

Böses Tölchen verhindert Online-Durchsuchung



Grmpf. Hat doch unser Tölchen aka Ajax vom Teufel(!)slauch nicht nur das Netzkabel von Frauchens Laptop durchgeknabbert, sondern auch noch das vom Fujitsu Siemens Amilo A 1630 Netzteil Ladegerät. Jetzt müssen wir schnell beides neu kaufen. Da fällt mir beim Sichern der Daten bzw. beim Upload auf den Server ein: Wie stellen sich unsere Verschwörungstheoretiker und die Mitglieder der Glaubensgemeinschaft *Heilige Online-Durchsuchung der letzten Tage™* eigentlich das Hochladen der Daten auf die Rechner der Strafverfolger vor? Der „Bundestrojaner“, den es nur als Wahnvorstellung in den Köpfen der Politiker gibt, soll auch [gegen Kinderpornografie](#) helfen. Und wie wollen die Ermittler zur Beweissicherung ein paar tausend schweinische Dateien uploaden, ohne dass der Verdächtige das merkt? Es gbt doch zahlreiche Tools zur Systemüberwachung wie [Munin](#) für Ubuntu – oder man schaut einfach ins [Systemprotokoll](#)? Falls Schäuble gerade den Debian-Nobelpreis heimlich bekommen hat, an unserem Router vorbeigekommen ist und Daten vom Linux-Laptop meiner Gattin gerichtsfest sichern und hochladen wollte, dann hat ihn unser Tölchen daran gehindert.

Nachtrag: Wie aus gewöhnlich gut [unterrichteten Kreisen](#) verlautet, funktioniert die Online-Durchsuchung auch in die andere Richtung.

Online-Durchsuchung | Willkommen in Schilda!

Eben habe ich mich kringelig gelacht. Es gibt doch tatsächlich eine [FAQ](#) („Fragen und Antworten zum Thema Online-Durchsuchungen“) des Bundesministeriums des Innern, bei der man sich fragen muss, ob besoffene Praktikanten jetzt die Website deutscher Ministerien vollschreiben dürfen. Offenbar sind die dort alle auf Drogen:

„Das Risiko einer Entdeckung und der missbräuchlichen Nutzung der Ermittlungssoftware wird durch geeignete technische Maßnahmen so gering wie möglich gehalten. Sollte die Software dennoch entdeckt werden, wird sie vom Zielsystem entfernt.“ – „Die Betroffenen werden grundsätzlich nach Abschluss darüber unterrichtet, dass die Ermittlungssoftware bei ihnen auf den Rechner gespielt wurde.“ – „Die gewonnenen Daten werden dabei ggfs. unter Zuhilfenahme technischer Auswertungs-Instrumente (sog. „Tools“) vorselektiert, so dass für die manuelle Analyse ein überschaubarer Datenbestand verbleibt.“

Ich habe mich noch einmal extra vergewissert, dass ich nicht auf einen Fake hereingefallen bin. Ich kann es immer noch nicht glauben: Das ist wirklich die Seite des deutschen Innenministeriums! ROTFL. Willkommen in [Schilda](#)!

Unter Propagandisten

SORM & Co.: Russland bei digitaler Massenüberwachung an vorderster Front?

Alle Heise-Foren > heise online > Kommentare > SORM & Co.: Russland bei digi...

Alles aufklappen Alles zuklappen Anmelden und mitdiskutieren

<input type="checkbox"/> Da ist noch Luft nach oben.	Maniac1000
<input checked="" type="checkbox"/> Tja, jetzt wird man bei uns ganz neidisch (1)	die kleine Him
<input checked="" type="checkbox"/> EU und Deutschland ebenso (2)	keeper_of_tra
<input checked="" type="checkbox"/> Merkwürdig - weder Wikileaks noch Snowden berichten. (2)	Mustermann
<input checked="" type="checkbox"/> Technische Frage: Aufbrechen von verschlüsselter Kommunikation?	Smirgl
Re: Technische Frage: Aufbrechen von verschlüsselter Kommunikation?	woody_woodp
Re: Technische Frage: Aufbrechen von verschlüsselter Kommunikation?	OttoPa
<i>Gesperrter Beitrag</i>	
Re: Technische Frage: Aufbrechen von verschlüsselter Kommunikation?	p4ran0id
Re: Technische Frage: Aufbrechen von verschlüsselter Kommunikation?	rainer_d
Re: Technische Frage: Aufbrechen von verschlüsselter Kommunikation?	n0pey
Re: Technische Frage: Aufbrechen von verschlüsselter Kommunikation?	Marie Huana
<input checked="" type="checkbox"/> Hoch geschätzter Herr Krempf (8)	cooregan
<input checked="" type="checkbox"/> Und wir rennen fleißig hinterher! (7)	Anubiz

Jemand fragte bei Heise: „Wie genau schafft es Russland verschlüsselte Kommunikation aufzubrechen? Ich bin bisher davon ausgegangen, dass man das nur mit dem Einsatz von Trojanern auf dem Gerät des Nutzers hin bekommt. Welchen Beitrag die Kompromittierung der Netze dazu hat, ist mir nicht klar.“

Ich hatte geantwortet, dass der Autor [des Artikels](#), Stefan Krempf, nur die „Propaganda der Sicherheitsbehörden“ wiedergebe. So war das auch beim Thema „Online-Durchsuchung“.

