Am letzten Donnerstag berichteten die NachDenkSeiten über einen skandalösen Vorgang. Drei unserer Leser berichteten uns unabhängig voneinander, dass sie unsere Seite nicht mehr aufrufen können und der technische Support ihrer jeweiligen Provider dies damit erklärte, dass die NachDenkSeiten „wegen der EU-Sanktionen gegen Russland gesperrt seien“. Wir fragten unsere Leser, ob sie ähnliche Probleme haben. Es kamen zahlreiche Antworten und auch hilfreiche Tipps, die wir an dieser Stelle gerne weitergeben wollen. Von **Jens Berger**.

Dieser Beitrag ist auch als Audio-Podcast verfügbar.

https://www.nachdenkseiten.de/upload/podcast/221221_Netzsperren_gegen_die_NachDenkSeiten_ein_Zwischenstandsbericht_NDS.mp3

Podcast: Play in new window | Download

Fangen wir mit dem Positiven an: Auch wenn zahlreiche unserer Leser über Verbindungsprobleme in den letzten Wochen klagten, bleibt die Zahl der nachweislich von Netzsperren betroffenen Leser überschaubar und scheint sich auf einige wenige kleine Provider zu konzentrieren. Kurz nach unserer Veröffentlichung und unseren Mail-Anfragen an die betreffenden Provider haben sich die Sperren offenbar in Luft aufgelöst. Eine Antwort bekamen wir jedoch nicht. Selbstverständlich werden wir uns damit nicht zufriedengeben und loten gerade rechtliche Schritte und die Möglichkeit von Beschwerden über diese Provider bei der zuständigen Bundesnetzagentur aus. Derartige Sperren sind keine Petitesse, sondern ein klarer Verstoß gegen den Grundsatz der Netzneutralität. Da die Netzsperren offenbar von kleineren Providern, dafür aber koordiniert und zeitgleich, erfolgten, liegt der Verdacht nahe, dass jemand gesetzwidrig die NachDenkSeiten auf eine zentrale Sperrliste gesetzt hat, die von diesen Providern übernommen wurde. Aber das ist zugegebenermaßen zurzeit noch spekulativ.

Ein Großteil der Leserzuschriften hatte glücklicherweise zum Inhalt, dass keine

nennenswerten Probleme vorlagen. Jedoch berichteten auch einige Leser von ernsteren technischen Problemen beim Aufruf unserer Seiten, die jedoch vom Schema her nicht auf Netzsperren, sondern auf Verbindungsprobleme hindeuten. Unsere Technik wird noch prüfen, was davon in unserem Verantwortungsbereich liegt und gegebenenfalls die nötigen Optimierungen vornehmen. Wir bedanken uns bei allen Leserinnen und Lesern, die uns durch ihre Zuschrift informiert und geholfen haben. Leider können wir nicht jede Mail persönlich beantworten.

Unter den Zuschriften gab es jedoch auch rund ein Dutzend Mails, die auf konkrete Probleme durch Netzsperren im Zeitraum von Montag bis Mittwoch letzter Woche hindeuten. Auch hier geht es vornehmlich um kleinere, meist von Stadtwerken betriebene Provider. Diese Fälle prüfen wir nun. Wir halten Sie auf dem Laufenden.

Unabhängig vom konkreten Fall der Netzsperren erreichten uns auch zahlreiche hilfreiche Tipps, wie Nutzer sich generell technisch gegen den Missbrauch von Netzsperren und anderen Zensuranstrengungen seitens des Staates und privater Anbieter schützen können. Einige dieser Vorschläge, die auch für technische Laien umsetzbar sein dürften, möchten wir Ihnen heute vorstellen. Diese Tipps sind übrigens auch hilfreich, wenn Sie weiterhin das Angebot von seitens der EU zensierten Medien wie RT nutzen wollen.

1. **Nutzung des Tor-Browsers**

   Parallel zu den herkömmlichen Verbindungsprotokollen, auf die die bekannten Browser Firefox, Chrome, Safari oder Edge aufsetzen, gibt es noch den in der Öffentlichkeit weniger bekannten Tor-Browser. Unter der Motorhaube greift dieser Browser auf das sogenannte Tor-Netzwerk zu, das über das Onion-Routing ein anonymes Surfen im Internet ermöglicht. Und das ist auch der große Vorteil dieser Lösung. Die Umgehung von Netzsperren ist hier eigentlich eher ein „Nebeneffekt“. Der Tor-Browser ist für Windows, macOS, Linux und Android erhältlich und kann auf der Seite des Projekts heruntergeladen werden. Für Nutzer von Apples Smartphone-Betriebssystem iOS empfiehlt sich die Nutzung des alternativen Onion-Browsers, der technisch ähnlich arbeitet. Ein Nachteil dieser Lösung ist freilich, dass die Geschwindigkeit im Vergleich zu den traditionellen Browsern, die über das normale Netz kommunizieren, geringer ist.

