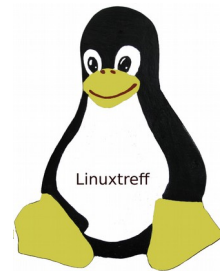


Tipps und Überlegungen:

Datenkraken allüberall



vorgestern ging es groß durch die Presse, dass sich der BND am größten Internetknotenpunkt bei Frankfurt anlasslos gewaltige Mengen an Daten abzapfen und ansehen kann. Das trifft uns alle. Zur weiteren Information:

<https://netzpolitik.org/2018/bnd-vor-dem-bundesverwaltungsgericht-masseneueberwachung-am-de-cix-rechtswidrig/>
und
<https://www.tagesspiegel.de/politik/bundesverwaltungsgericht-bnd-darf-weiter-daten-von-internet-knoten-abzapfen/22627648.html>

Das Bundesverwaltungsgericht hat dem Kläger, der sich gegen diese Praxis wehren wollte, nicht Recht gegeben.

Damit wird die Frage noch bedeutender: Wie schützen wir unsere Daten nicht nur gegen die Datenkraken aus den USA, sondern auch gegen den BND, unseren BundesNachrichtenDienst? Wie wohl man es ahnen konnte. Er handelt mit Nachrichten, deswegen heißt er so.

Solltet ihr nun anfangen, über einen weitergehenden Datenschutz (Verschlüsselung des E-Mailverkehrs, konsequenter Werbestopp, Auswahl datensicherer Webbrowser wie etwa Startpage u.a.m.) nachzudenken?

Wenn niemand unsere Daten schützt, müssen wir das offenkundig selbst in die Hand nehmen.

Wer übrigens bereits ein Schlüsselpaar hat und mit Thunderbird verschlüsselt, kann jedem anderen, der dasselbe bereits umgesetzt hat, verschlüsselt schreiben. Der öffentliche Teil des Schlüssels ist im Internet (oder auch beim Besitzer des Mailaccounts) abrufbar.

Und: Wer sich zusätzlich an folgende Regeln hält, hat mehr davon:

Am besten nie ein Dokument an eine E-Mail anhängen.

E-Mails grundsätzlich NICHT als HTML-Mail, sondern immer nur als Text (Reintext, Nur-Text).

Beim Prozess der Schlüsselherstellung wird auch eine einzigartige Signatur hergestellt. Sie ist ein so gut wie unfälschbarer Hinweis auf den Verfasser der Mail.

Auch das Lesen des Quelltextes (unter >Mehr< Quelltext lesen) kann sehr informativ sein.

Juni 2018