PRESSEMITTEILUNG

Abgesichert gegen WebRTC: Steganos Online Shield VPN schützt weiter echte IP-Adressen

- **WebRTC verrät IP-Adresse und Standort**
- **Steganos Online Shield VPN bleibt weiterhin voll funktionstüchtig**
- **Mit nur einem Klick wird WebRTC-Schutz aktiviert**

Berlin, 05. Februar 2015 – Wie in den letzten Tagen bekannt wurde, plaudern sowohl Mozilla Firefox als auch der Google-Browser Chrome trotz aktivierter VPNs die IP-Adressen der Nutzer aus. Als Grund dafür nennt der Entwickler Daniel Roesler die Implementierung von WebRTC. Mit Steganos Online Shield VPN bleibt die VPN-Verbindung gegen WebRTC abgesichert: Internetnutzer können mit dem von Steganos (www.steganos.com) entwickelten VPN-Tool weiterhin ihre echte IP-Adresse und damit ihren Standort sicher verschleiern.

WebRTC: Eine Gefahr für die Preisgabe von Standort und IP-Adresse

Bei WebRTC (Web Real-Time Communication) handelt es sich um eine Technik zur Echtzeitkommunikation im Browser. Damit wird Webseiten mittels eines einfachen JavaScripts die Möglichkeit gegeben, lokale und WAN-IPs zu ermitteln, und so bestimmten Diensten die Erlaubnis erteilt, direkt miteinander zu kommunizieren – beispielsweise für Telefonate und Video-Chats ohne Plug-ins im Browser. Es werden dabei Requests an sogenannte STUN-Server (Session Traversal Utilities for NAT) abgesetzt, die über alle im Rechner vorhandenen Adapter gesendet werden, um die vorhandenen IPs zu ermitteln. Bei VPNs wird in der Regel jeglicher Traffic durch den VPN-Tunnel gesendet. Da jedoch bei Default-Einstellungen in der OpenVPN-Konfiguration die 'normale' Route über den Standardgateway nicht gelöscht wird, kann jene am VPN vorbei benutzt werden, um den STUN-Request abzusetzen – die echte IP-Adresse kann so ermittelt werden.

Web-Browser: Steganos Online Shield VPN bleibt funktionstüchtig

Das VPN-Tool von Steganos bietet sowohl für Google Chrome als auch für Mozilla Firefox folgende Lösung, um WebRTC zu unterdrücken: Indem die Route über den Standardgateway während der VPN-Verbindung entfernt wird, kann die echte IP-Adresse nicht mehr nach außen gelangen. Mit nur einem Klick unter „Einstellungen“ direkt in der Software lässt sich der WebRTC-Schutz aktivieren. Solange der Schutz im Steganos Online Shield VPN aktiv ist, besteht keine Möglichkeit über WebRTC an die wahre IP-Adresse zu kommen.

Selbsttest offenbart IP-Lücke

Ob ein Browser das Auslesen der originalen IP-Adresse zulässt, kann jeder Nutzer sehr schnell selbst herausfinden. Dafür empfiehlt sich ein Besuch der Seite: https://diafygi.github.io/webrtc-ips/

Pressematerial

Druckfähiges Bildmaterial und die Pressemeldung zum Download finden Sie hier: https://www.steganos.com/de/unternehmen/presse-center/

Über Steganos Software GmbH

Steganos ist seit über 15 Jahren die Referenz beim Schutz der digitalen Privatsphäre. Das 1997 in Deutschland gegründete Unternehmen stellt bekannte Sicherheitsprodukte wie Steganos Privacy Suite, Steganos Passwort-Manager und Steganos Online Shield her. Mehr Infos erhalten Sie unter www.steganos.com

Pressekontakt

Steganos Software GmbH
Kristin Winter-Shangama
Immanuelkirchstraße 4
10405 Berlin
Telefon: +49 - 30 - 4849 27 78
E-Mail: kwinter@steganos.com