

# Allüberall Aktivismus

# sinnfreier

Meldungen, die man hiesigerseits hämisch, belustigt, gelangweilt oder verärgert kommentieren konnte, gab es in den letzten Tagen genug. Zum Thema „Jugendgefährdung“ fällt mir ohnehin nichts mehr ein. Man ist es gewohnt, nur noch keinen Nonsens dazu zu lesen. Zum Glück decouvrieren sich die üblichen Verdächtigen ohnehin ständig selbst als bigotte Heuchler, denen es nicht um irgendwelchen „Schutz“ einer wie auch immer definierten „Jugend“ geht, sondern ausschließlich um moraltheologisch verbrämte und gespreizte Selbstbeweihräucherung.

Aktuell in [Brandenburg](#): „Auf Anregung des Landeskriminalamtes (LKA) Brandenburg sind im vergangenen Jahr 36 Tonträger und DVD mit rechtsextremen oder gewaltverherrlichenden Inhalten für Jugendliche verboten worden.“ Und nun? War die [Matthäuspasion](#) von Johann Sebastian Bach dabei? Oder wurde [Richard Wagner](#) indiziert? Mitnichten. Das Motiv des *Meldens*, *Durchführens* und *Verbietens*, findet, wenn dann davon absieht, dass es der Deutschen an sich gern tut, in einem Satz des Heise-Artikels: „Damit sei das LKA in diesem Bereich erneut die aktivste deutsche Polizeibehörde gewesen, so Innenminister Jörg Schönbohm (CDU) laut der Mitteilung. (...) Dies unterstreiche, dass in Brandenburg der Extremismus auf allen Ebenen konsequent bekämpft werde.“ Damit haben wir alles beisammen: kamerad Schönbohm ist nur „gegen Extremismus“. Also Rot gleich Braun, Bautzen gleich Auschwitz – Totalitarismus-Doktrin, ick hör dir trapsen. Aktiv ssein, Fllgge zeigen, Gesicht zeigen, ahrt durchgreifen – sinnfreier Aktivismus, und wehe, jemand fragte nach dem Zweck des Ganzen.

Und nun zu etwas ganz Anderem. [Schäubles Traum](#) und der der CDU, die Sicherheit vor Freiheit setzt, wird bekanntlich in Indien wahr. Bei [Annalist](#) lesen wir etwas über die hiesige

Praxis: „BKA-Ratespielchen rund um GnuPG“. Wir haben nur den Blogbeitrag als einzige Quelle, es kann also nicht überprüft werden, ob die Angaben wahr sind. Das BKA wird sich wohl eines Kommentars enthalten. „Kann die Verschlüsselungssoftware PGP/GnuPG wirklich davor schützen, dass Unbefugte auf eigene Dateien Zugriff haben? “ Gute Frage. Offenbar wusste das BKA auch nicht weiter, und die „Experten“ waren zu teuer, hätten vermutlich auch nur mit den Achseln zucken können. Wenn ein geheimer Schlüssel in die Hände der Ermittlungsbehörden fällt, [wie bei mir auch](#), dann wird es spannend. „Die beiden hatten im Grunde aber auch nichts besseres anzubieten, als die Passphrase zu raten, die nötig ist, um mit dem Schlüssel die verschlüsselten Dateien öffnen zu können.“ Meine besteht übrigens aus zehn gemischten Zahlen und Buchstaben. Viel Spaß damit. Aber sie rätseln vermutlich noch an meinem Passwort des Rechners herum (acht). Ein Kommentar in Annalists Blog sagt alles: „PGP arbeitet noch ein wenig anders: es nimmt nicht die passphrase und macht daraus den hash, sondern es wiederholt diese Prozedur mehrmals. Somit muss auch jede Implementierung des BKA diese Prozedur entsprechend oft wiederholen. Und in den Standardeinstellungen wiederholt PGP diese Prozedur 65536 Mal. Entsprechend oft müßte also auch eine Hardware-Implementierung diese Prozedur iterieren, was zwar nicht mehr chips bedeutet, da einer 65536 Mal hintereinander genutzt werden kann, aber entsprechend alles 65536 Mal so lange dauert. Wenn Andrejs Passphrase also 8 Zeichen hat und nicht aus einem Wort besteht, wodurch eine Wörterbuch-Attacke möglich wäre, dann ist es schon relativ hoffnungslos.“

Dann haben wir noch die [Meldung](#): „Bürger-E-Post De-Mail soll ‚geprüfte statt geglaubte Sicherheit‘ bringen“. Dazu fällt mir nichts mehr ein. Ich „galube“ ohnehin nicht an asymmetrische Kryptografie, empfehle daher den wohlwollenden Leserinnen und geneigten Lesern nur, die Kommentare zu diesem Artikel zu durchstöbern, um sich mit mir zu amüsieren.