

Phishing-Angriffe gehören zu den häufigsten Ursachen für kompromittierte Zugänge, Datenverlust und Sicherheitsvorfälle. Die Sensibilisierung der Mitarbeiter und zusätzliche technische Schutzmaßnahmen gehören deshalb zu den grundlegenden Standards eines professionellen IT-Betriebs.

Checkliste

- Verdächtige E-Mails und Nachrichten werden vor dem Öffnen sorgfältig geprüft
- Absenderadressen und enthaltene Links werden kritisch kontrolliert
- Zugangsdaten und vertrauliche Informationen werden nicht über Nachrichtenlinks eingegeben
- Unbekannte oder unerwartete Anhänge werden nicht ungeprüft geöffnet
- QR-Codes aus unsicheren Quellen werden nicht unüberlegt gescannt
- Bei Verdacht auf Phishing wird der Vorfall sofort an die IT gemeldet
- Eingegebene Passwörter werden bei einem Vorfall unverzüglich geändert
- Aktive Sitzungen und betroffene Benutzerkonten werden sofort geprüft
- Zahlungsdaten und Bankzugänge werden bei Verdacht unmittelbar gesichert
- Für kritische Systeme ist Mehr-Faktor-Authentifizierung aktiviert
- Sicherheitsupdates und Schutzsoftware werden konsequent aktuell gehalten



Weitere Schutzmaßnahmen gegen Phishing

- E-Mail-Filter und Linkschutz zentral verwalten
- MFA für externe Zugänge verbindlich festlegen
- Sicherheitsvorfälle mit klaren Prozessen behandeln
- Benutzer regelmäßig schulen und sensibilisieren
- Kritische Konten und Cloud-Zugänge laufend überwachen

So finden Sie uns

 Heinrich-Landerer-Str. 72
73037 Göppingen

 vertrieb@mars-solutions.de

 Tel.: 07161 / 65492-50

 www.mars-solutions.de