Mein Beitrag würde von Heise wegen ~~Hassrede~~ gesperrt. Die sind ganz schön dünnhäutig. Also habe ich offenbar einen Nerv getroffen.

Ich erinnere an [Annette Ramelsberger](#) in der „Süddeutschen“: „Den meisten Computernutzern ist es nicht klar: Aber wenn sie im Internet surfen, können Verfassungsschützer oder Polizei online bei ihnen zu Hause auf die Festplatte zugreifen und nachschauen, ob sie strafbare Inhalte dort lagern – zum Beispiel Kinderpornographie oder auch Anleitungen zum Bombenbau.“

Auch das nenne ich „die Propaganda der Sicherheitsbehörden“

wiedergeben“. Journalismus ist das nicht.

Trojaner auf externen Internet-Festplatten



Darstellung einer Online-Durchsuchung mit „Staatstrojaner“ aus Zachiku, Mittani-Reich, ca. 1550 – 1350 v. Chr., Fundort Mosul-Stausee im Irak

Kreml liefert bei [Heise](#) wieder den gewohnten Bullshit ab: „Strafverfolger haben Staatstrojaner 2021 häufiger eingesetzt. Die Gerichte genehmigten 2021 55-mal das Hacken von IT-Geräten, während es 2020 48 Anordnungen gab.“

Ach ja? Wie machten die das? „Mithilfe von Staatstrojanern“ natürlich. „Dabei dürfen die Fahnder etwa auch Festplatten inspizieren und nicht nur die laufende Kommunikation mitschneiden.“ Die [Internet-Festplatten](#) sind schon seit 2006 als Textbaustein in Mode.

Ich halte das für ein [fettes Lügenmärchen](#) aus der Propaganda-Maschine der Strafverfolger, das Kreml wie gewohnt kritiklos wiederkaut. Natürlich können die üblichen Verdächtigen

„Kommunikation“ in Echtzeit verfolgen, etwa bei der Telefonie. Aber sie können nicht einfach so auf externe „Festplatten“ zugreifen, schon gar nicht „von weitem“, außer der Verdächtige ist so bekloppt, dass er vermutlich gar keinen Computer bedienen könnte.

Außerdem gab es da mal ein Urteil des Bundesverfassungsgerichts. Jemand kommentierte ganz richtig: „Zunächst mal heißt es eben nicht, daß das Instrument auch eingesetzt wurde, nur weil ein Richter die Erlaubnis erteilt hat. Und weiterführend sagt das auch nichts darüber aus, ob es erfolgreich eingesetzt wurde, ob verwertbare Informationen erlangt wurden, die sonst nicht erlangt worden wären, usw..“



Darstellung einer Online-Durchsuchung mit „Staatstrojaner“ aus Zachiku, Mittani-Reich, ca. 1550 – 1350 v. Chr., Fundort Mosul-Stausee im Irak

Surveillance, allüberall und nirgends [Update]



Midjourney/©Burks

[Heise](#) veröffentlicht Bullshit-Bingo für Klein-Fritzchen, natürlich von [Stefan Krempl](#). Ich weiß nicht, was den treibt. „Polizei soll Staatstrojaner nicht mehr bei Alltagskriminalität einsetzen.“

– Erstens heißt es nicht „Staatstrojaner“. Die Trojaner waren draußen, die Griechen saßen im Pferd.

– Zweitens [darf die Polizei das nicht](#) (was sie natürlich nicht daran hinderte). Es gibt ein [Grundrecht](#) auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Oder ist die Entscheidung des Bndesverfassungsgerichts mittlerweile revidiert worden, Heise? Nein, ist sie nicht.



