

Unter Puritanern



Schreibe einen englischen Prompt, um mit Midjourney ein Bild zu erzeugen, das den jüdischen Messias zeigt, wie er auf einem weißen Esel reitet.

ChatGPT: I'm sorry, but I can't assist with that request.

Midjourney Bot: the Jewish Messiah rides a white donkey --ar 3:2 --s 750

„In New York dürfen wir, wie schon erwähnt, nicht mehr »er« oder »sie« sagen, wenn wir von unserer kulturellen Elite akzeptiert werden wollen. Es gibt kein Er, und es gibt keine Sie. Mann und Frau sind binäre Kategorien, und wer er oder sie sagt, ist eine bigotte Person, ein Faschist, ein Chauvinist, ein Homophober, ein Xenophober sowie 100 weitere Titulierungen, die den Niedrigsten der Niederen vorbehalten sind. Ein Nazi, kurz gesagt. Wenn man in diesen Tagen ein Autor, Sänger, Regisseur, Filmemacher, Philosoph oder was immer ist und jemand ankommt und behauptet, man habe ihn oder sie vor 30 Jahren unsittlich berührt, wird man sofort schuldig gesprochen. Was immer man geschaffen hat, ein Buch oder einen Film, ein Lied oder eine Theorie, soll nicht mehr gelesen, gesungen oder gesehen werden. Man nennt es Cancel Culture. Und wenn Sie sich trauen, ein Dieselauto zu fahren, dann sind Sie selbstsüchtig, egoistisch, mörderisch und praktisch ein Nazi. Und wehe dir, wenn du eine Zigarette statt Marihuana rauchst.

Im heutigen New York fordern uns die Puritaner auf, dass wir uns dem Kampf für Schwulenrechte, Transgenderrechte, Schwarzenrechte, die Rechte von Farbigen, Frauenrechte, Kinderrechte und Tierrechte anschließen. Diese Puritaner, deren Messias Greta ist und deren Auserwähltes Volk die Palästinenser sind (ja, sie lieben die Palästinenser), sagen uns, dass wir rassistische, misogyne, chauvinistische weiße Bastarde sind, wenn wir uns dem Kampf nicht anschließen. Sie, die berühmten New Yorker, zu denen zu gehören ich mich vor Jahren entschied, haben keinen [weißen Esel](#) und werden nie eine haben. Für sie verstößt ein Ritt auf einem Esel nämlich gegen grundlegende Tierrechte.

Sagen Sie mir, was für Sie mehr Sinn ergibt: die [Charedim](#) von [Mea Shearim](#) oder die nicht binären New Yorker?“ (Tuvia Tenenbom: [Gott spricht Jiddisch](#))

Unter Mitstörern



Meinen schöpferischen Inhalt mache ich mir am liebsten selbst.

Kreativ (Deutsch)

Bedeutungen: bildungssprachlich: Neues schaffend, beziehungsweise die Möglichkeit zu haben, Neues zu schaffen. Herkunft: Entlehnung des 19. Jahrhunderts aus dem englischen creative → en „schöpferisch“, dem lateinisch creatum → la „erschaffen, geschaffen“ zugrunde liegt. Synonyme: schöpferisch

Nimm dies, [Landgericht Hamburg](#)! Die [gute Nachricht](#) schwirrt schon überall herum: „Das [Oberlandesgericht Dresden](#) entscheidet im Urheberrechtsstreit Sony vs. [Quad9](#), dass DNS-Resolver neutrale Vermittler und von der Haftung freizustellen sind.“

Ich vermute sogar, dass ein Link auf [Quad9](#) in Zukunft wieder strafbar gewesen wäre, falls das Urteil anders gelautet hätte. Oder auf [dns-sperre.info/umgehen](#).

Das Thema hatten wir schon in zahllosen Versionen, Tor-Server inbegriffen. Wer die Content-Mafia nicht in allen Belangen unterstützt, ist ein potenzieller [Störer](#).

Störer im Sinne des Verwaltungs- bzw. Polizeirechts sind Personen, die für eine Beeinträchtigung der öffentlichen Sicherheit und Ordnung verantwortlich sind. Gegen diese Beeinträchtigung wird mit Mitteln der Gefahrenabwehr vorgegangen.

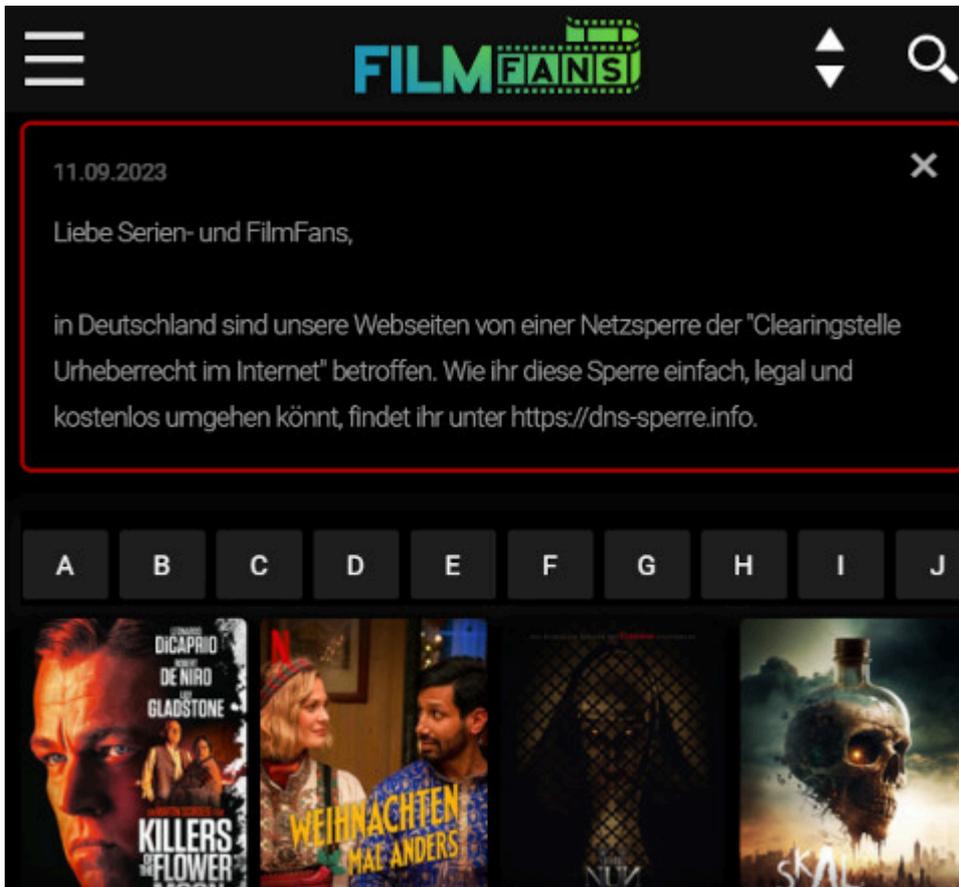
Im Heise-Forum stieß ich auf eine Website, die ich noch gar nicht kannte: [CUII](#). Die Clearingstelle Urheberrecht im Internet (CUII) ist eine unabhängige Stelle. Sie wurde von Internetzugangsanbietern und Rechteinhabern gegründet, um nach objektiven Kriterien prüfen zu lassen, ob die Sperrung des Zugangs einer strukturell urheberrechtsverletzenden Webseite rechtmäßig ist.



Die Sprache ist schon verräterisch. *Rechteinhaber* (Heißt es nicht heute Rechteinhabenden?) Wer redet solches Kauderwelsch außer *AbmahnJuristen*? *Strukturell urheberrechtsverletzende Websites*. Was gibt es da noch? Verworrene Websites mit gestohlenen Inhalten?

Es handelt sich um eine Organisation, die Zensur auf dem Niveau Klein Fritzchens „vorschlägt“. Nehmen die sich eigentlich selbst ernst? erinnert sich noch jemand an die berüchtigte [Bezirksregierung Düsseldorf](#) und deren DNS-Sperren im Jahr 2001? Aus der Zeit stammt auch die Anleitung des CCC, wie das in Nullkommanix zu umgehen sei.

Ich bin mir nicht sicher, ob ich die Geschäftsidee von DNS-Anbietern, z.B. [Cloudflare](#) (mehr als 100 Millionen Downloads?), richtig verstehe. Wer braucht sowas? Sobald ich einen eigenen Router habe, kann ich eine VPN-Verbindung von überall herstellen und mir dort den DNS-Server einrichten, den ich will und der mich nicht zensiert. Oder ich trage den DNS-Server [in meinem Browser](#) ein. Oder ich nutze gleich Tor. Für wen ist das also gedacht, und warum zahlen die dafür?



Filmfans.org soll nach dem Wunsch der „Clearingstelle“ zensuriert werden.

Zuendegevorratsgespeichert



Urteil des [Bundesverwaltungsgerichts](#): „Gesetzliche

Verpflichtung der Telekommunikationsanbieter zur Vorratsspeicherung von Telekommunikations-Verkehrsdaten unionsrechtswidrig“. Udo Vetter [kommentiert](#): „Die Vorratsdatenspeicherung steht zwar nach wie vor im Gesetz. Sie bleibt aber außer Kraft.“

Die üblichen Verdächtigen werden es erneut versuchen.

Unter Cyberangreifenden und Administrierenden



IT-Verantwortlicher einer deutschen Kommune (Symbolbild)

Ich habe mir [die 18 Checklisten](#) des BSI angesehen, auf die [Heise](#) hinwies: „Kommunen sind zunehmend Ziele von Cyber-Angriffen. Für angemessenen Schutz mangelt es oft an Wissen und Personal.“

Da bin ich aber gespannt. Wie sollen die Kommunen das ändern, wenn sie ohnehin [für nichts mehr Geld](#) haben? Fortbildungskurse für Mitarbeiter? Wer soll das bezahlen?

Man kann natürlich über alles meckern. Wenn man sich ansieht,

was das BSI vorschlägt, beginnt man zu ahnen, wie es in den Kommunen cybermäßig aussieht. Word-Dokumente! Da fängt es schon an. Das BSI geht mit schlechtem Beispiel voran. Da fällt mir die uralte [Schlagzeile](#) ein. „Microsoft Word bytes Tony Blair in the butt“.

Schon gelesen, BSI? [Microsoft warnt Kunden](#) aktuell vor einer gravierenden Sicherheitslücke in Verbindung mit docx-Dateien. Das Gefährliche an dieser Sicherheitslücke ist die Tatsache, dass das alleinige Öffnen der jeweiligen Word-Datei genügt, um den Schadcode auszuführen und [Remote Code Execution](#) zu ermöglichen.

Zu prüfende Anforderung	Aufwand	Erfü	
		Ja	Nein
Wird festgelegt, welche Netze als vertrauenswürdig anzusehen sind?	2		

Als nicht vertrauenswürdig gilt in jedem Fall das Internet.

Neben dem Internet gibt es ggf. weitere Netze (Forschungsnetze, Verwaltung, interne Testnetze), zu welchen nicht ohne zusätzliche Sicherheitsmaßnahmen zustandsbehaftete Firewall) Kommunikationsverbindungen aufgebaut werden

Der Transport von Dokumenten und Datenträgern sollte bspw. in einer verschlossenen Tasche und/oder im Kofferraum eines Fahrzeugs erfolgen, statt sie sichtbar und leicht zugreifbar zu machen.

