Grundsätzlich bist Du mit der Verwendung eines VPN-Services sehr gut geschützt. Wir raten dennoch Gegenmaßnahmen gegen IP-Leaks aufgrund von WebRTC (**Web Real-Time Communication**, deutsch „Web-Echtzeitkommunikation“) einzuleiten. Ob du von einem Leak betroffen bist kannst du mit Hilfe unseres WebRTC Leak Check herausfinden

IP-Leak

In Verbindung mit WebRTC können private IP-Adressen trotz VPN-Verbindung über JavaScript ausgelesen werden. Das Beispiel Firefox Hello schließt Rechner hinter einer Firewall und mit privaten IP-Adressen aus. Deshalb kann eine Website mit JavaScript einen STUN-Server nach der tatsächlichen IP-Adresse fragen lassen. Dies hat zur Folge, dass Anonymisierungsdienste ihren Zweck nicht mehr erfüllen und keinen Schutz mehr vor einem IP-Leak bieten können.

Gegenmaßnahmen

Zum Schutz vor einem IP-Leak bieten sich zwei Vorgehensweisen an. Eine Anleitung wie du WebRTC deaktivieren kannst haben wir dir in unserem Blog zusammengefasst. Eine Option bietet die Installation von **Add-Ons/Plugins WebRTC Leak Prevent**, um potenzielle IP-leaks zu managen. Ebenfalls verfügbar ist seit Ende 2016 die Erweiterung **Easy WebRTC Block**, welche auch in einer Version für **Opera** existiert.

Die andere Möglichkeit ist eine Änderung der Einstellungen im Browser.

Im Firefox kann über about:config der Wert media.peerconnection.enabled auf false gesetzt werden, wodurch ein IP-Leak verhindert wird.

Mehr zum Thema WebRTC unter: https://de.wikipedia.org/wiki/WebRTC

IP Leak aufgrund WebRTCs verhindern

SpyOFF Support
https://hilfe.spyoff.com/TroubleshooterGuide50077.aspx