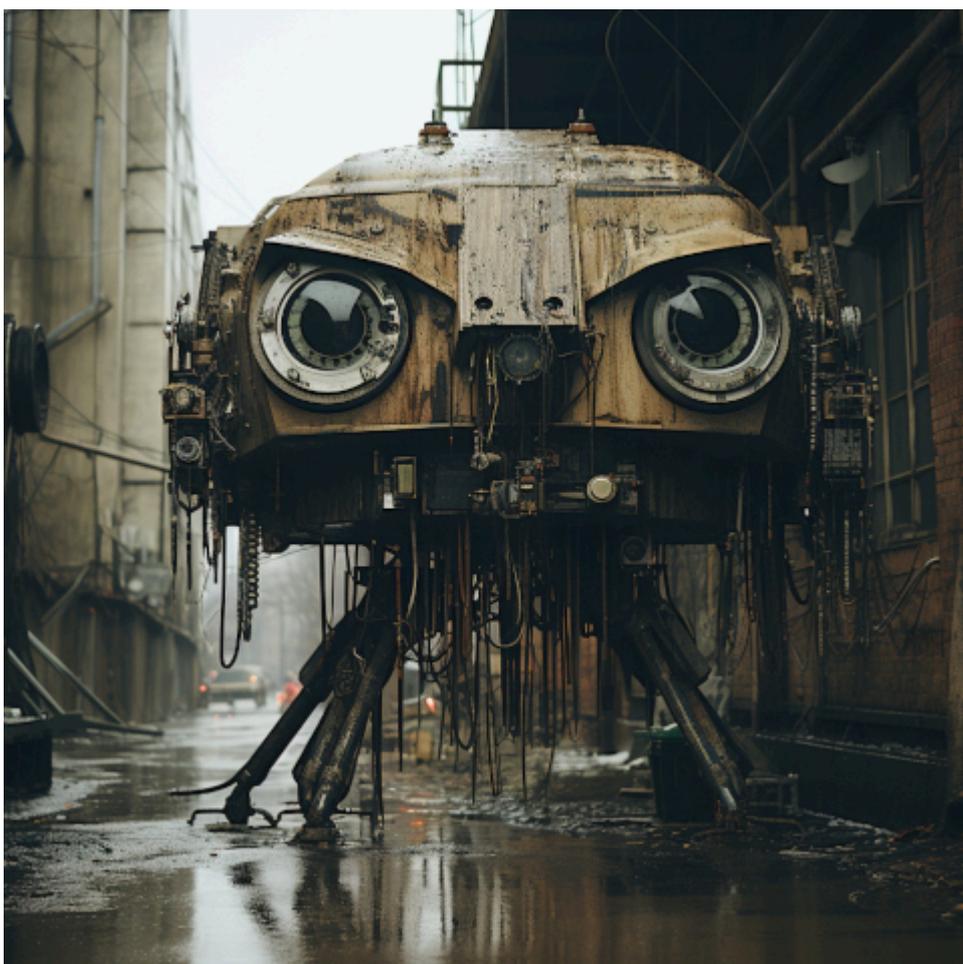
Midjourney/©Burks

– Drittens ist es technisch grober Unfug, auch wenn [tausend juristische Pappnasen](#) das immer wieder anders behaupten. Man sollte auch nicht die Transportverschlüsselung mit der Verschlüsselung von Inhalten auf einem Rechner verwechseln. Nur noch einmal, Krempl, zum langsamen Mitschreiben: **niemand** (in Worten: niemand) kann auf meine Rechner von „draußen“ zugreifen, selbst wenn ich einen Angriffskrieg vorbereitete. **Niemand** hat auch bisher erklärt, wie das gehen sollte. Die raunen nur alle geheimnisvoll herum und tun sich wichtig damit.

Ohne weiteres kann der Staat jedoch nicht erfassen, was auf einem Computer geschieht. Der einzige Weg ist über Sicherheitslücken in den betroffenen Systemen. Und hier muss man sich schon wundern: Statt, dass der Staat hilft, bekannte Lücken zu schließen oder zumindest auf sie aufmerksam zu machen, die letztlich alle Nutzer von Computern gefährden und

von Kriminellen ausgenutzt werden können, nutzt er sie selbst aus, um das Gerät zu hacken und „mitlesen“ zu können. (Das „schreiben [Mitarbeiter der intersoft consulting](#), die als Experten für Datenschutz, IT-Sicherheit und IT-Forensik international Unternehmen beraten.“)

Der Staat nutzt also Lücken aus? Wie denn? Beispiele?! Das Bundesinnenministerium kauft also [Zero-Day-Exploits](#), womöglich für Linux? Ihr spinnt doch.



Midjourney/©Burks

– Viertens gibt es die „Online-Durchsuchung“ weder bei „Alltagskriminalität“ noch bei schweren Straftaten, nur im nachhinein, wenn die Rechner des Verdächtigen beschlagnahmt wurden und dieser auch noch ein IT-Vollidiot ist.

Was will mir dieser Artikel suggerieren? „Bei der Quellen-TKÜ geht es darum, die laufende Kommunikation per Staatstrojaner direkt auf dem Gerät eines Verdächtigen abzugreifen, bevor sie

ver- oder nachdem sie entschlüsselt wurde.“ Ach ja? Und wie soll das gehen? Kreml, du bist ein Verschwörungstheoretiker.

