29.05.2026

Phishing wird raffinierter: Wie «Man-in-the-Middle»-Angriffe selbst MFA umgehen

Cyberkriminelle entwickeln ihre Phishing-Methoden laufend weiter. Besonders gefährlich sind sogenannte «Man-in-the-Middle»-Angriffe (MitM). Dabei schalten sich Angreifer unbemerkt zwischen Opfer und legitime Webseite und können so Zugangsdaten in Echtzeit abfangen.

Im Unterschied zu klassischen Phishing-Websites kopieren MitM-Angriffe nicht einfach nur eine Login-Seite. Die betrügerische Infrastruktur leitet die Eingaben direkt an den echten Dienst weiter und zeigt dem Opfer gleichzeitig die legitime Webseite an. Dadurch bemerken Betroffene den Angriff oft nicht. Selbst die Mehrfaktor-Authentifizierung (MFA) kann damit unter Umständen umgangen werden.

Angriffe nehmen deutlich zu

In der Schweiz wächst die Bedrohung durch Phishing weiter. Aktuell kursiert eine besonders tückische Form von Phishing – der Man-in-the-Middle-Phishing-Angriff. Cyberkriminelle setzen dabei zunehmend auf neue Hosting-Technologien und schwer erkennbare Infrastrukturen.

So funktionieren MitM-Phishing-Angriffe

Oft beginnt der Angriff mit einer scheinbar harmlosen E-Mail, SMS oder WhatsApp-Nachricht. Diese enthält einen Link zu einer gefälschten Anmeldeseite. Klickt das Opfer darauf und meldet sich an, werden Benutzername, Passwort und unter Umständen auch der MFA-Code in Echtzeit an die echte Plattform weitergeleitet. Der Angreifer erhält gleichzeitig Zugriff auf die aktive Sitzung.

Besonders perfide: Viele Angriffe nutzen mehrere Weiterleitungen und professionell gestaltete Websites, um Sicherheitslösungen zu umgehen. Teilweise werden sogar spezialisierte Cloud-Dienste oder dezentrale Plattformen verwendet, damit Phishing-Seiten länger online bleiben.

Wie sich Privatpersonen und Unternehmen schützen können

Ein vollständiger Schutz existiert nicht. Dennoch lassen sich Risiken deutlich reduzieren:

- Anmelde-Links aus E-Mails, SMS oder Messenger-Nachrichten kritisch hinterfragen
- Internetadressen genau prüfen
- Passwortmanager verwenden
- Moderne MFA-Methoden wie FIDO2- oder Passkey-Lösungen einsetzen, falls angeboten
- Betriebssystem, Browser und Sicherheitssoftware stets aktuell halten
- Mitarbeitende regelmässig sensibilisieren und schulen

Wichtig ist zudem, verdächtige Login-Aufforderungen oder unerwartete MFA-Anfragen seriös zu prüfen. Wer plöt-

zlich mehrere MFA-Bestätigungen erhält, obwohl keine Anmeldung durchgeführt wurde, sollte sein Passwort umgehend ändern und aktive Sitzungen beenden.

Mensch bleibt wichtigster Schutzfaktor

Trotz moderner Sicherheitstechnologien bleibt der Mensch ein zentrales Ziel von Cyberkriminellen. Phishing-Angriffe setzen gezielt auf Zeitdruck, Vertrauen und Gewohnheiten. Entsprechend wichtig bleibt Aufmerksamkeit und gesunde Skepsis im digitalen Alltag.