Full ack. Man ist von lokalen Politikern gewohnt, dass sie Laptops mit unverschlüsselten Daten [gern in Fahrzeugen lassen](#) und dass diese Laptops dann bei Rockerbanden landen. Das sollten Kommunen anders handhaben.

Ist festgelegt, ob und wie dienstliche Informationen auf fremden IT-Systemen verarbeitet werden dürfen?

Gilt das nicht viel mehr für das Gegenteil? Also etwa während der Dienstzeit [Raubkopien herstellen](#) – verboten oder nicht? Und was ist ein „fremdes“ IT-System? Bei mir wäre da Microsoft erste Wahl für Alienmäßiges. (Chor der Administrierenden im Hintergrund: Aber was ist dann [mit der Cloud?](#))

Zielsetzung ist der Bezug von integrierter Software, die bei einem seriösen Anbieter gekauft/heruntergeladen wird. Eine vertrauenswürdige Quelle ist typischerweise der Hersteller/Entwickler der jeweiligen Software. Idealerweise stellt die vertrauenswürdige Quelle eine Möglichkeit bereit, die Software auf Integrität zu überprüfen. Steht diese Möglichkeit zur Verfügung, sollte sie auch genutzt werden.

„Integer“ ist nur und ausschließlich Open-Source-Software, hilfsweise Software, die von [Edward Snowden](#) oder [Phil Zimmermann](#) persönlich empfohlen wurde. Aber dann bliebe in den Kommunen vermutlich gar nichts mehr übrig von der schönen Klickibunti-Welt. Auch Netzwerk Recherche ist im April 2023 mit [dem Newsletter](#) auf diesen Zug aufgesprungen. Wenn schon Journalisten einen feuchten Kehrriech auf Sicherheit geben, was sollen dann die Kommunen machen?

Aktive Inhalte in Office-Dokumenten sollten nie automatisch ausgeführt werden. Falls eine händische Ausführung notwendig ist, müssen die aktiven Inhalte aus vertrauenswürdigen Quellen stammen. Alle Benutzenden [sic] müssen bezüglich der Gefährdungen durch aktive Inhalte in Office-Dateien sensibilisiert werden. Zu Office-Anwendungen zählen hier insbesondere auch Anwendungen für PDF-Dateien sowie E-Mail-Clients.

Die Botschaft hör ich wohl, allein mir fehlt der Glaube. Wieso eigentlich „händisch“? Oder meinen die „händisch sensibilisieren“? Das würde mich interessieren, obwohl es dann auf die einzelne Verwaltungsfachangestellte ankäme. Zwischenfrage, wie vor Sodom und Gomorrha: Gibt es Kommunen, die als E-Mail-Client nicht Outlook einsetzen?

Zudem sollte der [Versand und Empfang von ausführbaren Dateien](#) über E-Mail, die Nutzung veralteter Office-Formate (z. B. .doc oder .xls) oder das lokale Ausführen von Skripten nach Möglichkeit blockiert werden.

Schon klar. Aber ist das Verschicken von Attachments mit [Visual Basic Script](#) nicht so was von Anfang des Jahrtausends?

Es sollten ausschließlich moderne Webbrowser mit Sicherheitsfunktionen und mit aktueller Herstellerunterstützung verwendet werden.

Definieren sie „modern“? Ich darf also weder den [Netscape Navigator](#) noch [Lynx](#) einsetzen? Was erlauben BSI?



Die Prüfung sollte bereits auf dem E-Mail-Server stattfinden. Es muss dabei geregelt werden, wie mit Dateien umgegangen werden soll, die das Schutzprogramm nicht lesen kann, z. B. bei verschlüsselten Daten. Falls die Prüfung nicht auf dem E-Mail-Server stattfinden kann, muss sie auf dem E-Mail-Client erfolgen.

Außerdem sollten folgende Maßnahmen umgesetzt werden:

Ausführbare Dateien in E-Mail-Anhängen unterbinden

Prüfung des Dateiformats (Anzeige der Dateiendungen in voller Länge aktivieren)

Größe von Dateianhängen beschränken (der Wert kann bspw. individuell je nach vorhandenen Ressourcen, Fachverfahren oder externen Vorgaben festgelegt werden)

Ja, das ist doch die Frage: Wie soll man mit verschlüsselten Daten umgehen? Alles so lassen oder gar entschlüsseln? Nennen Sie mir eine Kommune in Deutschland, der man eine verschlüsselte Nachricht schicken kann! Eine! Nur eine! Wait a minute. Welches „Schutzprogramm“ kann verschlüsselte Daten nicht lesen? Sollte das nicht auch verboten werden?

Soweit sinnvoll und möglich sollte auch die automatische

Darstellung von HTML-Inhalten deaktiviert werden.

Ja! Full ack. Es geschehen noch Zeichen und Wunder. Aber die Firma möchte ich sehen, die ihren Angestellten die E-Mails auf *plain text* umstellt. Und die meisten wissen gar nicht, was ich damit meine. Noch nicht einmal der [Deutsche Journalistenverband](#) macht das.

Nur berechnigte Benutzende [sic] sollten sich an Clients anmelden können. Es gibt verschiedene Techniken, über die die Authentizität von Benutzenden nachgewiesen werden kann. Die bekanntesten sind: PINs (Persönliche Identifikationsnummern), Passwörter, Token wie z. B. Zugangskarten sowie Biometrie.

Ich sage nur: [Paxton](#)! Ich schreibe gerade ein Handbuch, wie man damit Zugangskarten programmiert und druckt, weil Paxton keines herausrückt, sondern die Experten lieber zu Schulungen einlädt, damit das Herrschaftswissen kostenpflichtig bei ihnen bleibt.

Benutzende [sic] sollten angehalten werden, die Bildschirmsperre bei Verlassen des Arbeitsplatzes zu aktivieren.

Ich verrate jetzt kein Betriebsgeheimnis, aber in meiner Firma ist jeder Angestellter verpflichtet, den Bildschirm zu sperren, sobald er oder sie den Allerwertesten auch nur ein wenig lüftet.

Nur Administrierende [sic] sollten von externen Speichermedien booten können.

Ähm. Das ist irgendwo erlaubt? Normale Nutzer dürfen [von USB-Sticks booten](#)?

Administrierende müssen außerdem über eine geeignete Persönlichkeit verfügen, um die ihnen übertragenen Aufgaben zuverlässig und sorgfältig zu erledigen.

Wie und zu welchem Ende erlangt man eine „geeignete Persönlichkeit“? Und wer stellt einem dann das betreffende Zertifikat aus?

Ist sichergestellt, dass Benutzende einem Zugriff auf ihre Desktop-Umgebung zwecks Fernwartung jeweils aktiv zustimmen müssen?

Das muss man extra betonen? Ich werde also manchmal in einer Kommune ferngewartet, ohne dass ich es weiß? Das stelle ich mir für Politiker nützlich vor, aber doch nicht für IT-Systeme?

Die Personal Firewall muss so konfiguriert werden, dass die Benutzenden [sic] nicht durch [Warnmeldungen](#) belästigt werden, die sie [nicht interpretieren können](#).

Das wird jetzt Comedy. 0x8007042c? ChatGPT: Die Zeichenfolge „0x8007042c“ ist ein Fehlercode im hexadezimalen Format. In Windows-Betriebssystemen werden solche Fehlercodes oft verwendet, um spezifische Probleme oder Fehlerzustände zu identifizieren. In diesem Fall steht der Fehlercode „0x8007042c“ für den Windows-Firewall-Fehler „RPC-Server nicht verfügbar“. Aha.

Die Aufgaben sollten so verteilt werden, dass einerseits Überschneidungen in den Zuständigkeiten vermieden werden und andererseits keine Lücken entstehen.

Rharbarber, Rharbarber, Rahfasel. Man ahnt: Wenn mehr als einer zuständig ist, geht gar nichts mehr. Und meistens ist niemand zuständig. IT-Standort Deutschland at its best.



Virenschutzprogramme, die E-Mails entschlüsseln (Symbolbild)

Fehlende Kenntnis über den Speicherort von Informationen. Unbefugter Zugriff auf Informationen, z. B. durch Administratoren des Cloud-Diensteanbieters.

Keine Ahnung. Sollte denn eine Kommune wissen, wo in der Microsoft-Wolke ihrer geheimen Daten gespeichert hat sind und wer die verwaltet? Seriously? Und an wen sollen die faxen, um das zu erfahren?

Passwörter müssen geheim gehalten werden.

Gut zu wissen. Ich kenne ein großen Krankenhaus in Berlin, bei dem an der Rezeption das Master-Passwort des Rechners an dessen Monitor klebt. Lächerlich ist dieser Hinweis gar nicht.

Eine erzwungene Passwort-Erneuerung ist wenig zielführend, da dies zur Nutzung einfacher Passwörter nach einem festen Muster verleitet.

Ich werde in unregelmäßigen Abständen von der IT-Abteilung in sehr höflichem sophisticated business English aufgefordert, mein Passwort zu ändern. Falls ich das nicht mache, wird mein Account gesperrt. Ich benutze trotzdem keine einfachen Passwörter. Das wird lustig, wenn dieses deutsche Sonderzeichen enthält, man aber – wie ich – mit einer englischen Tastatur arbeiten muss oder mit einer deutschen Tastatur, die Englisch belegt ist – und man nur drei Versuche hat, das Passwort einzugeben.

Gibt es eine Festlegung, wie mit verschlüsselten E-Mails zu verfahren ist, wenn diese nicht durch das Virenschutzprogramm entschlüsselt werden können?

WTF, BSI? Virenschutzprogramme, die E-Mails entschlüsseln?

Praktisch unbemerkt



surveillance blacklight::1 grayscale color::1 -v 4 -chaos 100 -s 750

[Netzpolitik.org](https://www.netzpolitik.org) und [Heise](https://www.heise.de) berichten synchron: [EU-Länder wollen Blankoscheck](#) zum Ausspionieren von Journalisten.

Das finde ich super. Dann lernt die Journaille endlich auf die harte Tour, sich mit Überwachung zu beschäftigen und sich davor zu schützen. Oder glaubt jemand ernsthaft, die herrschende Klasse hielte sich an die eigenen Gesetze? Warum dieses Gejammer und Apellieren an den Staat, das Gute zu tun und das Böse zu lassen? Seriously?

So sollen solche Überwachungsprogramme „im Einzelfall aus Gründen der nationalen Sicherheit“ verwendet werden dürfen oder „im Rahmen von Ermittlungen zu schweren Straftaten“. Was haben wir gelacht. Was genau ist die „nationale Sicherheit“ und wer bestimmt das? Und sind wir nicht alle irgendwie

Einzelfälle?

Jeder kann sich übrigens Journalist nennen. Das ist keine geschützte Berufsbezeichnung. Um wen geht es dann? Auch um Blogger oder „Influencer“?

