Freies Internet für freie Bürger

Wie Surfer Netzsperren und Zensur umgehen

Findige Bürger nutzen VPNs, Tor und Anti-Zensur-Dienste, um Internetsperren in Russland und China zu umgehen. Der folgende Überblick zeigt die Stärken und Schwächen der aktuell beliebtesten Tools.

Von Ronald Eikenberg

Das freie und unzensierte Internet, wie wir es kennen, scheint ein Auslaufmodell zu sein: Zunehmend werden Inhalte gesperrt, sei es aus politischer Motivation oder aus Jugendschutzgründen. Was in China durch die Great Firewall Alltag ist, erreicht langsam auch andere Länder, darunter Russland. Einen guten Überblick über die Situation liefern die Daten des Open Observatory of Network Interference (OONI). Sie zeigen, wann der Kreml den Zugriff auf die internationale Berichterstattung von BBC, Deutsche Welle und Voice of America einschränkte (siehe ct.de/yxa3).

Angesichts der Kriegssituation und der Sperren von Medien verwundert es nicht, dass VPN-Apps die Top 10 der App-Stores bei Abrufen aus Russland dominieren. Überraschend ist es dennoch, denn in Russland ist der Gebrauch von Methoden, die Sperrungen für unerwünschte Inhalte umgehen, seit 2017 verboten (siehe ct.de/yxa3). Aber anscheinend hat Russland – anders als China – die App-Store-Betreiber bisher nicht zwingen können, VPN-Apps aus dem länderspezifischen Angebot zu tilgen. Außerdem deutet der intensive Gebrauch von VPN-Apps darauf hin, dass der russische Gesetzgeber die Nutzung zumindest nicht merklich ahndet, wenn überhaupt.

Bekannt ist immerhin, dass der Kreml Zugriffe auf einige VPN-Dienste gesperrt hat. Es gibt aber immer noch Ausweichmöglichkeiten zu anderen VPN-Diensten von Unternehmen und Initiativen gegen Zensur. Außerdem kann man Tunnel in Eigenregie aufsetzen, beispielsweise über SSH zu Root-Servern im Ausland.

Bei VPN baut man über den lokalen Internetzugang einen verschlüsselten Tunnel zum VPN-Server eines Anbieters auf. Der Server kann in einem beliebigen Land stehen und von dort aus geht der Verkehr weiter ins Internet – fast so, als sei man vor Ort. Allerdings muss man dem Anbieter vertrauen.

Kommerzielle VPN-Angebote sind nur eingeschränkt empfehlenswert. Auch wenn viele behaupten, die Internet-Bewegungen ihrer Kunden nicht zu protokollieren, überprüfen kann man das nicht. Grundsätzlich ist es eine gute Idee, sich an jene zu halten, die sich beharrlich einen guten Ruf aufgebaut haben und nicht mit aggressiven Rabattaktionen auffallen. Eine Übersicht finden Sie in c't 18/2021 [1]. Einen soliden Eindruck haben dort zum Beispiel AzireVPN, IVPN und Mullvad hinterlassen.

Abstand nehmen sollte man in aller Regel von Gratisangeboten, denn bei denen gilt der Grundsatz „wenn du nicht der Kunde bist, dann bist du die Ware". Der Betrieb eines VPN-Servers kostet Geld und das holt sich der Betreiber so oder so. Im besten Fall ist der Gratiszugang ein Lockversuch, um Kunden für kostenpflichtige Abos zu gewinnen, im schlechtesten Fall interessiert sich der Anbieter für die übertragenen Daten.

Man kommt also vom Regen in die Traufe. Es gibt bei den Gratisdiensten aber auch Ausnahmen: Bei spendenfinanzierten VPN-Diensten wie RiseUp VPN geht es den Betreibern darum, Kommunika-

