

# Nur bestimmte Verschlüsselungen sicher

**Hamburg.** Selbst der US-Geheimdienst NSA kann bestimmte Verschlüsselungsmaßnahmen nicht aushebeln. Die Verfahren PGP zum Schutz von E-Mails sowie die »Off-the-record«-Verschlüsselung von Chats (OTR) sind diesbezüglich geschützt. Das erläuterte der Sicherheitsexperte Jacob Appelbaum auf dem Chaos Communication Congress (31C3) am Sonntag abend in Hamburg, wo er die Recherchen vorstellte. Die NSA könne aber das Verschlüsselungsprotokoll SSL überwinden, führte der Aktivist aus. SSL wird verwendet, um Webseiten-Aufrufe und Eingaben gegen Überwachung zu schützen – etwa beim Onlinebanking. (dpa/jW)

*<https://www.jungewelt.de/artikel/253994.nur-bestimmte-verschlüsselungen-sicher.html>*