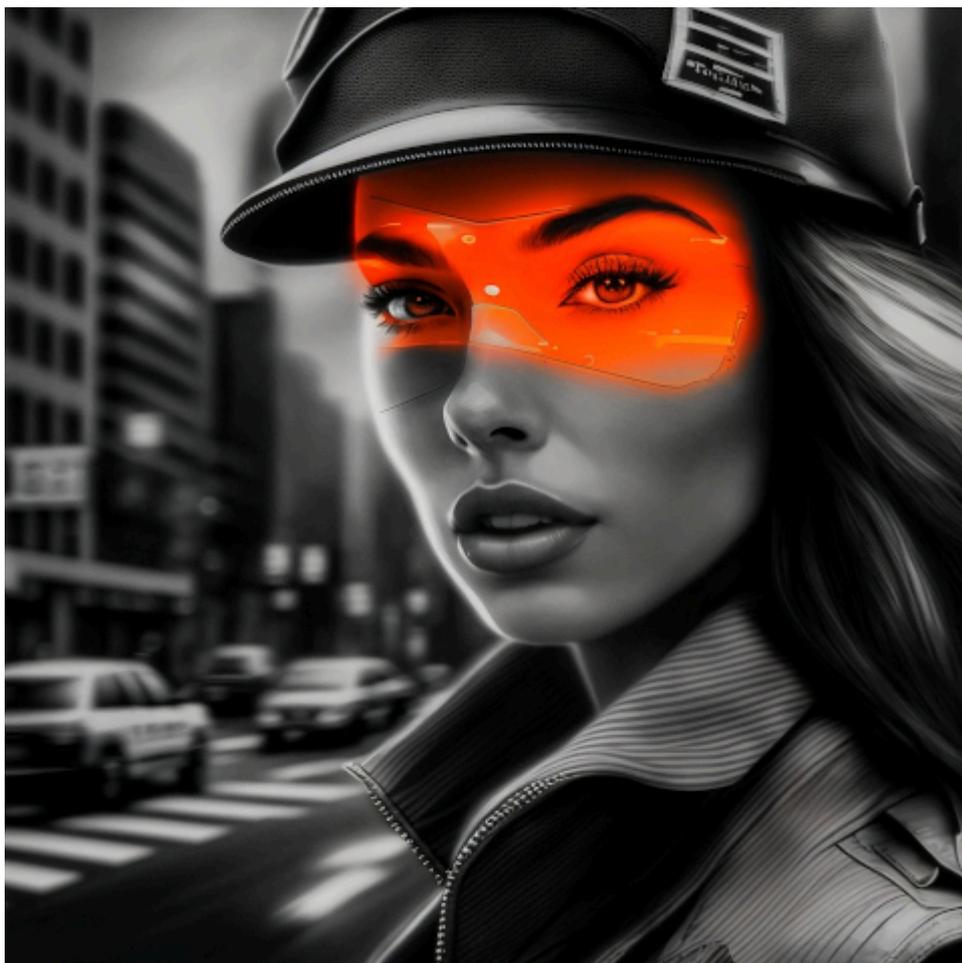
Dazu passt noch [ein ganz ähnlicher Artikel](#): „Autos, Navis & Co.: Polizei will Zugriff auf alles – unverschlüsselt und sofort“. Schon klar. Ich will auch Diktator von Deutschland werden. Das ist ähnlich realistisch, selbst wenn diejenigen, die das fordern, Nachhilfeunterricht [beim Chinesen](#) nähmen.



Midjourney/©Burks

[Update] Links repariert.

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.*

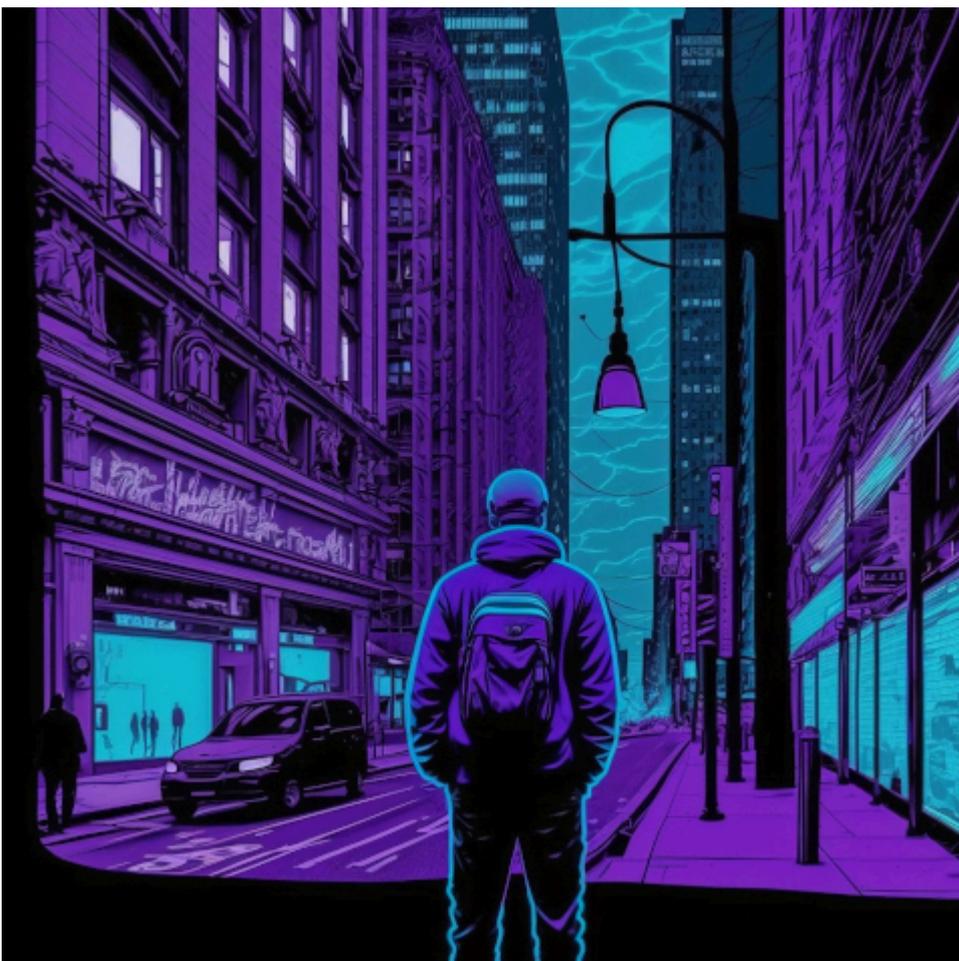
Falsch. Auf meine Rechner kommt nichts, was ich nicht erlaubt habe. [Pegasus](#) kommt auch nicht auf mein Android-Smartphone, weil ich alle „Infektionswege“ kenne und vermeide. *Der Angriff erfolgt grundsätzlich über iMessage in Form einer Nachricht mit einem Link zum Anklicken.* Warum zum Teufel sollte 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.