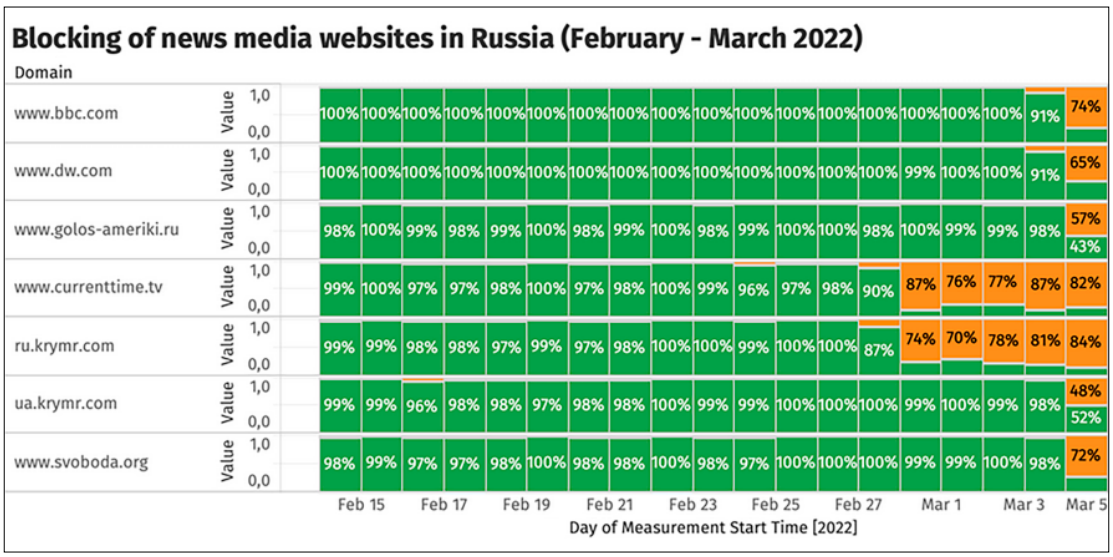
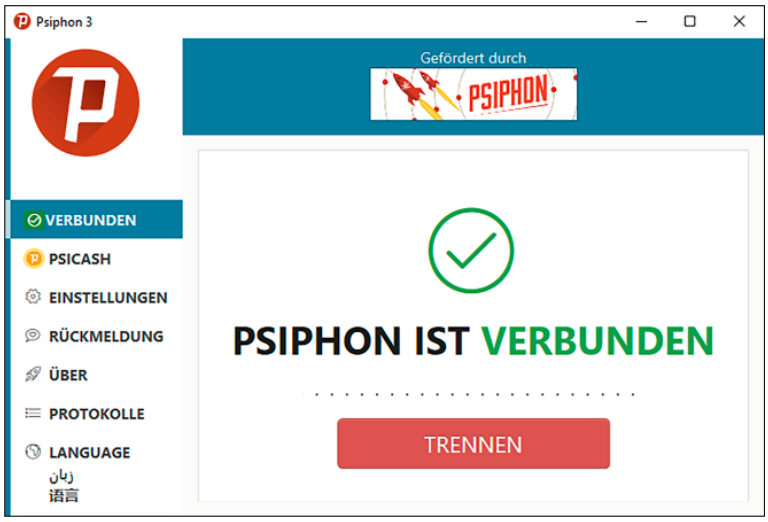


Bild: OONI

Das Open Observatory of Network Interference (OONI) beobachtet seit Ende Februar Anomalien beim Zugriff auf internationale Websites aus Russland.



Die Psiphon-App baut auch unter schwierigen Bedingungen einen Tunnel ins freie Internet auf.

tionswege zu schaffen, die nicht von Unternehmen oder Regierungen kontrolliert werden.

Anti-Zensur-Tool Psiphon

VPN-Traffic ist meist anhand der IP-Adressen der VPN-Server und der Kommunikations-Ports erkennbar. Eine Firewall kann solche Verbindungen leicht identifizieren und blockieren. Mittels Traffic Fingerprinting ist der VPN-Verkehr sogar dann identifizierbar, wenn er unübliche Ports nutzt. Dann helfen spezialisierte Dienste und Tools wie Psiphon weiter.

Durch die aktuellen weltpolitischen Ereignisse verzeichnet Psiphon einen deutlichen Anstieg an Nutzern aus Russland, Belarus und der Ukraine. Die quelloffene Anti-Zensur-Software, die aus einem Projekt des Citizen Lab der University of Toronto hervorgegangen ist, probiert mehrere Verbindungswege und Server durch, bis eine Verbindung steht. Zu den Verbindungswegen zählen das VPN-Verfahren L2TP mit IPsec, HTTP-Proxy und Obfuscated SSH (OSSH), welches den Verkehr vor gängigen Fingerprinting-Methoden verbirgt. Die vollständige Serverliste ist dem Client zu keinem Zeitpunkt bekannt, um Zensur zu erschweren.

In der kostenlosen Version liefert der Dienst maximal 2 Mbit/s, was zum Surfen knapp ausreicht. Zudem gibt es moderate Werbung. Mehr Speed und Werbefreiheit kosten ein paar Euro im Monat. Der Client ist auf https://psiphon.ca für Windows, macOS, Android und iOS erhältlich.