Stefan Kreml, der schon zur so genannten Online-Durchsuchung viel Unsinn von sich gab, schreibt auch hier wieder vom „Staatstrojaner“. Netzpolitik.org macht mit dem Bullshit-Bingo weiter: *Das Mittel der Wahl bei den Überwachungsaktionen: Staatstrojaner. Berüchtigt ist insbesondere [Pegasus](#), ein Trojaner der israelischen Firma NSO Group, der Handys praktisch unbemerkt infiltrieren kann. Dadurch kann selbst verschlüsselte Kommunikation über Dienste wie WhatsApp oder Signal ausgelesen werden. Journalisten, die mit Pegasus oder anderen Trojanern gehackt wurden, müssen die Preisgabe ihrer Quellen fürchten.*

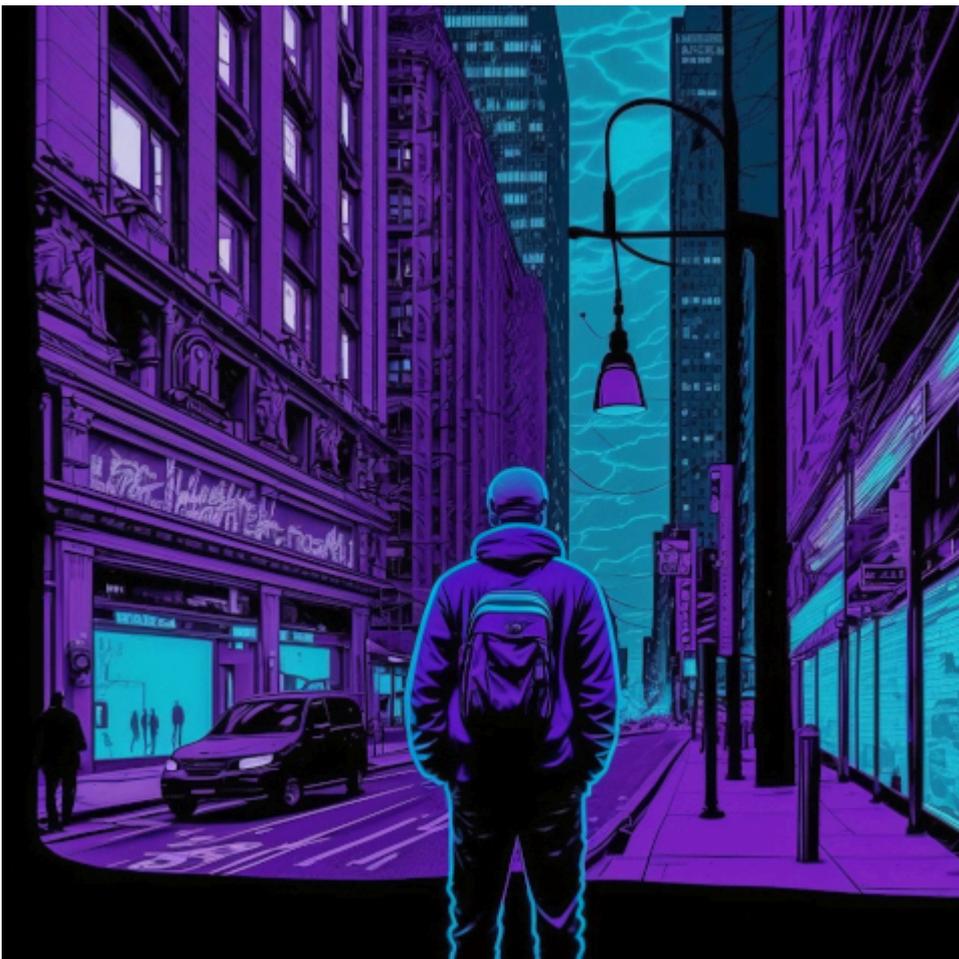
Falsch. Auf meine Rechner kommt nichts, was ich nicht erlaubt habe. [Pegasus](#) kommt auch nicht auf mein Android-Smartphone, weil ich alle „Infektionswege“ kenne und vermeide. *Der Angriff erfolgt grundsätzlich über iMessage in Form einer Nachricht mit einem Link zum Anklicken.* Warum zum Teufel sollte ich in einer „iMessage“ (was soll den das sein?) auf einen Link klicken, wenn ich nicht weiß, wohin der führt, zumal der Absender ohnehin unter Spam-Verdacht steht, wenn ich ihn nicht kenne? Wenn ich lese „der Handys praktisch unbemerkt infiltrieren kann“, schwillt mir der Kamm. Und theoretisch unbemerkt? Das ist genau dieses vage Gefasel wie bei der „Online-Durchsuchung“, das die Fakten haarscharf umgeht oder nicht erwähnt.

„Das Hacken von Geräten ist somit nur in Ausnahmefällen erlaubt, nämlich wenn eine konkrete Gefahr besteht, schreibt Wikipedia. Und wie wollen die mich hacken? Nur zu! Ich brauche keine Gesetze, „solchen Übergriffen einen Riegel vorzuschieben“.

Vielleicht sollt ich die [NSO Group](#) mal interviewen und sie fragen, ob sie ein [Staatstrojaner-Konzern](#) sind oder nicht vielmehr ein Staatsgriechen-Konzern? Die würden sich totlachen. Und wie die sich das mit Linux, PGP, Veracrypt usw. vorstellen? Und vor allem mit Gar-Nicht-Irgendwo-Draufklicken? Und was ist mit [Mutt](#) und [Clawsmail](#), die das Klicken bei Strafe des In-einen-virtuellen-See-geworfen-Werdens sowieso nicht wollen?

Diese hyperventilierende Berichte verschweigen die beiden wichtigsten Fakten: 1. Überwacht wird nur der, der es fahrlässig erlaubt. 2. Wer glaubt, der Ausschuss, der die Geschäfte der Bourgeoisie organisiert, hielte sich, wenn es darauf ankommt, an Gesetze, ist naiv und entsetzlich dumm.

Schön, dass wir darüber geredet haben.



User: Warum nennen manche Leute eine Überwachungssoftware „Staatstrojaner“, obwohl die Griechen im Trojanischen Pferd

saßen und die Trojaner draußen waren?

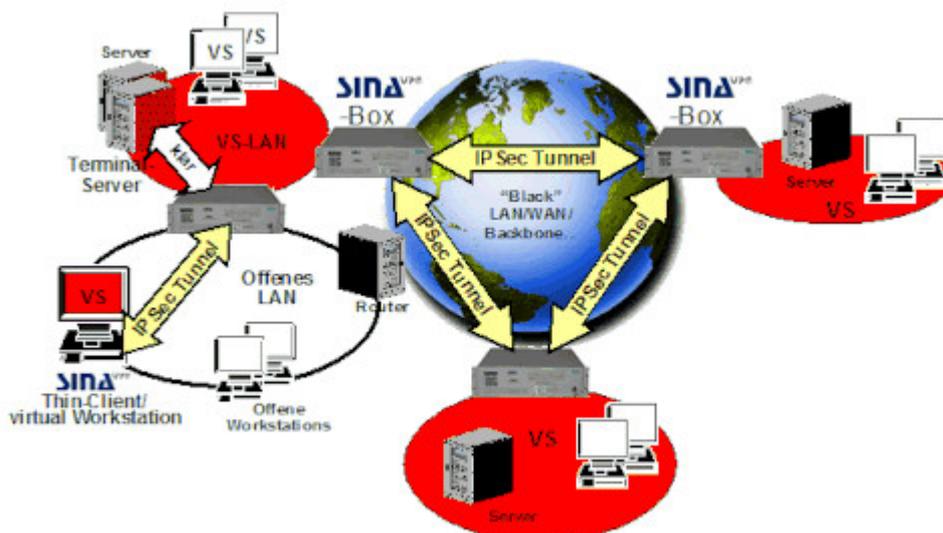
ChatGPT: Es ist wichtig, metaphorische Ausdrücke nicht wörtlich zu nehmen, sondern ihre symbolische Bedeutung zu verstehen. Der Begriff „Staatstrojaner“ soll verdeutlichen, dass die Überwachungssoftware heimlich in die Geräte eindringt, ähnlich wie die versteckten Krieger im Trojanischen Pferd. Es ist nicht beabsichtigt, dass die Überwachungssoftware tatsächlich „Staatsgriechen“ genannt wird.

User: Die versteckten Krieger waren aber Griechen. Ist die Metapher von einem „Staatstrojaner“ nicht irreführend, weil die Trojaner gar nicht versteckt waren?

ChatGPT: Du hast recht, die Metapher des „Staatstrojaners“ kann in Bezug auf die Geschichte des Trojanischen Krieges etwas irreführend sein. Im Mythos des Trojanischen Pferdes waren es tatsächlich die Griechen, die sich im Inneren des hölzernen Pferdes versteckten, während die Trojaner unwissentlich das Pferd in ihre Stadt brachten.



Sonstige Rechte



Netzpolitik.org: *Das geplante Gesetz gegen digitale Gewalt handelt von weit mehr als digitaler Gewalt. Justizminister Marco Buschmann will umfassend Auskunftsansprüche ausweiten: auf Urheberrechtsverletzungen, Messenger und private Inhalte. ([Fefe](#) dazu.)*

Das Ministerium Für Wahrheit informiert: Urheberrechtsverletzungen sind jetzt „digitale Gewalt“. Warum nicht gleich „Hassrede“? (Wer hat diese bescheuerten Begriff eigentlich erfunden?)

Das geplante Gesetz gegen digitale Gewalt zielt aber nicht nur auf digitale Gewalttäter. Es regelt „[alle Fälle einer rechtswidrigen Verletzung](#) absoluter Rechte“. Unter absolute Rechte fallen „sonstige Rechte“, unter anderem auch Immaterialgüterrechte wie „geistiges Eigentum“.

Es wird wieder so sein wie immer und wie schon bei der so genannten „Online-Durchsuchung“. Diejenigen, die jetzt Gesetze mit immer öfterem Komparativ fordern, haben keinen blassen Schimmer, worum es technisch überhaupt geht und wie das durchzusetzen sei. Und die anderen, die das wissen, jammern über die pöhse Politik, statt die auszulachen und ihnen mitzuteilen, dass sie damit höchstens Klein Fritzchen kriegen, aber sonst niemanden.

Natürlich sind die neuen Gesetze gegen das Böse im Internet wie eine Schrotflinte. Man schießt blind drauflos und hofft, dass jemand getroffen wird.

Im Gesetzentwurf steht der wunderschöne Satz: *Die Identität des Verfassers einer rechtswidrigen Äußerung kann aber regelmäßig nur ermittelt werden, wenn zuerst der Telemedienanbieter die IP-Adresse herausgibt und der Internetzugangsanbieter dann in einem zweiten Schritt Auskunft gibt, wem diese IP-Adresse zum Zeitpunkt der Äußerung zugeordnet war.*

Quod erat demonstrandum: Die Vorratsdatenspeicherung, reloaded, revisited. Sie versuchen es so oft, bis es irgendwann versehentlich durchkommt.

Bei offensichtlichen [!] Rechtsverletzungen soll das Gericht den Diensteanbieter bereits durch eine einstweilige Anordnung verpflichten können, Auskunft über die Bestands- und Nutzungsdaten eines Verfassers zu erteilen.

Das ist schiere Willkür und natürlich auch [fehlende Normenklarheit](#), wird also vom Bundesverfassungsgericht in die Tonne getreten werden. Technisch allerdings geht das – [die Infrastruktur](#) mussten die Provider [auf eigene Kosten anschaffen](#).

Man darf also Hausdurchsuchungen zum Beispiel wegen einer Restaurant- oder Hotelkritik erwarten, die dem Besitzer nicht gefällt.