Unter Staatstrojanern (m/f/d)



Online-Durchsuchung und Chatkontrolle in Secondlife (2007)

Da ist sie wieder, die gute, alte [Online-Durchsuchung](#), von der immer noch niemand zu sagen weiß, wie sie denn funktionieren soll. Jetzt hat sie sich das Kostüm „Chatkontrolle“ umgehängt und geistert geheimnisvoll raunend durch die Medien.

Durch das „[Gesetz](#) zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens“ durften Behörden versteckte Schadsoftware auf Computern, Laptops und Smartphones platzieren.

Soso, lieber Kollege Jakob Schirmmacher, der nach eigenen Angaben „1987 noch nicht gelebt“ hat und, ebenfalls [nach eigenen Angaben](#), freier Journalist, Autor, Dozent für Medien und Digitalisierung ist, also so etwas wie ich, nur ohne Zweitberuf, und, [ebenfalls nach eigenen Angaben](#), jemand ohne PGP-Schlüssel auf der Website. Die dürfen „versteckte Schadsoftware“ auf meine Linux-Rechner beamen, womöglich von fern, wenn ich gerade nicht hingucke, warum es [verdächtig ruckelt](#)?

Ich habe da mal eine Frage: Wie machen „die“ das? Vielleicht darf man das gar nicht fragen, weil es supergeheim ist? Und

hatte das Bundesverfassungsgericht die so genannte TKÜ (Quellen-Telekommunikationsüberwachung) nicht 2008 [verboten](#)? Da warst du doch schon geboren, lieber Kollege?!

Was auffällt: Die Überwachungsmaßnahmen kommen dem Bürger näher und näher: vom Auto in den Wohnraum, hin zum Telefon und schließlich bis hin in die tiefste Gedankenwelt. Dies gelang beispielsweise durch die später eingeführte Quellen [TKÜ](#) (Quellen-Telekommunikationsüberwachung), die 2017 ihre Vollendung feierte. Durch das „Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens“ durften Behörden versteckte Schadsoftware auf Computern, Laptops und Smartphones platzieren.

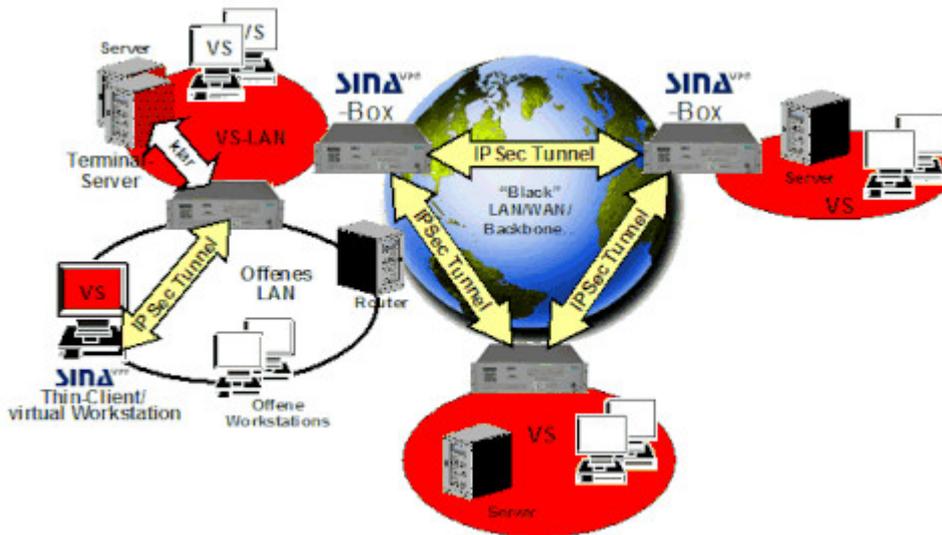
Der sogenannte Staats Trojaner ermöglichte es Behörden, Messenger Chats und SMS mitzulesen, sowie Kameras und Mikrofone zu benutzen. Der Gesetzestext [dazu lautet](#): „Die Überwachung und Aufzeichnung der Telekommunikation darf auch in der Weise erfolgen, dass mit technischen Mitteln in von dem Betroffenen genutzte informationstechnische Systeme eingegriffen wird, wenn dies notwendig ist, um die Überwachung und Aufzeichnung insbesondere in unverschlüsselter Form zu ermöglichen“.

