Whitepaper & Notfall-Checkliste

E-Mail-Konto kompromittiert

ANGRIFF

✓ Richtig vorbeugen

- Zwei-Faktor-Authentifizierung für alle E-Mail-Konten aktivieren.
- Regelmäßige Überprüfung hinterlegter Weiterleitungsregeln.
- Starke, einzigartige Passwörter verwenden.
- Anmeldeversuche und ungewöhnliche Standorte überwachen, falls verfügbar.

■ Im Ernstfall – Schritt für Schritt

Vorfall-Protokoll (bitte ausfüllen)

Datum:	
Uhrzeit:	
Betroffenes System / Gerät:	
Gemeldet durch:	
Gemeldet an (IT-Verantwortlicher):	

- ■ **1.** Passwort sofort ändern, alle aktiven Sitzungen abmelden.
- ■ **2.** Weiterleitungsregeln und Postfach-Regeln auf Manipulation prüfen.
- ■ **3.** Zwei-Faktor-Authentifizierung aktivieren, falls noch nicht geschehen.
- ■ **4.** Kontakte informieren, falls Spam/Phishing im Namen des Kontos versendet wurde.
- ■ **5.** IT-Abteilung zur forensischen Prüfung hinzuziehen.
- ■ **6.** Verknüpfte Konten (z. B. Passwort-Reset über diese E-Mail) prüfen.
- ■ **7.** Vorfall dokumentieren.