Was ist ein Sitzungstoken, und warum ist der Diebstahl eines solchen schlimmer als der Diebstahl eines Passworts?

Kurze Antwort: Ein Sitzungstoken (Session Token) ist der Berechtigungsnachweis, den Ihr Browser oder Ihre App *nach* der Anmeldung besitzt und der beweist, dass Sie bereits authentifiziert sind. Der Diebstahl eines solchen Tokens ist oft schlimmer als der Diebstahl eines Passworts, da er in der Regel sowohl das Passwort als auch die Multi-Faktor-Authentifizierung umgeht — der Angreifer setzt einfach Ihre bestehende Sitzung fort.

Warum es das gibt

Bei jeder Anfrage das Passwort erneut einzugeben, wäre nicht praktikabel. Deshalb stellt der Dienst nach einer erfolgreichen Anmeldung ein Token aus. Jede weitere Anfrage trägt dieses Token anstelle Ihrer Anmeldedaten. Der Dienst vertraut darauf als Nachweis, dass Sie sich bereits authentifiziert haben.

Warum Angreifer es bevorzugen

- **Es umgeht MFA.** MFA wird bei der Anmeldung geprüft. Ein Token, das *nach* dieser Prüfung ausgestellt wird, repräsentiert eine bereits erfolgte Authentifizierung, sodass das erneute Verwenden dieses Tokens in der Regel nicht erneut den zweiten Faktor auslöst.
- **Es wirkt legitim.** Für den Dienst ist ein gültiges Token ein gültiger Benutzer. Es gibt kein Signal für fehlgeschlagene Anmeldungen und nichts Auffälliges, das einen Alarm auslösen würde.
- **Es ist übertragbar.** Viele Token funktionieren von einem anderen Rechner, Netzwerk oder Land aus.

Warum sich dadurch das Verhalten von Angreifern verändert hat

Angreifer vermeiden es zunehmend, sich lange in einem Netzwerk aufzuhalten. Ein längerer Verbleib erhöht die Wahrscheinlichkeit einer Entdeckung. Stattdessen entwenden sie Identitätsmaterial und verschwinden — um anschließend jederzeit als authentifizierter Benutzer zurückzukehren. Das Token ist eine legitim aussehende Hintertür, die vom Authentifizierungssystem selbst ausgestellt wurde.

Wie Cyber Crucible dem begegnet

Token-Diebstahl wird im Moment des Zugriffs gestoppt. Wenn ein Programm auf den Browser- oder Anwendungsspeicher zugreift, in dem Token abgelegt sind, wird dieser Zugriff in unter 200 Millisekunden bewertet. Ein übergriffiges, aber legitimes Programm erhält gefälschte Daten oder wird abgewiesen; ein unbekanntes oder kompromittiertes Programm wird abgelehnt oder ausgesetzt. In beiden Fällen wird das echte Token niemals preisgegeben.

Revision #1
Created 2026-07-24 04:28:50 UTC by Dennis Underwood
Updated 2026-07-24 04:28:50 UTC by Dennis Underwood