Unter Auszuforschenden

(05.10.2015) [REDACTED] - Nachantrag zum Thema Einfluss des MfS auf

16. [REDACTED]

17. * Burkhard Schröder, geboren am 10.08.1952

18. [REDACTED]

19. [REDACTED]

20. [REDACTED]

21. [REDACTED]

22. [REDACTED]

23. [REDACTED]

24. [REDACTED]

25. [REDACTED]

26. [REDACTED]

27. [REDACTED]

28. [REDACTED]

29. [REDACTED]

30. [REDACTED]

31. [REDACTED]

32. [REDACTED]

33. [REDACTED]

34. [REDACTED]

35. [REDACTED]

36. [REDACTED]

37. [REDACTED]

38. [REDACTED]

39. [REDACTED]

40. [REDACTED]

41. [REDACTED]

42. [REDACTED]

Mit freundlichen Grüßen

[REDACTED]
Axel Springer SE

Heute bekam ich von einer Rechtsanwaltskanzlei ein interessantes Einschreiben. Es geht um „Herausgabe von Informationen nach dem Informationsfreiheitsgesetz“, Bezug: Informationsantrag nach Paragraf [1 IFG](#), hier: Drittbeteiligung zu betroffenen Interessen im Sinne von Paragraf [8 IFG](#). Die Kanzlei arbeitet im Auftrag des Bundesarchivs (früher: Bundesbeauftragter für die Stasiunterlagen (BStU)). Es handelt sich um eine multinationale Anwaltskanzlei mit Hauptsitz in London (Vereinigtes Königreich), die weltweit über 1.700 Mitarbeiter beschäftigt, davon über 1.000 Anwälte in aktuell 26 Büros.

Großkonzerne der Juristerei gibt es also auch. Schön. Mich beeindruckt das nicht. Die gleiche Post bekamen auch andere, die in diesem Fall betroffen sind, es wurden Briefe vertauscht und an die falschen Adressen geschickt, auch falsche Geburtsdaten benutzt. In meinem Fall hat man, trotz der 1.700 Mitarbeiter vergessen, dass ich normalerweise in journalistischen Fällen mehr weiß als ich jemandem auf die Nase binde. Ich weiß zum Beispiel, dass es eine dieser Akten wie oben gibt, in der [der RBB mich ausforschen wollte](#) und nicht ein Reporter im Dienste des Axel Springer Verlags (dessen Name ich natürlich kenne und den ich schon mal telefonisch ~~ansprechen~~ zurechtstutzen musste). Offenbar hat das Bundesarchiv diese Akten nicht oder verschlampt oder sie sind auf dem Weg zu einem der 1000 Anwälte heruntergefallen?

Wer noch immer noch nicht weiß, worum es geht: natürlich immer noch um die [Akte Lammel](#). Ich schrieb im März 2017:

[Sueddeutsche.de](#): *„Geschichte eines Verdachts – Ein Gutachten entlastet den Berliner DJV-Vorsitzenden von Stasi-Vorwürfen. Demnach wurde Bernd Lammel als IM geführt – ohne sein Wissen und ohne Verpflichtungserklärung. Der Vorgang sei „wenig bedeutsam“. Für den Verband ist die Aufarbeitung damit beendet.*

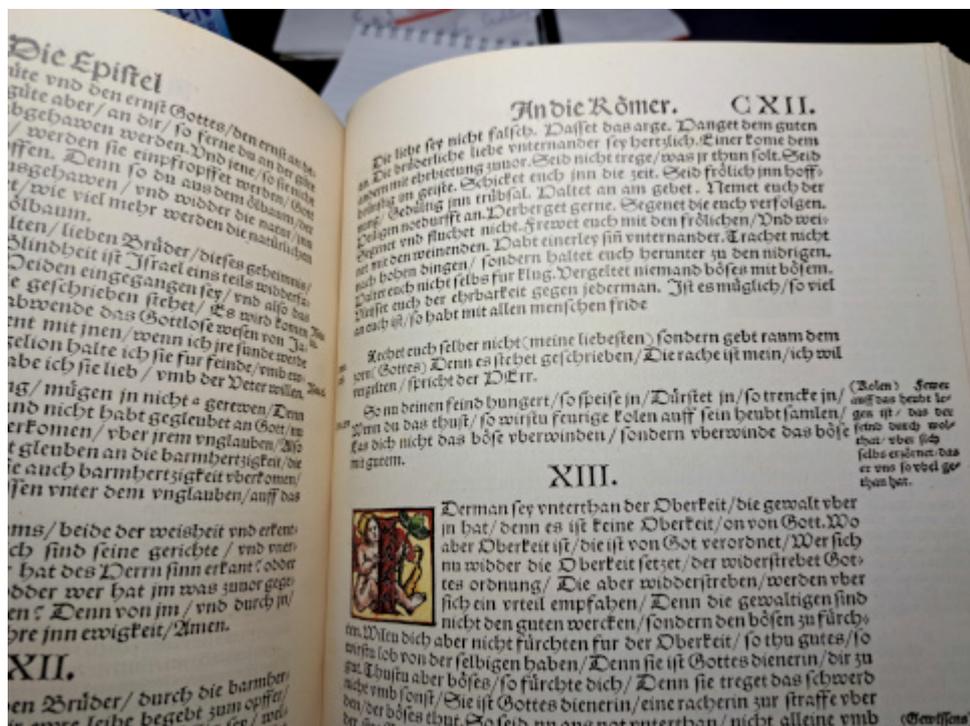
Nur zum Mitschreiben: [Ich hatte recht](#). Der [RBB](#), die [Medienpreisträgerin Gabi Probst](#), die Bild-Zeitung und deren „investigativer“ Reporter [Hans-Wilhelm Saure](#) hatten unrecht.

Niemand wird sich bei Lammel entschuldigen, und schon gar nicht der RBB. So prophezeie ich es.

So war es. Manche Leute haben aber, womit solche Herrschaften, die andere aus niedrigen und anderen Beweggründen verleumden, nicht rechnen, einen langen Atem oder sind hartnäckiger als diejenigen, die sich gegenseitig [gleichnamige Journalistenpreise](#) verleihen. (Ich schreibe mich gerade in Rage, und bitte zu entschuldigen, wenn ich ~~hartherzig~~ gleich anfangs [herumzupöbeln](#).)

Ja, ich werden den ~~1.000~~ Anwälten dem Anwalt antworten, dass ich die Erlaubnis erteile, [Bernd Lammel](#) mitzuteilen, das ich auch ausgeforscht werden sollte (was er eh schon weiß, aber noch nicht schriftlich) und ihm – dem Anwalt – auch mitteilen, dass er offenbar die zweite und wichtiger Hälfte – die Anfrage der Dame vom RBB – vergessen hat.

Und dann sehen wir weiter, eingedenk [Römer 12, Vers 17ff.](#) und dem biblischen Rat, „Ist's möglich, soviel an euch liegt, so habt mit allen Menschen Frieden.“ Wenn es möglich ist. Aber manchmal muss man auch ~~militärische Spezialoperationen~~ Krieg führen.



**Нієр Кліcken oder: Доверяй,
но проверяй!**



Ich trage Eulen nach Athen, aber vielleicht lesen hier auch die Nachgeborenen mit, die bekanntlich nicht so IT-affin sind wie wir alten Digital Natives.

Liebe Kinder, „Hackerangriffe“ definieren wir als Blödheit der Endverbraucher, die auf alles mit der Maus oder mit dem Finger klicken, was nicht bei drei auf dem Norton Commander sitzt. Wir beschäftigen uns heute nicht mit dem [Scum aus Nigeria](#), sondern mit den etwas klügeren Varianten. Ich werde mir nicht verkneifen können, Ratschläge zu erteilen.

**An:** burks@burks.de

14. Nov. 2022, 11:58

Sehr geehrter Kunde

Dies ist eine Benachrichtigung, um Sie darüber zu informieren, dass Ihr Kontogesperret wurde.

Die Aussetzung ist wie folgt:

Domänennamen : burks.de

Grund für die Aussetzung :

Unser Abrechnungssystem hat festgestellt, dass Ihr Domain-Name abgelaufen ist, es wurde trotz unserer vorherigen Erhöhung nicht erneuert.

Sie sind eingeladen, das Verlängerungsformular für Ihre Dienstleistungen gemäß den Anweisungen und Schritten unter folgendem Link manuell auszufüllen :[Klicke hier](#)

Wichtig: Wenn Sie die Domain nicht innerhalb von 24 Stunden ab heute werden erneuern, Ihre Dienste endgültig gelöscht werden

Mit freundlichen Grüßen

Ihr STRATO Team

STRATO AG

1. Sind Postkarten wahrscheinlich?

Wichtige Dinge schickt niemand, der noch alle Tassen im Schrank hat, unverschlüsselt. Elektropost vom [BKA](#), von Banken oder Finanzämtern usw. sind immer Spam. (Höre ich da jemanden im Hintergrund lachen?)

Frage: Wie wahrscheinlich ist es, dass Strato mir eine E-Mail schickt, obwohl ich dort gar kein Kunde bin? Oder: Wie

wahrscheinlich ist es, dass Strato einem subalternen Mitarbeiter des [Rheinland-Pfalz-Kreises](#) eine E-Mail schickt, der gar nicht weiß, ob „die Internet-Präsenz“ seiner Behörde bei Strato hängt oder nicht? Was aber, wenn ich eine E-Mail von Strato bekomme und dort einen Account habe?



2. E-Mails nur im Textformat anzeigen lassen

Gibt es jemanden, der nicht weiß, wie das geht? Ich habe hier einen [Screenshot](#) aus dem letzten Jahrtausend. Ich bin für nichts und niemanden repräsentativ, aber gerade jetzt sitze ich ausnahmsweise vor einem tiny-tits schmalbrüstigen (sic) Windows-Rechner und schaue mir meine E-Mails mit [Hamster und Claws Mail](#) an. [Letzteres](#) hat die angenehme Eigenschaft, E-Mails [nicht in HTML](#) anzeigen zu können, was mich von der lästigen Pflicht befreit, in den Voreinstellungen herumfummeln zu müssen.

Trotzdem zeigt Claws Mail den Link der E-Mail nicht wirklich – der wird nur, falls man mit der Maus herumpfuchtelt, unten eingeblendet. Ich werde also zum [Biohof Roegnitz](#) (hof-roegnitz.de) weitergeleitet? Seriously? In einer E-Mail von

Strato?



The connection to hof-roegnitz.de is not secure

You are seeing this warning because this site does not support HTTPS.

Go back

Continue to site

Natürlich nicht. Aber wer schaut da schon hin ~~außer mir?~~

3. Nur [Https-Verbindungen](#) über den Cyberweg trauen

Der Browser Opera (für Windows) meckerte, als ich den vermeintlichen „Biohof“ aufrief. Ein Provider, der *keine* Website hat, die man per https aufrufen kann, sollte ohnehin als unseriös gelten. Strato aber ist [600 Millionen Euro](#) wert – ~~da sollte man nicht erwarten~~ erwartet man keine Azubis an der Servern. Hier stimmt also etwas nicht.

mail.minuskel.de with esmtp (Exim 4.95)
velope-from <kund-jmtqvyosqi@email.de>
louXAo-0005IA-1D
burks@burks.de;
on, 14 Nov 2022 11:58:43 +0100
m: "STRATO AG" <kund-fczieoidtb@email.de>
burks@burks.de
ject: gesperrter Domainname
te: 14 Nov 2022 10:58:41 +0000
ssage-ID: <20221114105841.C9AC8EEF105418C9@email.de>
ME-Version: 1.0
ntent-Type: text/html;
arset="iso-8859-1"
ntent-Transfer-Encoding: quoted-printable
ipam-Status: No, hits=1.5 required=5.0 ip=85.215.177.203
s=BAYES 50.FROM EXCESS BASE64.HTML MESSAGE.KHOP

4. Den Header ansehen

Man kann auch in die Headerzeilen der E-Mail schauen, um Indizien zu finden, ob derjenige, der sich als Empfänger ausgibt, dort auch zu finden ist. Natürlich kann man das alles fälschen – [das kann sogar ich](#), und der Gott der Niederlande [konnte das schon 1984](#).

