

Hide and Seek



Manchmal muss man sich über die Berichterstattung bei Heise doch wundern. Wenn jemand sachlich und richtig technische Themen im Internet dargestellt haben möchte, wer sollte sonst vernünftig aufklären?

[Aktuell](#): „Missing Link: Wie Staaten die Verschlüsselung im Internet per Gesetz aushebeln“. Der Artikel ist zwar lang, aber, mit Verlaub, richtig schlecht.

Erstens: Was ist überhaupt gemeint? [Transportverschlüsselung](#) oder [Ende-Ende-Verschlüsselung](#) der Nutzer? Oder gar beides?

Zweitens: Hat das irgendjemand angekündigt, die üblichen Verdächtigen hätten es gern (gähn) oder geschieht es real?

Drittens: Geht es um eine gesetzliche Grundlage, Verschlüsselung zu verbieten oder möchte man es nur umsetzen oder beides?

Viertens: Geht es um die Provider oder um die so genannten Endverbraucher oder beide?

Fünftens: Oder geht [es um alles](#), Politiker haben aber keinen

blassen Schimmer und raunen deshalb geheimnisvoll herum? „... nicht zuletzt der Einbau von Verschlüsselung in Basisprotokolle des Internets drohe den Zugriff auf kriminelle Inhalte zu erschweren“ – großes Bullshit-Bingo!

[Australiens Assistance and Access Act](#) ist gerade hoch im Kurs bei denen, die auch für Europa ein Anti-Verschlüsselungsgesetz fordern. (...) Bei den Technical Assistance Requests (TARs), versorgen die Provider die australische Polizei sowie die verschiedene Geheimdienste mit entschlüsselten Daten von Zielpersonen.

Entschlüsselte Daten von Zielpersonen? Meinen sie die Zugangsdaten für E-Mail-Konten? (Was hülfe das?) Zugangsdaten für Websites und Social Media? Oder möchten jemand – am besten per Ferndiagnose – meine [Veracrypt](#)-Passwörter entschlüsseln? Have fun!

Australiens Regierung tritt dem Vorwurf, Hintertüren einzubauen, mit einer eigenen FAQ entgegen, in der sie über „Mythen“ spricht, die über das Gesetz verbreitet wurden.

Hintertüren? Ich will ja nicht schon wieder über die so genannte Online-Durchsuchung zeteren (wenn die funktionierte, brauchte man ja keine Hintertüren). Nur für Windows oder auch für Linux Mint? Oder weiß man nichts Genaues wie immer nicht?

Oder sind andere Staaten nur neidisch über unsere schöne deutsche [Sina-Box](#)?

[Guckst du hier](#): „Kanther fordert in seiner Rede, den Risiken, die sich aus der Technik ergeben auch mit den Mitteln der Technik zu begegnen und führt dabei unter anderem auch elektronische Wegfahrsperrern als Mittel zur Verhinderung von Kraftfahrzeugdiebstählen an. Dieser Vergleich mutet seltsam unpassend an, handelt es sich dabei doch genau wie der Einsatz von kryptographischen Mitteln um ein klassisches Mittel zu Verbrechensprävention, nicht um ein staatliches Instrument zur Strafverfolgung. Eine Umsetzung von Kanthers Vorschlägen würde

den Anwender von Datennetzen seiner legitimen Verteidigungsmöglichkeiten gegen Computerkriminelle berauben. Kanther führt weiter aus, wie er sich die Kontrolle des Staates vorstellt: "Dies kann dadurch geschehen, daß die verwendeten Schlüssel sicher hinterlegt werden. Durch eine Kombination von organisatorischen, personellen, technischen und juristischen Maßnahmen kann jedem Verdacht einer Mißbrauchsmöglichkeit begegnet werden."

Das war am 28 April 1997! Es gibt noch andere hübsche Beispiele. Vor [20 Jahren](#) fragte Florian Rötzer auf Telepolis: „Nichts mehr mit Pretty Good Privacy?“ Oder der [Guardian](#) (2001): „Pakistan to ban encryption software“.

Ich schrieb hier vor [12 Jahren](#): Der Artikel von Heise erinnerte mich an meinen Text auf *spiegel.de* vom 10.02.2007: „[Geheimes Schreiben gegen Schäuble](#)“, in dem ich [Steganografie](#) unter Linux vorstellte. Mit ein paar Befehlen kann man Texte so in Bildern verstecken, dass sie kaum gefunden werden.

Hier ein Beispiel, die Fotos oben sind das Ergebnis: Das linke Bild ist das Original, im rechten Foto ist ein längeres Zitat aus dem [Koran](#) verborgen. Ich habe vorher [nachgesehen](#), in welchen Passagen es um den Jihad geht.

```
burks@master:~/burksfiles/temp5$ touch osama.txt
burks@master:~/burksfiles/temp5$ echo "Und wenn die heiligen
Monate abgelaufen sind, dann tötet die Götzendiener, wo immer
ihr sie findet, und ergreift sie und belagert sie und lauert
ihnen aus jedem Hinterhalt auf. Wenn sie aber bereuen und das
Gebet verrichten und die Zakah entrichten, dann gebt ihnen den
Weg frei. Wahrlich, Allah ist Allvergebend, Barmherzig;">
osama.txt
burks@master:~/burksfiles/temp5$ zip secretmessage.zip
osama.txtupdating: osama.txt (deflated 36%)
burks@master:~/burksfiles/temp5$ cat 181008_2.jpg
secretmessage.zip > 181008_3.jpg
```

Oder wünscht das Publikum, weil es besorgt ist, dass ich hier einen Online-Lehrgang über Steganografie anbiete? Gehe ich richtig in der Annahme, dass niemand mehr [Windows 3.11](#) benutzt?