

Was ist ein Refresh-Token, und warum ist der Verlust eines solchen besonders schädlich?

Kurzantwort: Ein Refresh-Token ist ein langlebiges Zugangsdatum, das verwendet wird, um im Hintergrund neue Access-Token zu erhalten, ohne dass sich der Benutzer erneut anmelden muss. Darauf beruht die Funktion „Angemeldet bleiben“. Da damit potenziell unbegrenzt neuer Zugriff erzeugt werden kann, kann ein gestohlenes Refresh-Token einem Angreifer dauerhaften Zugriff verschaffen, weit über das Ende Ihrer Sitzung hinaus.

Access-Token vs. Refresh-Token

- **Access-Token (Sitzungs-Token):** kurzlebig, wird bei jeder Anfrage verwendet, läuft innerhalb von Minuten oder Stunden ab.
- **Refresh-Token:** langlebig, wird nur verwendet, um neue Access-Token anzufordern. Teilweise wochen- oder monatelang gültig.

Ein gestohlenes Access-Token läuft irgendwann ab. Ein gestohlenes Refresh-Token kann wiederholt verwendet werden, um neue Access-Token zu erzeugen – wodurch aus einem einmaligen Diebstahl dauerhafter Zugriff wird.

Warum „Angemeldet bleiben“ ein Kompromiss ist

Um angemeldet zu bleiben, muss etwas Dauerhaftes auf dem Gerät gespeichert werden. Genau diese Bequemlichkeit macht das gespeicherte Token für einen Angreifer wertvoll. Browser- und App-Zugangsdatenspeicher befinden sich an standardisierten, vorhersehbaren Orten, sodass automatisierte Tools direkt darauf zugreifen.

Schadensbegrenzung

Das Widerrufen eines Refresh-Tokens macht den damit erzeugbaren Zugriff ungültig – deshalb sind „Von allen Geräten abmelden“ und der Widerruf von Token nach jedem Verdacht auf eine

Kompromittierung so wichtig. Ein Widerruf ist jedoch eine Reaktion, die *nach* dem Diebstahl erfolgt.

Der Ansatz von Cyber Crucible besteht darin, das Auslesen von vornherein zu verhindern. Der Zugangsdatenspeicher ist ein geschützter Ort: Ein legitimes Programm, das dort unbefugt zugreifen will, erhält gefälschte Daten oder wird abgewiesen, während ein unbekanntes oder kompromittiertes Programm blockiert oder gesperrt wird. Das Refresh-Token selbst wird niemals preisgegeben.

Revision #1

Created 2026-07-24 04:29:02 UTC by Dennis Underwood

Updated 2026-07-24 04:29:02 UTC by Dennis Underwood