

### **Teil 3: Anonym im Internet surfen - einfach erklärt!**

Dieser Teil ist grandios erläutert aber Ergänzungen hätte ich dennoch:

1. Der Tor-Browser hat standardmäßig „https everywhere“ an Bord (siehe oben) und das auch in anderen Browsern nützliche „NoScript“. Das ist ein Add-on, das alles, was sich unerlaubt bewegen möchte zunächst unschädlich macht. Wer sich Mediendateien anhören oder ansehen möchte, muss das ausdrücklich gestatten (temporär oder, bis zum Widerruf, permanent). Was auch immer gerade nicht funktionieren mag, ein paar Sekunden Lebenszeit für das Nachdenken vor der Freigabe von Funktionen sollten immer zur Verfügung stehen.
2. Die Anonymität des Tor-Browsers bleibt nur dann unangetastet, wenn die Größe des Browserfensters nicht verändert wird und auch sonst keine für Dritte erkennbaren Änderungen vorgenommen werden. Die Wirkung beruht auf dem verschleierte und verschlüsselten Transportweg über zufällig gewählte Server und, wenn am Ziel, dem Untertauchen in der Masse gleichartig konfigurierter Browser ohne identifizierbaren „Fingerabdruck“.

Zum ersten Punkt hat sich Frank Rieder (CCC) im bereits erwähnten Video im 2. Teil eindeutig geäußert. Alle Medien, ob Bild oder Ton sind kompromittierbar und alle Browser können über unentdeckte, unbekannte oder bisher nicht beseitigte Schwachstellen das Einfalltor für Schädlinge sein. Es ist wie bei manchen wilden Tieren, was schön oder niedlich ist, kann trotzdem gefährlich sein.