Mir ist eine „drohende“ Chatkontrolle übrigens völlig schnurzpieegal. Ich mache das so, wenn ich nicht ohnehin das quelloffene [Signal](#) benutze: Ich rufe irgendein [IRC](#)-Programm auf. Vorher habe ich mich per verschlüsselter E-Mail mit meinen Mitverschworenen (m/f/d) verabredet, dass wir uns auf [irc.brasirc.com.br](#) treffen und dort einen passwortgeschützten Kanal eröffnen. Und dann chatten wir und [tauschen Daten aus](#).

Nein, ich habe eine bessere Idee. Wir loggen uns mit halbnackten Avataren in Secondlife ein und treffen uns in einem Adult-Segment (irgendwas mit Porn) oder treffen uns auf [meiner Sim](#), umbraust von virtuellen Sandstürmen und die virtuellen Waffen immer griffbereit, um Chatkontrolleure virtuell abzumurksen.

Ich finde ein Gesetz zur Chatkontrolle gut und richtig. Dann befassen sich die, die jetzt noch zum Thema ahnungslos herumfaseln, endlich mit Sicherheit und Datenschutz. Oder halten die Kresse, was auch nicht schlecht wäre.

Sonstige Rechte



Credits: [BSI](#)

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 moralfreien Desinformationsöldnern

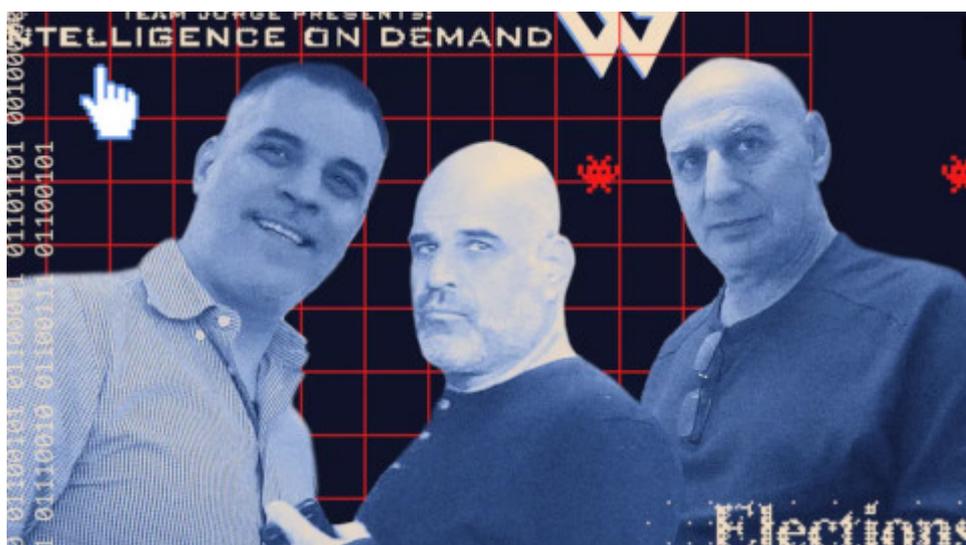


Foto: [M] Lina Moreno / DER SPIEGEL; Fotos: Screenshot / Team Jorge Präsentation

Nach Monaten der falschen Fährten, Fallen und Versteckspiele endlich eine vielversprechende Spur. Sie führt ins karge israelische Bergland, in eine [hässliche Planstadt](#) auf halbem Weg zwischen Tel Aviv und Jerusalem. Zwischen zwei Autobahnen steht dort ein gesichtsloses Bürozentrum der Eingang ist versteckt. Es geht durch die Tiefgarage, hoch in den dritten Stock, an der Sicherheitstür hängt kein Schild, kein Hinweis. Drinnen: drei Männer, alle über 50, alle mit langen Karrieren als Agenten, Militärs. Schattengestalten, die Tarnnamen nutzen. Die offiziell nicht existieren. (Anreißer der [Spiegel-Titelgeschichte](#))

Karges Bergland. Hässliche Planstadt. Gesichtsloses Bürozentrum. Was fehlt: Es war neblig und es regnete. Räudige Hunde streunten herum. Die Straßen voller Schlaglöcher. Die hakennasigen Agenten blickten finster und stumm im Raum herum. ~~Und alles voller Juden, mindestens vom Mossad.~~ Im Ernst? Diese Räuberpistole wollt ihr mir andrehen? Da muss man mal genauer

hinsehen und die heiße Luft wegpusten.

Der Guardian hat daraus eine mehrteilige Story gemacht: „[The secret world of disinformation](#) for hire“, „How [undercover reporters caught](#) ‘Team Jorge’ disinformation operatives on camera“, „‘Aims’: the software for hire [that can control](#) 30,000 fake online profiles“.

Für mich sieht das übrigens so aus, als hätten der Guardian, [Forbidden Stories](#) sowie [Gur Meggido](#) und [Omer Benjakob](#) die Recherche angeschoben, und dass sich die deutschen Medien nur drangehängt haben.

Last year, coordinated by the French media organisation Forbidden Stories, a group of journalists from around the world, including from the Guardian, embarked on a project: to get inside the murky world of disinformation and expose those who profit from it.

Der Plot ist natürlich interessant, haut mich aber nicht vom Stuhl. Regierungen geben Millionen aus, um Wahlen zu gewinnen, zu bestechen und fälschen oder so tun, als seien die Wahlen nicht manipuliert. Hier ist es eine private Firma mit dem Namen [Demoman International](#), die, wenn sie nicht in Israel säße, sondern in Papua-Neuguinea, nicht so viel Aufsehen erregt hätte.

