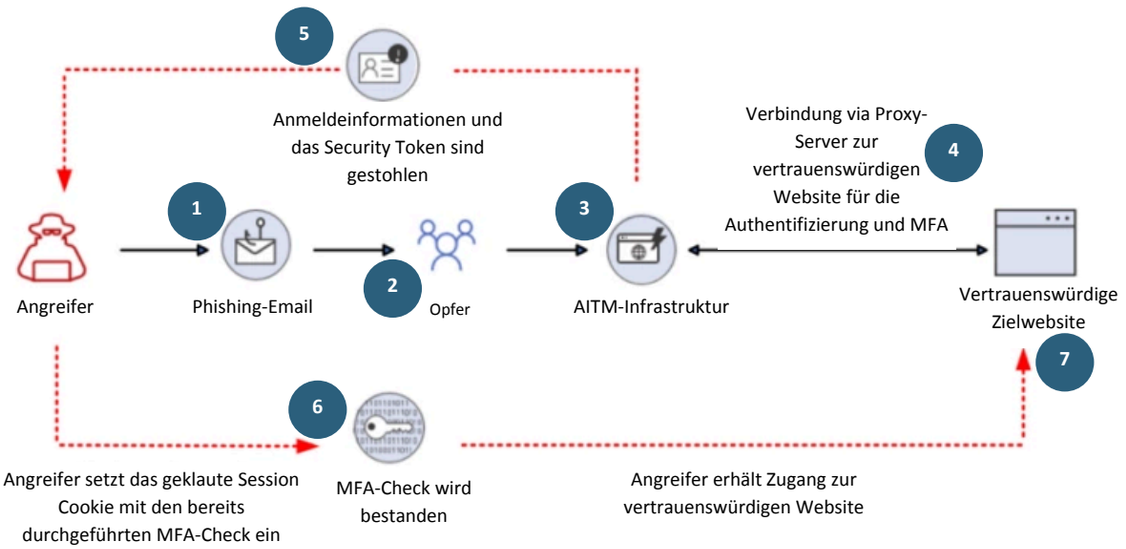
Was passiert bei einer AITM-Attacke in der Praxis?

Der Phishing-Angriff Schritt für Schritt



Die AITM-Attacke ist eine perfide Phishing-Methode. Nachfolgend ist Schritt für Schritt dargestellt, wie die Angreifenden vorgehen:

1. Der Angreifer möchte einen AITM-Angriff auf sein Opfer ausüben. Innert wenigen Stunden können alle erforderlichen Komponenten, die für die Attacke nötig sind, beschafft und konfiguriert werden. Es benötigt eine Linux-Maschine, welche als Proxy-Server zwischen Opfer und der Internetseite von Microsoft fungiert, sowie ein möglichst echt aussehendes Phishing-Mail. Dieses Mail wird nun vom Angreifer ans das Opfer verschickt.

2. Das Opfer hat heute eine E-Mail erhalten. Darin steht, dass es angeblich von einer Arbeitskollegin eine Nachricht in Microsoft Teams erhalten hat. Routiniert klickt das Opfer der Phishing-Attacke auf den Button «In Teams ansehen» - ohne den Absender und die im Button hinterlegte URL zu prüfen.

3. Das Opfer wird jetzt auf eine Website weitergeleitet, die genau wie das Anmelde-Fenster von Microsoft aussieht. Nichtsahnend meldet sich das Opfer mit seiner E-Mail-Adresse, seinem Passwort und dem MFA-Code an, welches es über seine Microsoft Authenticator App erhielt.

4. Nach der Authentifizierung fällt dem Opfer sofort auf, dass es nicht direkt auf die Microsoft Teams-Seite weitergeleitet wurde. Im ersten Moment geht es davon aus, dass es sich um eine Störung bei Microsoft handelt. Da das Opfer nun eingeloggt ist und im Browser beim URL-Feld die URL von Microsoft enthalten ist, agiert es weiter bedenkenlos.

5. Der Angreifer hat nun mithilfe seines Opfers die E-Mail-Adresse, das Passwort und das MFA-Session-Token im Klartext erhalten. Mit simplem Copy-Paste wird das Session Cookie im Browser eingegeben - der Angreifer hat nun die volle Kontrolle über die Session seines Opfers.

6. Der Angreifer ruft nun «mysignins.microsoft.com» im Browser auf und wird - dank Session Cookie - ohne weitere Anmeldung und mit bestandenem «MFA-Check» eingeloggt.

7. Der Angreifer ändert nun das Kennwort, entfernt die alte MFA-Authentifizierungsmethode und hat volle Kontrolle über den Account seines Opfers.

Am nächsten Tag möchte sich das Phishing-Opfer wie gewöhnlich im Outlook-Web anmelden. Es bemerkt, dass die Anmeldung aufgrund eines falschen Passworts nicht möglich ist und will das Passwort zurücksetzen. Der Link für das Zurücksetzen des Passworts wird jedoch an eine unbekannte Telefonnummer geschickt.

Das Phishing-Opfer hat nun seinen Microsoft Account trotz MFA verloren - obwohl MFA als Sicherheitsvariante lange Zeit ausreichend war.

SmartIT