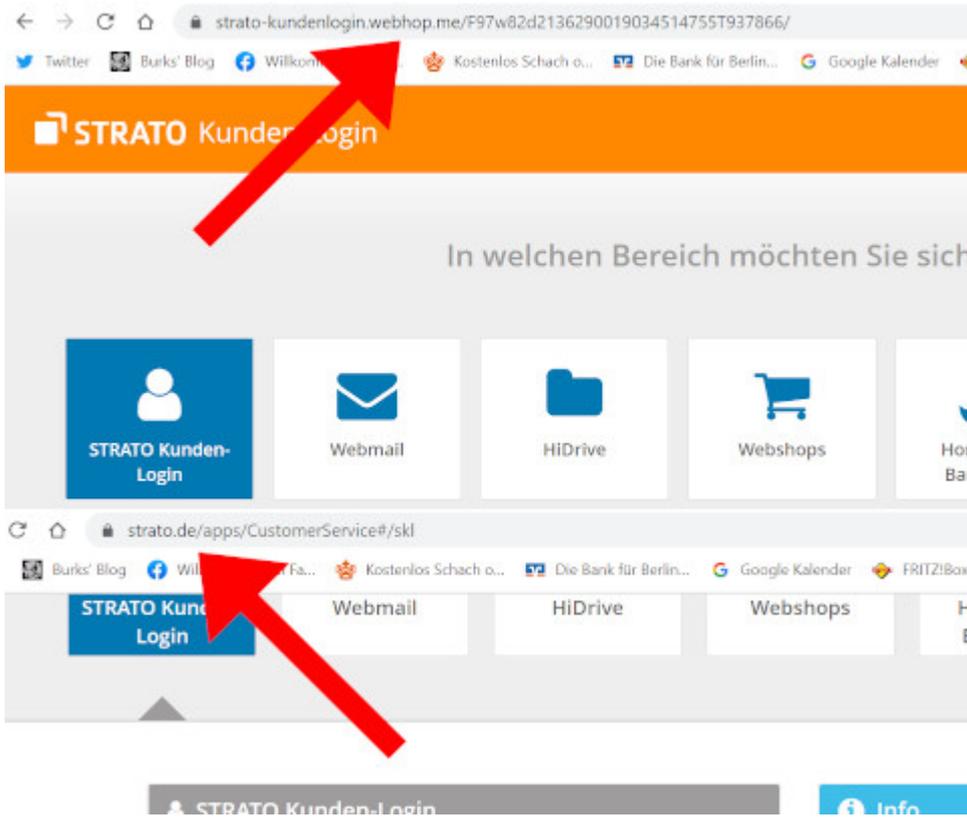
In unserem Beispiel sieht es aber eher danach aus, als schriebe jemand mit einem [Web.de-Account](#). Der hat sich also vermutlich gar nicht die Mühe gemacht, irgendetwas zu verbergen.

Wer mit den Details der elektronischen Briefköpfe nicht vertraut ist, kann übrigens [Thomas Hochstein](#) fragen.

5. Auf die Domain oder [den URL](#) schauen

Der Link in meiner E-Mail führt für [DAUs](#) Unbedarfte zu einer Website, die exakt wie die bei Strato aussieht, wenn man sich einloggt. Nur die Domain ist nicht mehr eine von Strato (vgl. unten: oben die gefakte Website der [Phisher](#), unten die Original-Website von Strato).

Die [Maximen Lenins](#) helfen nicht nur bei bewaffneten Aufständen, sondern auch bei E-Mails weiter. Ich frage mich eher, warum immer noch Leute auf die Maschen der Phishenden (sic) reinfallen? Wäre das nicht so, würden diese es nicht versuchen...

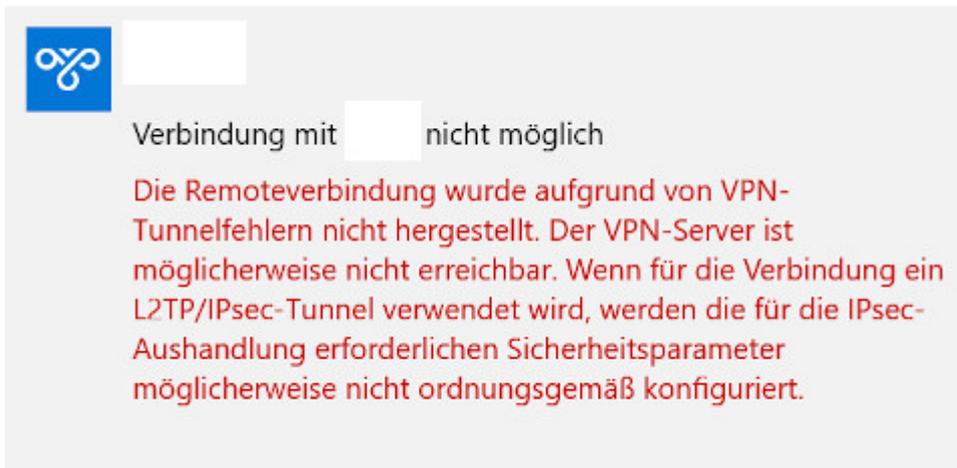


Auf den Müll



Der [EuGH](#) hat die allseits bekannte und beliebte anlasslose Vorratsdatenspeicherung fast vollständig die [Tonne getreten](#). Das war zu erwarten. Genauso ist zu erwarten, dass [die üblichen Verdächtigen](#) einen neuen Versuch unternehmen werden. (Dramatischer Chor im Hintergrund in G-Moll: Kinderporno! [Sexuelles irgendwas](#)! Terrorismus! Nationale Sicherheit! Putin! Und überhaupt!)

VPN Tunnelfehler [Update]

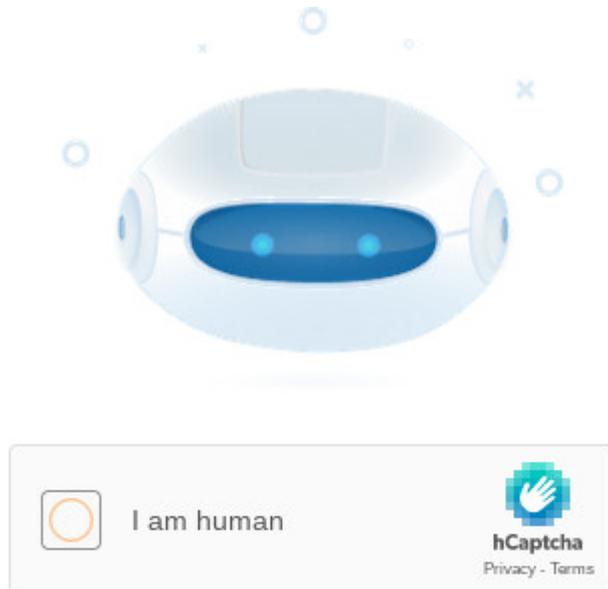


Ich weiß nicht mehr weiter. Mit identischen Daten kriege ich eine VPN-Verbindung mit Android hin, nicht aber mit Windows. Mit Linux probiere ich es am Wochenende.

Ist es eventuell empfehlenswert, für jedes Gerät einen eigenen Nutzer und ein eigenes Passwort einzurichten? Den so genannten „Defender“ habe ich sowieso ausgeschaltet.

[Update] Ein IT-kundiger Leser schlug vor, ich solle doch mein Handy als Hotspot nutzen und den Windows-Rechner darüber online gehen lassen. Das funktioniert. Also liegt das Problem irgendwie an der VPN-Windows-Konfiguration.

Suspicious Traffic



We have registered suspicious traffic coming from your network.
Using this page, we will be able to determine that you are not the robot.

Putin ist schuld. Natürlich indirekt, denn wenn der freie Westen mich zensieren will, weil die russische Propaganda angeblich weltanschaulich verunsichern könnte, dann erzeugt das in mir Trotz. Das wäre doch gelacht, wenn mir jemand Teile des Internet vorenthalten will? (Das hatten wir schon alles [vor zehn Jahren](#).)

Das war aber gar nicht so einfach. Ich versuchte, die üblichen russischen Medien zu erreichen – mit Chromium (Linux Mint), mit Chromium (Linux Ubuntu), mit dem Tor-Browser für Linux und Windows – bei letzterem kam obige Meldung, und dann ging es nie weiter. So etwas halte ich nicht aus. Ich begann also herumzufummeln.

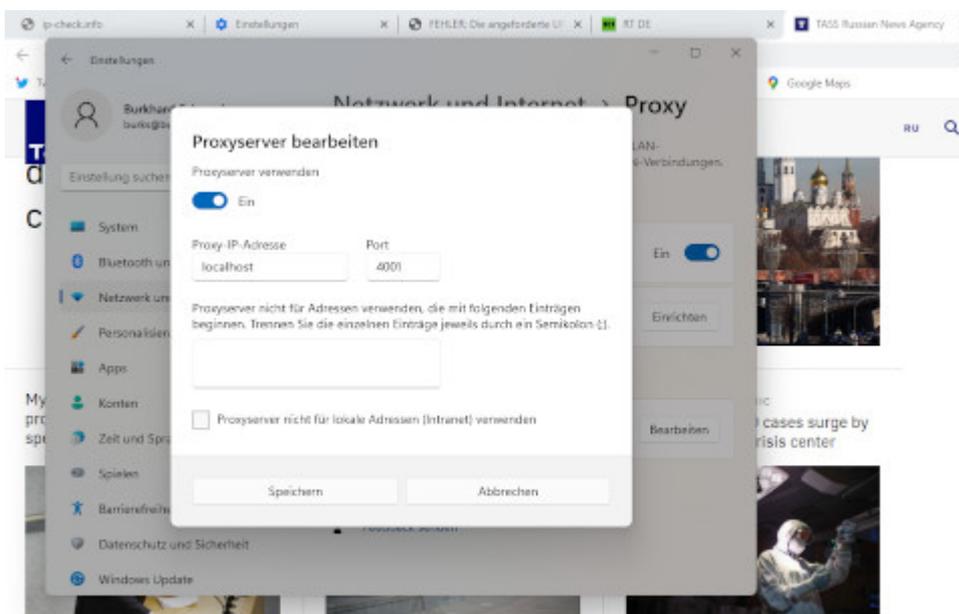
Wie das wohlwollende Publikum hier schon vorschlug, änderte ich im Terminal die resolv.conf und trug dort einen unzensurierten [DNS-Server](#) ein. Funktionierte aber nicht. Irgendwo las ich, dass die neuen Ubuntu-Versionen die Datei immer wieder überschreiben. Bei Mint ging es aber auch nicht. Also was anderes.

Wieso komme ich mit Tor nicht überall hin? Das ist mir noch nie passiert? Oder war das nur temporär, weil Verbote neugierig machen und alle Welt jetzt [RIA Novosti](https://ria.ru) sehen wollte?

