INCIDENT-PLAYBOOK PHI-01

Verdächtige Nachricht erhalten

Phishing & Social Engineering

Eine Mail oder Chat-Nachricht wirkt nicht echt. Sie drängt zur Eile, kommt von einem unerwarteten Absender oder verlangt eine Anmeldung, eine Zahlung oder die Weitergabe von Daten. Du hast noch nichts angeklickt und nichts eingegeben.

- Angebliche Sperrung eines Kontos mit Frist von 24 Stunden
- Rechnung von einem Absender, der nie Rechnungen schickt
- Bitte um Freigabe eines geteilten Dokuments
- Nachricht der Geschäftsführung über einen fremden Kanal

Sofortmaßnahmen

ERSTE 15 MINUTEN

01 Nichts anklicken, nichts herunterladen, nicht antworten. Solange die Nachricht nur im Postfach liegt, ist nichts passiert.

02 Absenderadresse vollständig anzeigen lassen und mit der echten Adresse vergleichen. Der angezeigte Name sagt nichts aus.

03 Bei angeblich internen Absendern über einen bekannten Weg rückfragen, nie über die Kontaktdaten aus der Nachricht.

04 Melden, auch wenn du sicher bist, dass es Phishing ist. Die IT braucht die Info, um andere Empfänger zu schützen.

Melden

SOFORT

WEN

IT-Verantwortliche oder IT-Dienstleister. Bei Nachrichten mit Zahlungsbezug zusätzlich die Buchhaltung.

WIE

Über den internen Meldeweg aus dem Kontaktblatt. Falls vorhanden, den Melde-Button im Mail-Programm nutzen.

WAS BEREITHALTEN

- Vollständige Absenderadresse, nicht nur der angezeigte Name
- Betreff und Eingangszeitpunkt der Nachricht
- Worum die Nachricht bittet
- Ob du etwas angeklickt oder geantwortet hast
- Ob Kolleginnen und Kollegen dieselbe Nachricht bekommen haben

Nicht tun

HÄUFIGE FEHLER

- × Die Nachricht an Kolleginnen und Kollegen weiterleiten, um zu warnen. Wer den Link dort öffnet, ist im selben Fall.
- × Auf Abmelden oder Kein Interesse klicken. Auch diese Links bestätigen, dass die Adresse aktiv gelesen wird.
- × Die Nachricht einfach löschen. Ohne Meldung erfährt die IT nichts von der laufenden Welle.
- × Den Absender anrufen, um nachzufragen, wenn die Nummer aus der Nachricht selbst stammt.

Was danach passiert

IT · DATENSCHUTZ · LEITUNG

- → Die IT prüft, wie viele Postfächer die Nachricht erreicht hat, und entfernt sie zentral aus allen betroffenen Konten.
- → Absender und Zieladresse werden gesperrt, damit Folgewellen aus derselben Quelle nicht mehr durchkommen.
- → Häufen sich gleichartige Nachrichten, folgt eine kurze Information ans Team mit den konkreten Erkennungsmerkmalen.

Verweise: Incident-Kontaktblatt (PDF) · Phishing-Link angeklickt (PHI-02) · CEO-Fraud oder Rechnungsbetrug (PHI-04) · 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