Capulcu: Digitale Selbstverteidigung mit TAILS

► **von https://capulcu.blackblogs.org/**

Anleitung zur Nutzung des Tails-Live-Betriebssystems für sichere Kommunikation, Recherche, Bearbeitung und Veröffentlichung sensibler Dokumente.

Seit den „späteren“ Snowden-Veröffentlichungen vom März 2014 wissen wir leider mit Sicherheit, dass die Geheimdienste NSA [1], GCHQ [2] und weitere für eine maßgeschneiderte Infiltration unserer Rechner keine menschlichen Hacker mehr benötigen, sondern automatisiert mit dem Spionageprogramm “Turbine” unbemerkt spezifische Schnüffel-Software auf unseren Rechnern installieren.

Wir empfehlen angesichts dieser Angreifbarkeit über massenhaft infizierte Rechner, Tails als unveränderliches „Live-Betriebssystem“ für das Kommunizieren, die Recherche, das Bearbeiten und Veröffentlichen von sensiblen Dokumenten zu benutzen. Ein Live-Betriebssystem ist ein eigenständiges Betriebssystem, was von DVD oder USB-Stick gestartet werden kann, ohne es zu installieren. Euer Standard-Betriebssystem auf der Festplatte wird nicht angefasst

Tails hilft euch bei der Bearbeitung von sensiblen Text-,Grafik- und Tondokumenten. Tails verwendet beim Surfen, Mailen und Chatten automatisch die Anonymisierungssoft ware „Tor“ und verändert zusätzlich die sogenannte „MAC-Adresse“ eurer Netzwerkkarte. Was das ist und wozu das von Nutzen ist, erklärt euch die Einführung dieser Anleitung.

❖ **[3]weiterlesen [4]**

Quell-URL: https://kritisches-netzwerk.de/content/widerstand-gegen-den-digitalen-zugriff-widerstand-gegen-spionageprogramme?page=51#comment-0

Links
[1] http://de.wikipedia.org/wiki/National_Security_Agency
[2] http://de.wikipedia.org/wiki/Government_Communications_Headquarters
[3] http://www.kritisches-netzwerk.de/forum/klage-gegen-israels-regierungschef-netanjahu-chile-eingereicht
[4] http://www.kritisches-netzwerk.de/forum/widerstand-gegen-den-digitalen-zugriff-capulcu-digitale-selbstverteidigung-mit-tails