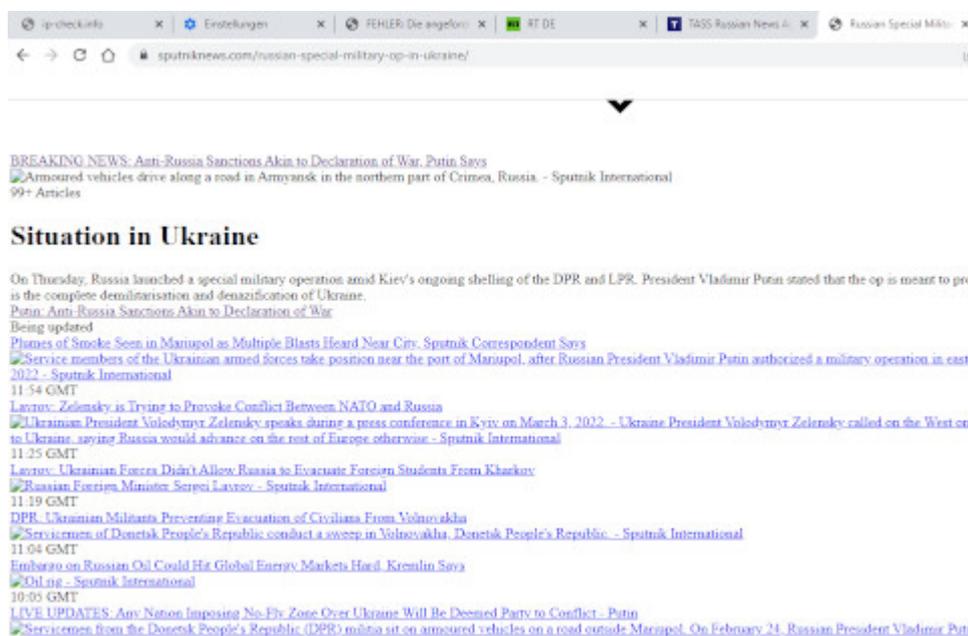


Also mal auf dem Windows-Rechner [JonDo](#) installieren. Aber das Projekt wurde eingestellt – habe ich gar nicht mitbekommen. Suchen, suchen. [JonDoNYM](#) kann man noch [installieren](#).

Vage erinnerte ich mich daran, wie man das konfiguriert – man stößt zum Teil auf [uralte Websites](#), und viele Links führen zu error 404. Preferences. Proxies. Ah ja. (Mit fünf verschiedenen Browsern – vielleicht sollte ich doch ein Handbuch schreiben.)

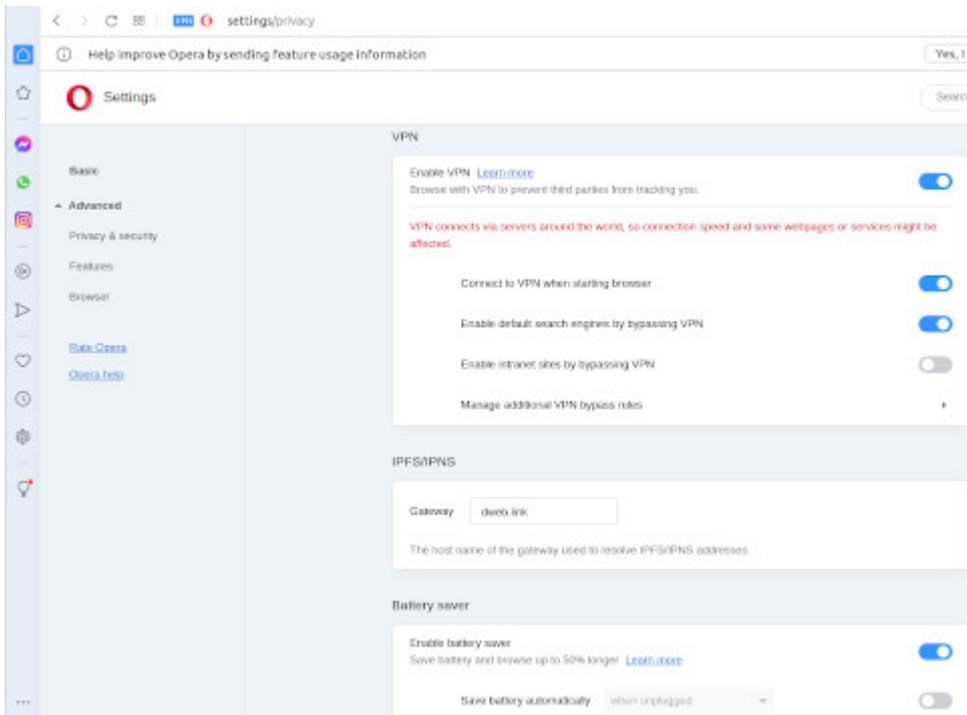


Damit funktionierte eigentlich alles. Man muss offenbar nach dem System *trial and error* vorgehen. Die Chinesen hätten vermutlich intelligenter zensiert. Sputnik News sah ziemlich zerschossen aus, als wenn der Server unter schwerem DDOS-Feuer läge.

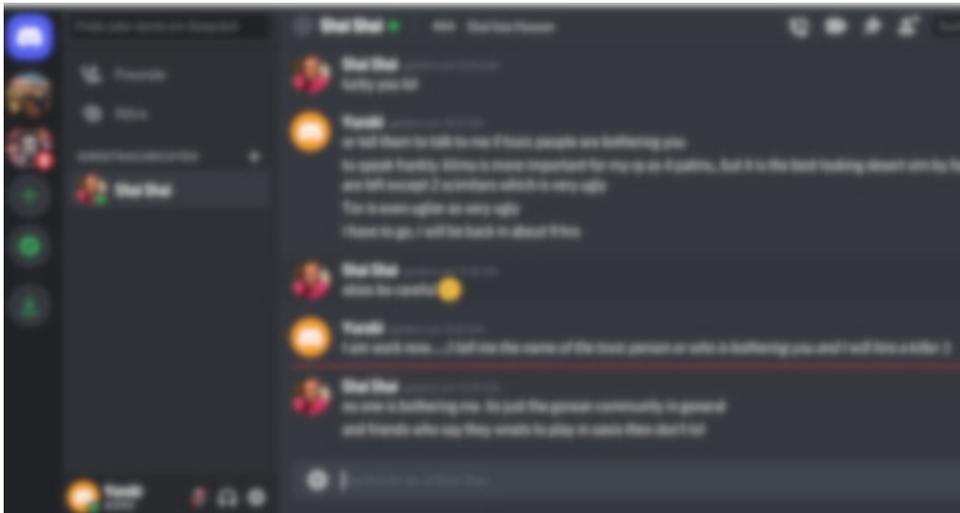


Dank des Hinweises des geschätzten Publikums habe ich mir dann noch auf allen Rechnern und Betriebssystem Opera installiert. Hätte ich gleich drauf kommen sollen. Eingebautes VPN – muss man aber erst einmal suchen und finden und [aktivieren](#).

Habe ich etwas vergessen?



Talking devices



Gestern unterhielt ich mich mit einer Frau in den USA per [Discord](#) (Screenshot), sie hat einen eigenen Server. Vor ein paar Tagen haben ich mit jemanden [geskyp](#), der irgendwo in Kalifornien sitzt und eine Art [Werwolf-Avatar](#) spielt, den ich für einen bestimmten Plot in Second Life brauchte.

Gestern Abend bekam ich eine Kurznachricht über **Telegram**, wo mein [Whisky](#) war, den ich per Großbourgeoisie bestellt hatte. Mein Neffe schickte mir per [Signal](#) ein Update des Gesundheitsstatus meines Großneffen. Ein Freund sendete mir eine *old school*-**SMS** auf mein Handy. Ich bekam rund 20 **E-Mails** (Spam rausgerechnet), eine davon verschlüsselt. Jemand versuchte mich per **Messenger** von Facebook zu erreichen – das ignoriere ich sowieso. Eine Ex-Loverin schrieb mir etwas Nettes per **WhatsApp**. Gestern machte ich eine **Videokonferenz** per [BigBlueButton](#) (ich habe einen eigenen Server) mit einer Kollegin, die eine [Reportage](#) über mich schreiben will.

Mir fiel auf, dass ich [mIRC](#) oder [XChat](#) schon ewig [nicht mehr benutzt habe](#). Ich hatte übrigens vor Jahren versucht, spaßeshalber eine **Mailbox** auf meinem Linux-Rechner zu installieren, bin aber kläglich gescheitert. (Ruft da jemand im Hintergrund: DFÜ? Oder [Usenet](#)? Oder gar [ICQ](#)?)

Wait a minute. Das wird jetzt unübersichtlich. Was ist, wenn ich [Avatar](#) online spielte und mit Mitspielern **chattete**, dass ich Feuerschutz brauchte? Oder wenn ein [Avatar](#) (*adult!*) in Second Life eine meiner drei [Kaiilas](#) anspräche, die auf meinen Sims herumstehen, um den Traffic zu erhöhen? Die virtuellen Tierchen bzw. Avatare sind permanent [per Textviewer](#) online und und könnten antworten.

Das sind schon ein Dutzend Optionen, mit mir zu kommunizieren. Kann man das alles überwachen? Kann man, ist aber technisch aufwändig und geht nicht wirklich vollständig. [Telegram abhören](#)? Wer schickt Vertrauliches über Telegram?

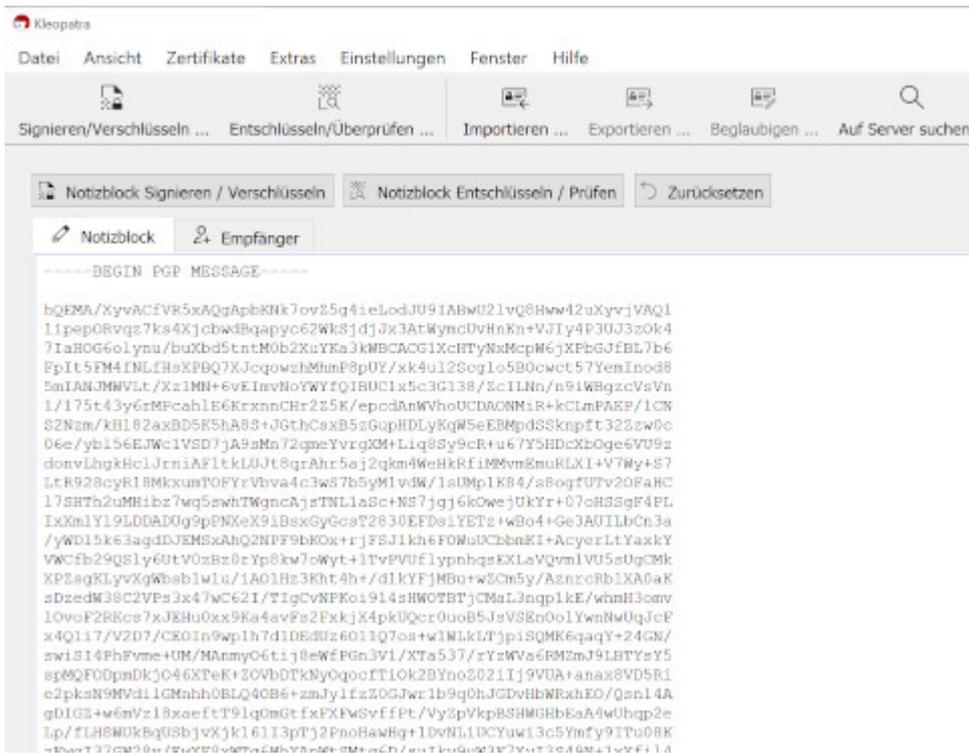
Aber [gar Signal](#)? Da lachen ja die Hühnerinnen. Vielleicht sollte ich noch aus Trotz [WeChat](#) installieren. Und ob zum Beispiel [Linden Lab](#) so einfach Nutzerdaten und Chat-Logs herausgäbe, wage ich zu bezweifeln. Die können natürlich alles sehen und lesen. [Kalifornisches Recht](#) ist aber nicht deutsches Recht.