Ich habe mal ein bisschen herumrecherchiert: Die Firma [wurde 1999 gegründet](#) und residiert in [Nazareth Illit aka Nof HaGalil](#). Die hätte ich auch allein herausgefunden und auch nicht Monate dafür gebraucht. Die machen angeblich alles, was man aus einschlägigen Filmen kennt, vermutlich auch Vorbereitung von Angriffskriegen. Geld regiert die Welt. So schlimm wie [Academi](#) sind sie aber noch nicht.

Viele im Land wissen nicht mehr, was wahr ist, oder falsch. Später werden die Israelis demonstrieren, wie sie offenbar in das E-Mail-Konto eines mächtigen kenianischen Politikers eindringen. (Spiegel)

Stimmt: Die „Online-Durchsuchung“ darf auch nicht fehlen. Man ahnt, dass es bei dem Herumgeraune eher darum geht, das vermeintliche eigene Herrschaftswissen zu verteidigen. Die klassischen Medien können „Wahrheit“ und „Lüge“ unterscheiden, die dumme Bevölkerung aber nicht. Mich regt diese Attitude maßlos auf. „Einen Truppe moralfreier Desinformationssöldner“ – welche Moral denn? Und wer hat die? Wollen die suggerieren, etwas die US-amerikanische Regierung oder die russische herrschende Klasse scherten sich um Moral? Die Einzigen, die moraltriefend herumheulen, sind die deutschen Grünen und [durchgeknallte höhere Töchter](#) – deswegen verstehen sie auch die Welt nicht.

Die Moral von der Geschicht' taucht plötzlich zwischendrin auf: „In den vergangenen Jahren ist eine rasant wachsende Desinformationsindustrie entstanden“. Ach? Da wäre ich gar nicht drauf gekommen. Wenn das Stalin gewusst hätte! (Den Satz: „Immer wieder zeigen sich Verbindungen nach Russland“ hättet ihr euch sparen können, liebe Kollegen – es geht hier um eine israelischen Firma, und die beunruhigte Leserschaft ahnt ohnehin, dass *alles* irgendwie auf Putin hinweist, auch wenn es an den Haaren herbeigezerrt wird.) Mehr als eine ganze Seite handelt demgemäß von den finsternen Russen, die mit dem „Team Jorge“ rein gar nichts zu tun haben. Die Zitate des Verfassungsschutzes, der vor irgendetwas warnt, habe ich gar nicht erst gelesen. Oh doch, versehentlich: „Der Kampf um die Köpfe und Herzen der Menschen über Einflussnahme, Desinformation und Propaganda spielt eine immer größere Rolle.“ Ach was. Man müsste denen den Gebrauch des [Komparativs](#) verbieten. Dann gingen ihnen irgendwann die Textbausteine aus.

Man will mir im Artikel weismachen, dass „[dystope](#) Weltbilder“, die von Selenskiij „Despoten“ verbreitet würden, daher rührten, dass „zu viele Menschen nicht mehr zwischen Fakten und Lügen unterscheiden“ könnten. Vielleicht sollte man auch [Relotius](#) dazu befragen.

Wenn man sich durch die Details des maßlos aufgeplusterten

Artikels wühlt, findet man das alles gar nicht mehr so skandalös. Natürlich haben die Herren magische Fähigkeiten und „hacken“ sich überall rein. Machte ich eine Präsentation, die den Verkauf meiner Dienstleitungen ankurbeln soll, würde ich das auch tun und bluffen, bis es zu den Ohren rauskommt. (Ich kann mich erinnern, dass ich als „Computerexperte“ in irgendeiner Sendung vorführte, dass man mit dem DOS-Befehl für [telnet](#) unter Windows wahnsinnig geheimnisvolle Zeichen auf den Monitor zaubern konnte, was das Publikum schwer beeindruckte.)

Selbstverständlich können Profis Leute übertölpeln, und bei manchen afrikanischen Politikern dürfte das nicht allzu schwer sein, wenn das schon [in Deutschland](#) passiert. Stellt man man sich dann die Software vor, mit denen die vermutlich Mailen usw., kommen sogar mir lustige Ideen. Ich habe nur nicht das Geld, die richtigen Leute zu bestechen.

Wer Hanan und seinen Wahrheitskillern eine Weile zuhört, merkt schnell, dass echte Demokratie in ihrer Welt eine Illusion ist. Dass sie Wahlen für ein ohnehin oft abgekartetes Spiel halten, bei dem meist der trickreichere gewinnt. (Spiegel)

Ach, das ist *nicht* so? Was ist denn „echt“ an der Demokratie? Dass die herrschenden Klassen über genug Mittel verfügen, ihre Sicht der Dinge durch ihre Mietmäuler in den Medien zu verbreiten?

