Mit einer DNS-Verschlüsselung surft man noch sicherer

29. April 2018

Über sicheres und privates Surfen im Internet haben wir in der Vergangenheit schon oft berichtet. Einen großen Anteil an Sicherheit und Privatsphäre haben Proxyserver und VPN. Doch diese Verschlüsselungsvarianten haben oft auch einige Lücken.

Sie verschlüsseln beim Surfen zwar das Wo und das Was, vernachlässigen aber oft das Wer. Insbesondere dann, wenn die Clients nicht korrekt konfiguriert wurden.

Das **DNS** (Domain Name System) wandelt die Namen von Webseiten in numerische IP-Adressen um, damit die Datenpakete zwischen dir und der Webseite ausgetauscht werden können. Dies geschieht in der Regel unverschlüsselt und wird von deinen Internet Service Provider durchgeführt.

Der Provider (z. B. Kabel Deutschland oder Unitymedia) weiß genau, wen du wann kontaktierst, auch wenn er nicht sehen kann, welche Daten ausgetauscht werden. Ebenso kann er Webseiten zensieren (DNS-Blocking).

Um noch sicherer zu surfen, kannst du den DNS-Datenverkehr mit dem Gratis-Tool **Simple DNSCrypt** verschlüsseln. Nach dem Download der Software schaltest du die Verschlüsselung einfach nur mit dem Schalter **DNSCrypt Dienst** ein.

Lediglich bei **WLAN-Hotspots,** die eine Anmeldeseite vorgeschaltet haben, kann es vorkommen, dass die Verschlüsselung nicht sofort funktioniert. In diesem Fall aktivierst du **Simple DNSCrypt** erst **nach der Anmeldung**.

Simple DNSCrypt ist ab Windows 7 mit allen Versionen kompatibel.