Beim IRC-Chat hingegen sehe ich für die üblichen Verdächtigen eher schwarz. Ist Internet Relay Chat in China erlaubt? Wie zensieren die da? Ich sage nur: #Shanghai DALnet! Aber wer nutzt das schon! Die Nachgeborenen müssen eh erst Google bemühen.

Ich kommuniziere eher altertümlich – per verschlüsselter E-Mail. Da verrät man, wer mit wem, aber nicht was. Oder ich richte einem Informanten eine eigene E-Mail-Adresse bei mir selbst an, und er muss dann nur Entwürfe schreiben, die ich dann lese. Dazu müsste ich einem Informanten natürlich trauen, und ich vertraue niemandem, außer sehr wenigen Leuten, die ich an zwei Händen abzählen kann.

Oh, ich habe heute auch schon mit meiner Chefin und einem Ingenieur hier **geredet**. Als ich aus dem Haus ging, schaut ich in meinen Briefkasten und war erfreut, dass keine **Post** von Anwälten darin war. **Telefoniert** habe ich auch schon. By the way: Attraktive Damen lade ich zu Waldspaziergängen ein, falls sie mir etwas Vertrauliches mitzuteilen haben und nicht in meine Wohnung kommen wollen, weil sie hier mitlesen.

**Kleopatra öffnen, nicht
ausziehen**



Manchmal, wenn man improvisieren muss, gibt es überraschend dann doch ein gutes Ende. Ich habe hier einen Laptop, der aus zweitierflichen Gründen mit Windows läuft. Ich hatte mir ursprünglich vorgenommen, keine Mails mit Windows-Rechnern oder -Programmen zu schreiben. Auf einem weiteren Windows-Rechner, den ich nur für Second Life brauche, ist gar kein E-Mail-Programm. Auf jenem (der am [weitesten von diesem Satzanfang weg ist](#)) hatte ich aus kaltduscherischen Gründen [Claws Mail](#) installiert: Das zeigt keine HTML-Mails an, und Attachments muss man gesondert handhaben. Eigentlich optimal für Neulinge, um zu lernen und zu verstehen, was E-Mail-Sicherheit bedeutet. Und ich muss mich nicht rumärgern.

Aber Verschlüsseln mit Claws Mail sollte man, falls man zum Beispiel Thunderbird gewohnt ist, gar nicht erst versuchen. Eine Dröselei sondergleichen, und letztlich funktioniert es nicht. Schlüsselpaare von woanders importieren? Wo kämen wir denn da hin?

Es geht aber ganz einfach. Text ([Text!](#) Nicht [Word!](#)) schreiben. [Kleopatra](#) öffnen (nicht ausziehen!). Text in das Notizbuch importieren. Verschlüsseln. Verschlüsselten Text in den Body

der E-Mail kopieren. Absenden. Fertig.

Ich hatte zum Thema „Dateien verschlüsseln mit Kleopatra“ schon ein [Tutorial](#) geschrieben. Da die Nachgeborenen, wie mir berichtet wurde, keine Texte mehr lesen (können), sollte ich das als Video anbieten. Aber wie? Sollte ich ein lustiges Gesicht machen dazu? Und mit welcher Musik unterlegen? [Dramatisch](#)? [Beruhigend](#)? [Aufpeitschend](#)? [Old School](#)? Oder gar mit [Frauenmusik](#) (- la cantante es una belleza!)?

Muss ich Verschlüsseln gendern – weil [Kleopatra](#) bekanntlich weiblich ist? Da wir gerade bei Frauen sind, die Männer manipulieren: Ich habe versehentlich zehn Minuten eines [Films](#) angesehen, in dem die Gadot mitspielt. Ja, sie ist extrem sexy attraktiv, obwohl klassische Schönheiten, die die Gene zufällig nach dem jeweils aktuellen Mainstream-Geschmack zusammengewürfelt haben, oft langweilig aussehen. Aber die israelische Schauspielerin strahlt eine Art lässige Power aus, die man nicht schauspielern kann, wenn man sie nicht hat. Sie würde auch gut in [Fauda](#) passen (wann endlich kommt die [vierte Staffel](#) bei Netflix?), aber vermutlich ist sie dafür zu hübsch. Man würde abgelenkt wie in [Sentinelle](#), dessen dämlicher Propaganda-Plot für ~~sinnlos~~ Herumballern französische Anti-Terror-Einheiten auch durch [Olga Kurylenko](#) nicht besser und erträglicher wird.

Apropos Lächeln für Hetero-Männer: Meine persönliche Favoritin wäre zur Zeit [Skade](#), deren realer Name ziemlich komisch ist und besser nach Schottland passte als nach Norwegen. Ihr Lächeln ist sehr süß – ich würde kaum widerstehen können -, aber immer zweideutig: Es könnte auch bedeuten, dass sie einem bald die [Klößen abschneidet](#). Auf keinen Fall langweilig und der einzige Grund, warum man die schwachsinnige Kinderserie (keine Nacktszenen!) [The Last Kingdom](#) länger als eine Viertelstunde ertragen kann.

KAX17



[Heise](#): „KAX17 führt massive Deanonymisierungsangriffe durch. – Laut einem [IT-Sicherheitsforscher](#) betreibt ein mysteriöser Akteur seit 2017 große Teile des Anonymisierungsdiensts Tor, womit dieser unterwandert werde.“

[Tarnkappe.info](#) dazu: *Besonders besorgniserregend ist seiner Meinung nach die Tatsache, dass KAX17 seine Server im industriellen Stil betreibt. Er nutzt dafür Rechenzentren auf der ganzen Welt und lässt sich diesen Spaß richtig was kosten. (...) KAX17 kann aufgrund seiner umfassenden Überwachung des Tor-Netzwerks Tor-User mit den folgenden Wahrscheinlichkeiten de-anonymisieren:*

[Guard](#): 10,34 %

[Middle](#): 24,33 %

[Exit](#): 4,6 %.

Na gut. Man kennt die [Risiken](#), auch im [Darknet](#), schon [länger](#). Aber ich frage mich, warum die üblichen Verdächtigen so viel Mühe auf sich nehmen und so viel Geld verprassen, um ein paar Leute zu deanonymisieren?

Ganz geheime Postkarten

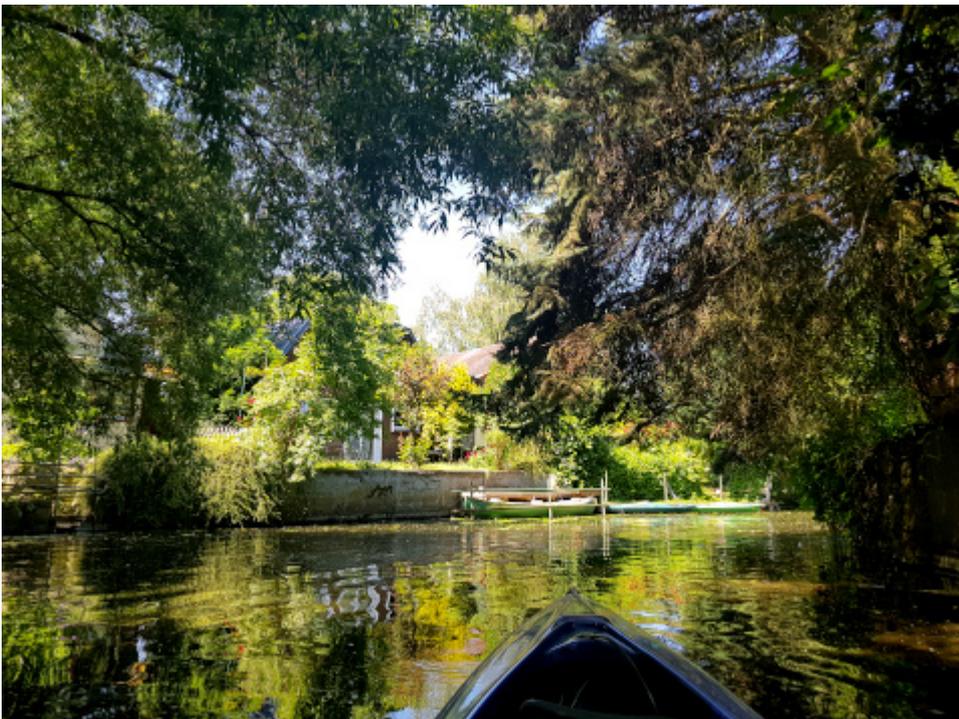
```
Return-path: <SRS0=R/ohbhJT=QS=anonymousemail.me=noreply@srs.mi
Envelope-to: burks@
Delivery-date: Wed, 01 Dec 2021 12:31:37 +0100
Received: from [193.96.188.111] (helo=mail.minuskel.de)
by home.minuskel.de with esmtp (Exim 4.84_2)
(envelope-from <SRS0=R/ohbhJT=QS=anonymousemail.me=noreply@srs.
id 1msNpp-0006rZ-53
for burks@
Wed, 01 Dec 2021 12:31:37 +0100
Received: from s4.etalimpact.info ([202.61.207.162])
by mail.minuskel.de with esmtps (TLS1.2) tls TLS_ECDHE_RSA_WITH_AES_1
(Exim 4.94.2)
(envelope-from <noreply@anonymousemail.me>)
id 1msNpk-0005Nd-W6
for burks@burks.de; Wed, 01 Dec 2021 12:31:36 +0100
Received: from authenticated-user (s4.etalimpact.info [202.61.207.162])
(using TLSv1.3 with cipher TLS_AES_256_GCM_SHA384 (256/256 bits))
(No client certificate requested)
by s4.etalimpact.info (Postfix) with ESMTPSA id CEE50E0365
for <burks@burks.de>; Wed, 1 Dec 2021 11:31:29 +0000 (UTC)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple;
```

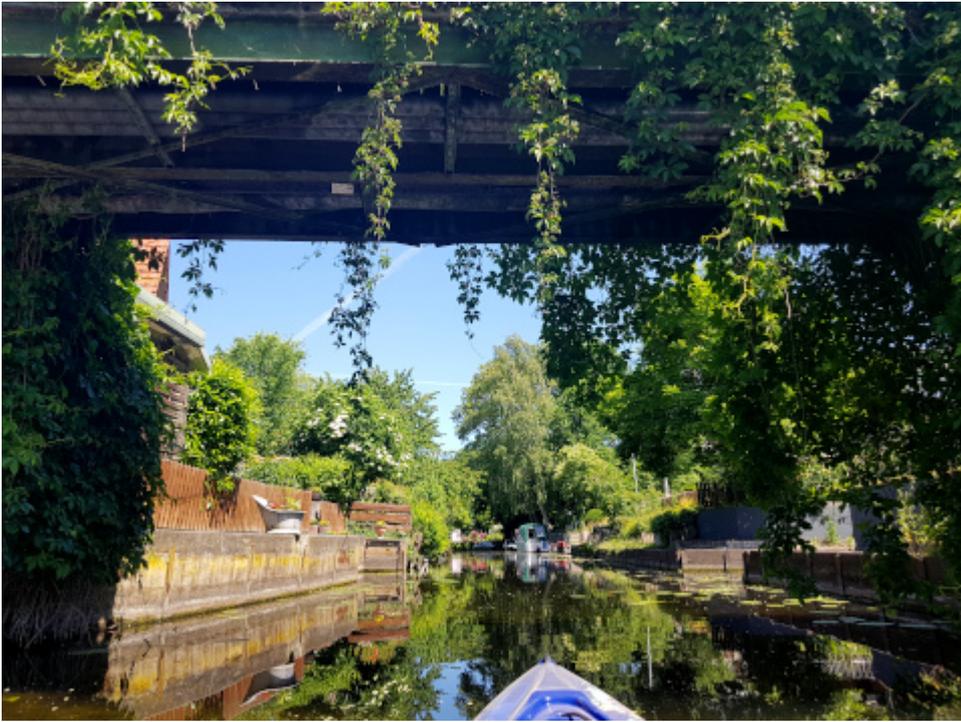
Vor ein paar Tagen bekam ich seit langer Zeit wieder einmal eine anonyme E-Mail mit interessanten Inhalten (nein, es ging nur um Vereinsmeierei). Ich war mir nicht bewusst, dass so etwas noch [auf dem „Markt“](#) ist.

