Datenschutz - Wie schütze ich mich?

Es gibt Empfehlungen, für besseren Schutz der Daten den Tor Browser und Open Source Software zu verwenden, z.B. hier:

https://prism-break.org

Sie erreichen durch die Zwischenschaltung der Tor Server Folgendes:

- Verschlüsselung der Daten **während der Übertragung**
- Anonymisierung Ihrer Abfrage **gegenüber der abgefragten Webseite**
- der Inhalt Ihrer Abfragen kann nicht mehr von dem nationalen Internetprovider nachvollzogen werden, wohl aber die Tatsache, dass Sie über Tor surfen.

Ziel des Tor Netzwerkes ist es, staatliche Zensur zu umgehen. Ihre Abfragen können weiterhin von den Betreibern des Tor Netzwerkes (insbesonders der Betreiber von Exit Nodes) nachvollzogen werden. Die Exit Nodes (letzte Server über die die Abfrage ausgeführt wird) sind nicht anonym und erhalten die Daten im Klartext. Sie sind eine zusätzliche Sicherheitslücke, wenn ihre Betreiber Logins und Passwörter auslesen.

Man kann das Tor Netzwerk unterstützen, indem man selbst Server bereitstellt - eine Anleitung findet sich hier. Allerdings macht die Nutzung von TOR besonders verdächtig - auch TOR wird von der NSA ausgespäht.

Annähernd anynonymes Surfes erfordert hohe Aufmerksamkeit der Nutzer..

Sinnvoll - und wichtiger - ist es auf Verschlüsselung zu achten. Auch die verfügbaren Verschlüsselungen sind kein vollständiger Schutz, sie erschweren das Lesen übermittelter Daten lediglich.

Der russische Geheimdienst arbeitet bei wirklich vertraulichen Dingen mit der Schreibmaschine, handschriftlich und mit althergebrachten Telefonleitungen.

Aktuell wird Datenschutz wieder in der Diskussion um die Förderung der Entwicklung Künstlicher Intelligenz.

Anonymität im Internet

Barbara Funke - Online Publizistik und -PR - www.bfunke.de
