parkautomaten
- SMS zu einer angeblich fehlgeschlagenen Paketzustellung
- QR-Code in einer Mail statt eines Links
- SMS von der angeblichen Bank mit Bestätigungslink

Sofortmaßnahmen

ERSTE 15 MINUTEN

01 Nichts eingeben und die Seite schließen. Solange keine Daten eingetippt sind, ist meist nichts passiert.

02 Wurde bereits etwas eingegeben: sofort das betroffene Passwort ändern und alle aktiven Sitzungen abmelden.

03 Wurde eine App oder ein Profil installiert: Gerät vom WLAN und Mobilfunk trennen und die IT anrufen, bevor du weiter tippst.

04 Screenshot der Nachricht oder Foto des QR-Codes machen, samt Absendernummer.

05 Melden, auch wenn du nichts eingegeben hast. Der Fund selbst ist die nützliche Information.

Melden

SOFORT

WEN

IT-Verantwortliche oder IT-Dienstleister. Bei QR-Codes im eigenen Gebäude zusätzlich Empfang oder Facility-Verantwortliche.

WIE

Über den internen Meldeweg aus dem Kontaktblatt. Bei installierter App oder Profil telefonisch, nicht schriftlich vom betroffenen Gerät.

WAS BEREITHALTEN

- Wo der QR-Code hing oder von welcher Nummer die SMS kam
- Wie die Zielseite ausgesehen und was sie verlangt hat
- Ob du etwas eingegeben oder installiert hast
- Ob es ein dienstliches oder privates Gerät war
- Wann genau du den Code gescannt oder den Link geöffnet hast

Nicht tun

HÄUFIGE FEHLER

- × Den Code ein zweites Mal scannen, um ihn Kolleginnen und Kollegen zu zeigen.
- × Den Link zur Warnung an andere weiterleiten. Wer ihn öffnet, landet auf derselben Seite.
- × Auf die SMS antworten, auch nicht mit einer Absage. Eine Antwort bestätigt, dass die Nummer aktiv ist.
- × Verdächtige QR-Aufkleber entfernen, bevor jemand sie fotografiert hat.

Was danach passiert

IT · DATENSCHUTZ · LEITUNG

- → Die IT prüft, ob weitere Personen dieselbe Nachricht erhalten haben, und sperrt die Zieladresse.
- → Bei eingegebenen Zugangsdaten werden Konto und Anmeldeprotokolle geprüft und die Anmeldedaten neu aufgesetzt.
- → Bei installierten Apps oder Konfigurationsprofilen wird das Gerät untersucht und im Zweifel neu aufgesetzt.

Verweise: Incident-Kontaktblatt (PDF) · Verdacht auf Kontoübernahme (ACC-03) · Interne Kontakte siehe Incident-Kontaktblatt