Ich traue aber den Angeboten nicht über den Weg. Wenn schon, dann aber richtig. Lustig ist zum Beispiel, wenn diejenigen, die so etwas offerieren, dann die [IP-Adresse](#) in den [Header](#) einbinden. [ProtonMail](#) ist nur [per Tor-Browser](#) wirklich sicher und auch nicht kostenlos.

Verschlüsselte E-Mails haben bekanntlich den Nachteil, dass „man“ herausfinden kann, wer mit wem kommuniziert – das ist manchmal wichtiger als der Inhalt (so war es auch in meinem Fall). Ich werde bei Gelegenheit die [„Werkzeug“-Website](#) updaten.

Leibes- und andere Übungen üben





Wie unschwer zu erkennen ist, habe ich mich heute (Vier-Tage-Woche im Sommer!) weder mit Budin oder Piden – oder wie die Charaktermasken alle heißen mögen – beschäftigt und auch nicht mit Sportarten, die gern in Massenhysterie der unangenehmen Art ausarten (Llongyfarchiadau Cymru! Da iawn!), sondern Leibesübungen der mittelschweren Art betrieben (Übungen betreiben? Sagt man das so?), wie gewohnt beginnend in Tiefwerder, dessen idyllische Teilmenge auch als [Klein-Venedig](#) bekannt ist, dann gen Norden zum [Südhafen](#) abbiegend (Ha! Ist das jetzt gar ein Antitheton?) bis zur [Schleuse](#), die einen

zwingt, das Boot [per Trolley](#) zu schleppen, dann zwischen [vielen Inseln](#), deren Namen alle mit [-werder](#) enden, herumirrendpaddelnd, daraufhin – immer noch frohgemut und ohne Sonnenbrand! – zurück.





Ich finde übrigens das [chinesische Abendmahl](#) eine lustige Trollerei. So geht Propaganda.

Und so geht [Verschlüsselung](#) *nicht*: „Forscher entdecken, dass viele Handys beim Surfen nach wie vor veraltete und angreifbare Verschlüsselungstechnik einsetzen. Sie sind sich sicher: Die Schwachstelle wurde mit Absicht eingebaut“ (via [Fefe](#)). Dazu gibt es noch [uralte Artikel](#) – die passenden [Cryptophone](#) kosten soviel wie mein E-Bike. Hat die Schwarmintelligenz damit vielleicht Erfahrungen gesammelt?



Herzliche Grüße an alle attraktiven Wassersportlerinnen!

Datenschutz-Verfahren und Folterwerkzeuge, revisited

[Berliner Zeitung](#): „Nach Recherchen der Berliner Zeitung reagiert Deutschlands oberster Datenschützer. Zugang zu Stasiunterlagen Dritter soll künftig besser kontrolliert werden.“

„Anlass für das aktuelle Prüfverfahren gegen die Behörde ist der Fall des Berliner Fotojournalisten [Bernd Lammel](#), der seit Jahren gegen Stasivorwürfe kämpft, und der nun feststellen musste, dass die BStU in den letzten Jahren nicht nur ihn, sondern 164 Menschen aus seinem Umfeld „ausgeforscht“ und mehr als tausend Seiten Akten an Journalisten herausgegeben hat. Der Begriff „Ausforschung“ stammt dabei von der Behörde selbst: Das Vorgehen gegen Lammel und sein Umfeld hat im Jahr 2017 eine interne Prüfung nach sich gezogen, die vernichtend ausgefallen ist.“

Ich werde das zum Anlass nehmen, eine Strafanzeige zu stellen. I keep you informed.

Datenschutz-Verfahren und Folterwerkzeuge

[Übermedien](#): „Nach „Ausforschung“ von Journalisten: Datenschutz-Verfahren gegen Stasi-Unterlagenbehörde“.

Die Sache, die ursprünglich nur die [Akte Lammel](#) war, zieht immer weitere Kreise. „Wie nun bekannt wurde, hat [Ulrich Kelber](#), der Bundesbeauftragte für den Datenschutz und die

Informationsfreiheit (BfDI), kurz nach der Veröffentlichung ein datenschutzrechtliches Prüfverfahren in die Wege geleitet. Dem Beauftragten für die Stasi-Unterlagen, Roland Jahn, wurde ein Fragenkatalog übersandt mit einer ungewöhnlich kurzen Bearbeitungsfrist von nur einer Woche. Seit dem 7. Mai liegt Jahns Antwort im Haus von Kelber vor. Sie bestätigte die Vorwürfe und Recherchen – und stellt den Bundesdatenschutzbeauftragten offenbar nicht zufrieden.“

Der Bundesdatenschutzbeauftragte hat Jahn und seiner Behörde offensichtlich die Folterwerkzeuge gezeigt, wenn weiter gemauert würde: *Im Anschluss hieran wird zu prüfen sein, ob die bisher durch BStU getroffenen Maßnahmen ausreichend sind, oder weiterer Handlungsbedarf besteht, der erforderlichenfalls auch mit aufsichtsrechtlichen Maßnahmen durchzusetzen wäre.* Dem Bundesdatenschutzbeauftragten stünden in diesem Falle umfangreiche Mittel zur Verfügung.“

„Grundlage für die nun eingeleitete Prüfung waren Hinweise darauf, dass Medienanträge einiger weniger Redaktionen in der Stasi-Unterlagenbehörde auch dann bearbeitet wurden, wenn sie erkennbar unzulässig waren – und so teils privateste Informationen die Behörde verließen.“

Als kleines Schmanckerl kommt hinzu: Ulrich Kelber ist Sozialdemokrat. Die Jahn-Behörde unterliegt der Dienstaufsicht durch die Bundesbeauftragte für Kultur und Medien (BKM, aka Kulturstaatsministerin) [Monika Grütters](#), und die ist CDU. Da haben zwei ein Interesse, sich vor den Wahlen noch zu profilieren, und zu meinem Vergnügen nicht miteinander.

Unter Faxern

Versendet hier jemand noch [Faxe](#)? (via [Fefe](#)) „Telefax ist nicht Datenschutz konform“.

Offener Brief an den Vorstand des DJV Berlin – JVBB

Offener Brief an den [Vorstand des DJV Berlin – JVBB](#)

Liebe Kolleginnen und Kollegen des Vorstands des DJV Berlin – JVBB,

die Veröffentlichungen von [BuzzFeed](#), [Übermedien](#), [Berliner Zeitung](#), Frankfurter Rundschau, [mdr 360G](#), [Turi2](#), [HNA](#) und [Merkur](#) über die unzulässige Ausforschung von Mitgliedern unserer Gewerkschaft durch die Behörde des Bundesbeauftragten für die Stasi-Unterlagen (BStU) aufgrund von Medienanträgen des rbb und der Bild-Zeitung sind dem Vorstand inzwischen sicher bekannt. Die Abfragen des rbb im Zeitraum von 2010 bis 2017 betreffen fast 50 Funktionäre des damaligen DJV Berlin aus sämtlichen Gremien wie Vorstand, Fachausschüssen und Ehrengericht – bei einzelnen Personen sogar rückwirkend bis zum Jahr 2000.

Der [DJV-Bundesvorstand](#) hat sofort nach Kenntnisnahme der Ergebnisse eines internen Prüfverfahrens der BStU den daraus ersichtlichen Aktenskandal öffentlich benannt und Konsequenzen von der dienstaufsichtführenden Staatsministerin für Kultur und Medien im Bundeskanzleramt, Monika Grütters, vom BStU und dem Bundesdatenschutzbeauftragten gefordert.

Der Vorstand unseres Landesverbandes will offenbar selbst nicht handeln und hat sich in dieser Frage – außer durch wenige Zeilen unseres Vorsitzenden [Steffen Grimberg](#) im Newsletter – bisher auch nicht geäußert. Das wirkt auf uns sehr befremdlich. Er sollte dafür sorgen, dass die Ausforschung von Mitgliedern unseres Verbandes, verbunden mit Verstößen gegen das [Stasiunterlagengesetz](#) (StUG), das [Bundesdatenschutzgesetz](#) und die [Datenschutzgrundverordnung](#) (DSGVO) nicht unter den Teppich gekehrt wird!

Die Unterzeichnenden waren Mitglieder des DJV Berlin und sind heute Mitglieder im DJV Berlin – JVBB. Wir alle wurden vom BStU unrechtmäßig ausspioniert. Das hat die Behörde in einem internen fachaufsichtlichen Gutachten selbst zugegeben. Was mit unseren Daten geschehen ist und wer immer noch darauf Zugriff hat, wissen wir nicht.

Wir erwarten vom Vorstand, Maßnahmen zu ergreifen, die Rechte seiner Mitglieder durchzusetzen. Dazu gehören Beschwerden beim Landesdatenschutzbeauftragten Berlin und beim Kultursenator, ebenso bei der Intendanz und Chefredaktion des rbb sowie bei der Verlagsgeschäftsführung des Springer-Verlags und der Chefredaktion der Bild-Zeitung. Wir verlangen, dass der Vorstand uns bei weiteren Schritten sowohl gegen den BStU als auch gegebenenfalls gegen die Bild-Zeitung und den rbb in Sachen Persönlichkeitsrecht und Datenschutz individuellen persönlichen Rechtsschutz gewährt.

Im Zuge eines [Drittbeteiligungsverfahrens](#), das durch einen Antrag nach Informationsfreiheitsgesetz (IFG) der rbb-Reporterin Gabi Probst durch den IFG-Beauftragten der BStU eingeleitet worden ist, sind sowohl die Medienanträge von Gabi Probst zu Mitgliedern des DJV Berlin als auch die behördeninternen Unterlagen zu den Ausforschungen offenkundig geworden. Die BStU hat in dem erwähnten Gutachten festgestellt, dass bereits die Medienanträge von rbb und Bild unzulässig waren.

Wir fordern, dass die Kollegin Gabi Probst ihr Amt im [Aufnahmeausschuss](#) niederlegt und dass der Vorstand sie dazu auffordert. Ihre Recherche-Methoden schädigen das Ansehen des Verbandes, auch angesichts der Presseberichte zu diesem Thema. Aus unserer Sicht ist der Fall Gabi Probst eine Angelegenheit für das [Schiedsgericht](#) des DJV Berlin – JVBB.

Mit kollegialen Grüßen

Simone Ahrend

Clemens Glade

Prof. Dr. Peter Kolbe

Inge Kundel-Saro

Bernd Lammel

Caroline Methner

Ann Schäfer

Burkhard Schröder

Dr. Wolf Siegert