2. **VPN-Anbieter**

   Eine weitere Möglichkeit, Ihre Herkunft zu verschleiern und die deutschen Sperrlisten zu umgehen, sind VPN-Anbieter. Diese bieten – vereinfacht gesagt – eine

Softwarelösung an, mit der ihr gesamter Außenverkehr mit dem Internet über einen anderen Server als den ihres Providers gesteuert wird. Bei den größeren VPN-Anbietern können Sie sich beispielsweise aussuchen, ob dieser Server nun in Deutschland, der Schweiz, Island, Singapur oder einem anderen Land steht. Die Server dieser Anbieter haben in der Regel keine Sperrlisten oder ähnliches und wenn Sie eine Internetseite über einen VPN-Server aufrufen, können die Seitenbetreiber Sie nur bis zu diesem VPN-Server zurückverfolgen. Seiten, die beispielsweise in Deutschland oder der EU gesperrt sind oder von sich aus Nutzer aus bestimmten Ländern sperren, können Sie so über einen VPN-Server außerhalb der EU in der Regel problemlos aufrufen.

Ein großer Vorteil ist, dass die Software der größeren VPN-Anbieter sich nahtlos in die verbreiteten Betriebssysteme integriert und so auch von Laien einfach zu bedienen ist, zumal man seinen gewohnten Browser weiterbenutzen kann. Sie sollten jedoch aufpassen, wenn Sie Angebote nutzen, die sich nur an deutsche Kunden richten – wie z.B. bestimmte Inhalte der Mediatheken der Öffentlich-Rechtlichen oder der Streamingangebote von Netflix, Amazon und Co. Hier empfiehlt es sich, den VPN abzuschalten oder für dieser Angebote eine Ausnahme einzurichten.

Der wohl größte Nachteil ist, dass der Betrieb von VPN-Servern Kosten mit sich bringt und die allermeisten Angebote daher nicht kostenfrei sind. Beispiele für VPN-Anbieter sind Perfect Privacy oder der Marktführer NordVPN, die auch von Mitarbeitern der NachDenkSeiten genutzt werden.

Einige Leser wiesen uns auch auf den Opera-Browser hin, der eine eingebaute kostenlose VPN-Lösung enthält.

3. **DNS-Einträge**

Netzsperren setzen in der Regel bei der Auflösung des Domainnamens bei ihrem Provider an. Wenn Sie also z.B. die Adresse nachdenkseiten.de aufrufen, übersetzt der Zugangsrechner ihres Providers dies in eine IP-Adresse und lenkt den Datenverkehr auf die entsprechenden Server im Internet. Wenn ein Provider eine Netzsperre verhängt, heißt dies konkret, dass der Eintrag, also nachdenkseiten.de, nicht mehr in eine IP-Adresse übersetzt wird und der Datenverkehr nicht mehr eingeleitet werden kann. Um dies zu umgehen, hilft in den meisten Fällen bereits der Eintrag eines alternativen DNS-Servers in ihrem Betriebssystem. Das „Übersetzen“ der Internetadresse erledigt dann nicht mehr der Server ihres Providers, sondern dieser alternative „Domain Name Server“.

Empfehlenswert sind hier die Angebote von digitalcourage. Aber auch die DNS-Server der großen US-Konzerne Google oder Cloudflare ermöglichen in den allermeisten Fällen eine problemlose Umgehung von Netzsperren und haben eine einwandfreie Performance. Sollten Sie jedoch aus Datenschutzgründen diesen Konzernen misstrauen, empfiehlt sich die Nutzung eines anderen Anbieters.

Leitfaden: Die besten kostenlosen und öffentlichen DNS-Server im Jahr 2022

Wenn du dich bereits mit DNS-Servern auskennst, findest du hier die komplette Liste, damit du sofort loslegen kannst.

DNS-Anbieter	Primäre Adresse	Sekundäre Adresse
1. Google Public DNS	8.8.8.8	8.8.4.4
2. Cloudflare	1.1.1.1	1.0.0.1
3. OpenDNS	208.67.222.222	208.67.220.220
4. CyberGhost	38.132.106.139	194.187.251.67
5. Quad9	9.9.9.9	149.112.112.112
6. OpenNIC DNS	192.71.245.208	94.247.43.254
7. DNS.Watch	84.200.69.80	84.200.70.40
8. Yandex DNS	77.88.8.88	77.88.8.2
9. Neustar DNS	156.154.70.5	156.154.71.5
10. CleanBrowsing	185.228.168.9	185.228.169.9
11. Comodo Secure	8.26.56.26	8.20.247.20
12. UncensoredDNS	91.239.100.100	89.233.43.71
13. FreeDNS	45.33.97.5	37.235.1.177
14. Verisign Public DNS	64.6.64.6	64.6.65.6
15. SafeServe	198.54.117.10	198.54.117.11
16. Safe DNS	195.46.39.39	195.46.39.40
17. AdGuard	176.103.130.130	176.103.130.131

Ein Problem könnte sein, dass sie diese Einträge manuell vornehmen müssen. Wie das geht, wird z.B. hier für Windows 10 und hier für MacOS erklärt. Zu beachten ist, dass manuelle DNS-Server nur Netzsperren umgehen und keine Vorteile bei der Anonymität bieten. Sie sind weiterhin über ihren Provider verbunden und der

Datenverkehr lässt sich von der aufgerufenen Internetseite zurückverfolgen.

Titelbild: ivector/shutterstock.com