VORFALLART 01 · ERKENNEN & MELDEN

Phishing & verdächtige Nachrichten

Wie du gefälschte E-Mails, SMS und Messenger-Nachrichten erkennst und richtig darauf reagierst.

Was ist das?

Phishing ist der Versuch, über gefälschte Nachrichten an Zugangsdaten oder Zahlungen zu gelangen oder Schadsoftware auszuführen. Die Nachricht gibt sich als vertrauenswürdiger Absender aus – Bank, Lieferant, Kollege oder Behörde – und erzeugt Druck oder Neugier.

Phishing ist oft der Startpunkt größerer Vorfälle: aus einem geklickten Link werden gekaperte Konten, Zahlungsbetrug oder Ransomware.

Was kann im Betrieb passieren?

- Zugangsdaten werden auf einer gefälschten Login-Seite abgegriffen
- Schadsoftware wird über Anhang oder Link installiert
- Ein Konto oder Postfach wird übernommen und für weitere Angriffe genutzt
- Der Vorfall wird zum Ausgangspunkt für Ransomware oder gefälschte Zahlungen

Woran erkennst du es?

- Unerwarteter Absender, künstlicher Zeitdruck („sofort“, „letzte Mahnung“)
- Absenderadresse oder Link-Ziel weichen von der echten Domain ab
- Ungewöhnliche Anrede, Sprache oder Formatierung
- Aufforderung zu Login, Zahlung oder Bestätigung einer MFA-Anfrage
- Unerwarteter Anhang oder Aufforderung, Sicherheitswarnungen zu ignorieren

Sofort richtig reagieren

Der Handlungsrahmen aus der Fortbildung – Schritt für Schritt:

1	**Trennen**	Nichts weiter anklicken. Wenn schon geklickt oder eine Datei geöffnet wurde: Gerät vom Netz trennen (Kabel und Funk) und nicht neu starten.
2	**Festhalten**	Nachricht nicht löschen. Absender, Uhrzeit und was angeklickt oder eingegeben wurde notieren; Screenshot machen.
3	**Melden**	IT und Cyber-Ersthelfer über den vereinbarten, unabhängigen Kanal informieren. Wurde ein Passwort eingegeben, das Konto sichern lassen.
4	**Bewahren**	Keine eigenen „Reparaturen“. Den Zustand für die Fachhilfe erhalten und im Protokoll festhalten.

Buch zur Fortbildung: „Betrieblicher Cyber-Ersthelfer“ · ISBN 978-3-6967-6362-6

Merksatz

„Danke, dass du es sofort sagst.“ Eine gemeldete Verdachtsmail ist erwünscht – auch wenn sie sich als harmlos herausstellt.

Das ist erst der erste Schritt

In der Fortbildung „Geprüfter Betrieblicher Cyber-Ersthelfer“ (290 €, 2× 100 Min live & digital) übst du genau diesen Ablauf für jede typische Vorfallart – mit Checklisten, Mailvorlagen, Urkunde & Badge. Empfehlung: zwei Ersthelfer je Betrieb. Anmeldung & Termine: info@secumetrix.de

Grenzen dieses Whitepapers: Es vermittelt allgemeines Wissen und ersetzt keine Rechtsberatung, keine technische Einzelfallprüfung und keine Versicherungszusage. Die Bewertung eines konkreten Vorfalls, die verbindliche rechtliche Einordnung und die Entscheidung über Versicherungsschutz erfordern die Prüfung des Einzelfalls. Führe nur Maßnahmen aus, für die du im Betrieb beauftragt und eingewiesen bist.