Internationale Sender wie BBC und Deutsche Welle (DW), die von den Netzsperren unmittelbar betroffen sind, empfehlen Psiphon, um ungehindert auf deren Nachrichtenangebote zugreifen zu können. In die von der Deutschen Welle angebotenen App „Breaking World News“ ist Psiphon sogar integriert. Schaltet man in den Einstellungen „Proxy aktivieren“ ein, kommuniziert die App über das Anti-Zensur-Netz und ist so auch in Ländern nutzbar, die den üblichen Zugriff auf DW blockiert haben.

Tor zur Welt

Geht es um maximalen Schutz der Privatsphäre, dann ist Tor das Mittel der Wahl. Dabei wird der Traffic zwischen Client und Internet verschlüsselt durch drei zufällig ausgewählte Relays geschleust, die jeweils nur die nächste Zielstation kennen, nicht aber die vollständige Route.

Tor hat allerdings auch Nachteile: Durch die Verschlüsselung und die zusätzlichen Relays nimmt die Signallaufzeit zu, was zu einem deutlich verlangsamten Aufbau von Webseiten führen kann. Und das letzte Glied in der Kette, der Exit Node, ist kritisch: Auch er weiß zwar nicht, für welche Nutzer er arbeitet, kann den Traffic Richtung Internet jedoch mitlesen und manipulieren, was für manche autokratisch regierten Länder bereits belegt wurde. Daher sollte man mit Tor nur transportverschlüsselte Protokolle wie HTTPS nutzen.

Snowflake gegen Tor-Sperren

Auch Tor lässt sich blockieren, etwa durch Firewallsperren für bestimmte Ports. Dann kann man sich behelfen, indem man austauschbare Übertragungsarten (Pluggable Transports) verwendet, die den Tor-Traffic zum Beispiel als Surfverkehr tarnen (siehe ct.de/yxa3). Solche Übertragungsarten kann man in den Einstellungen des Tor-Browsers unter „Bridges“ aktivieren.

Snowflake lebt von freiwilligen Helfern, denn je mehr es davon gibt, desto schwieriger lassen sich die Verbindungen blockieren. Mithelfen kann jeder: Installiert man etwa die Browser-Erweiterung für Chrome oder Firefox (siehe ct.de/yxa3), wird der eigene PC zum Snowflake-Proxy, der anderen Nutzern ins Tor-Netz hilft.

Den Tor Browser gibt es für Windows, macOS, Linux, Android und iOS (siehe https://torproject.org). Wer seinen digitalen Fußabdruck auch auf dem lokalen Rechner so gering wie möglich halten möchte, kann zu dem Live-Linux Tails greifen, das standardmäßig über Tor mit dem Internet spricht.

Alternative DNS-Server

Nicht immer ist es nötig, den kompletten Internetverkehr umzuleiten, um Zensurmaßnahmen zu umgehen. In manchen Fällen werden Web-Zugriffe nur anhand von Filtern in DNS-Server zensiert. Fragt der PC oder das Smartphone nach einer gesperrten Domain, antwortet der Server, dass er die Domain nicht kennt oder liefert eine falsche IP-Adresse.

In diesem Fall genügt es, einen anderen Server zu konfigurieren, zum Beispiel den zensurfreien DNS-Server von Digitalcourage (siehe ct.de/yxa3). Wer das Mitlesen des DNS-Verkehrs verhindern will, richtet eine verschlüsselte DNS-Kommunikation ein (DNS-over-HTTPS, DoH oder DNS-over-TLS, DoT). Neuerdings lässt sich die DNS-Kommunikation auch anonymisieren [2].

Fazit

Der freie Zugriff auf Informationen ist keine Selbstverständlichkeit, wie die aktuellen Entwicklungen in Russland zeigen. Doch findige Programmierer haben diverse Methoden implementiert, um die Restriktionen zu umgehen. Dabei sind einfache VPN-Dienste nicht immer die beste Wahl, da sie sich leicht blockieren lassen. Mit Anti-Zensur-Tools wie Psiphon oder Tor ist jedoch oft auch unter schwierigen Bedingungen ein Zugriff aufs freie Netz möglich. *(rei@ct.de)* c't

Literatur

[1] Keywan Tonekaboni, Tunnelblick, Elf VPN-Anbieter mit WireGuard im Vergleich, c't 18/2021, S. 18
[2] Dušan Živadinović, Absender unbekannt, Privatsphärenschutz mit DNSCrypt-Proxy einrichten, c't 21/2021, S. 110

Statistiken & Tools: ***ct.de/yxa3***