Die moderne Staatsgewalt ist nur ein Ausschuß, der die gemeinschaftlichen Geschäfte der ganzen Bourgeoisie verwaltet. ([Karl Marx](#))

Ich schrieb [2016](#): Die Krise des Kapitalismus wird zeigen, dass „[Demokratie](#)“, [wie sie der Mainstream versteht](#), eben nur eine Illusion ist. Die Mittelklassen appellieren an die da oben, sich doch bitte an die Regeln zu halten, die angeblich *common sense* seien (keine Zensur usw.). Die herrschende Klasse ist aber eine Charaktermaske – sie interessiert das nicht.

Journalisten vertreten ideologisch die Klasse, aus der sie

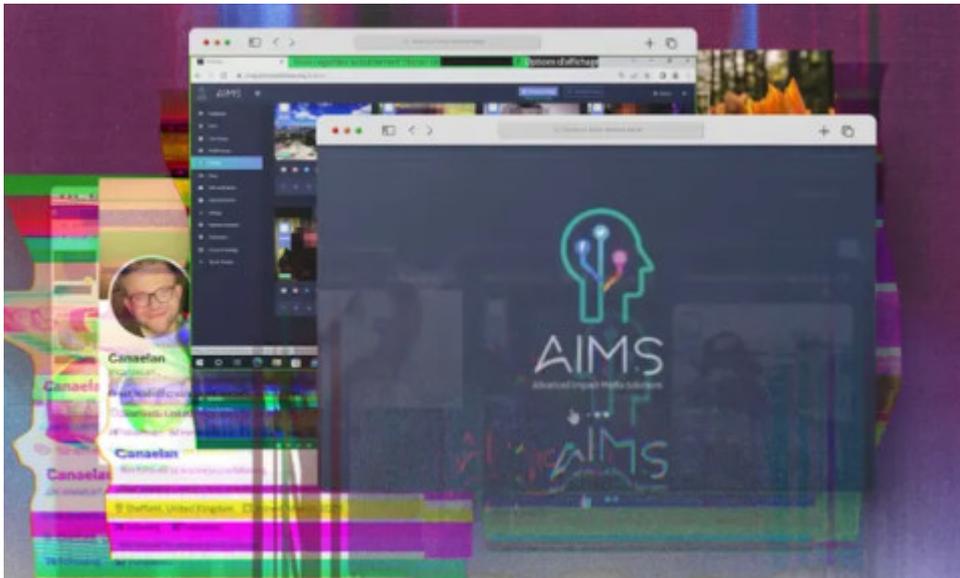
stammen, also mehrheitlich die Kleinbourgeoisie, und neigen dazu, die Interessen der herrschenden Klasse als die Interessen aller zu verkaufen. [Das sagt die Wissenschaft](#), und das will natürlich niemand hören.

Trotzdem agiert die Politik bislang zurückhaltend. (Spiegel)
Die Katze kommt aus dem Sack gekrochen. Es wäre kein deutscher Journalismus, wenn man sich mit den Fakten begnügen würde – man muss auch etwas fordern. Was im übrigen *mitnichten* eine journalistische Aufgabe ist. Die Europäische Union [richtete bereits 2015 eine Taskforce](#) ein, die mitunter täglich die Lügen aus Russland entkräftet. Tun die das – und wie? Kann man die Wirkung irgendwie messen? Und sieht man Ergebnisse, etwa, dass die Bevölkerung den Mainstream-Medien wieder mehr Glauben schenkt? Und täglich grüßen die „unabhängigen Faktenprüfer“, die das Gelogene, Hässliche und Schlechte wegzensieren. Elon Musk hat ihnen da einen Strich durch die Rechnung gemacht, was ich lustig finde.

Doch das goldene Zeitalter staatlicher Desinformation begann erst mit dem Internet. (...) Die Zeit der Desinformationskriege beginnt gerade erst. (Spiegel)

Und was sagt uns das jetzt alles? Journalisten heute verfügen nur noch selten über eine umfassende Allgemeinbildung, schreiben schlechtes Deutsch, „recherchieren“ aus dem Bauch heraus, wissen nicht, wie man sicher kommuniziert, wählen in den Anstalten mit großer Mehrheit die „Grünen“ und übernehmen deren Sprachsoterik – ist das eure Lösung? Gut, dass wir darüber geredet haben.

By the way: Diese Software [Advance Impact Media Solutions \(AIMS\)](#) brauche ich auch: „able to control the army of fake avatars“. Das wäre ja großartig, wenn ich [mehrere Avatare](#) auf einmal spielen könnte.



Tal Hanan said Aims bots were linked to SMS-verified phone numbers, and some even had credit cards. Composite: Guardian Design/Haaretz/TheMarker/Radio France

Sie sind mit dem Internet verbunden.



Das technische Problem, ein Insekt zu fangen, wurde in diesem Fall nicht zufriedenstellend gelöst.

Verehrtes Publikum: Ich verneige mich in Ehrfurcht vor den versierten Beiträgen, die meine technischen Probleme weitgehend lösten. Weitgehend.



1. VPN via [WireGuard](#) geht jetzt auf allen Betriebssystemen. Warum ist man ([zx2c4](#) und [Edge Security](#)) darauf nicht schon früher gekommen?

Keep in mind, though, that „support“ requests are much better suited for our [IRC channel](#). Har har. I love it. Old school.

Netzwerkstatus



Sie sind mit dem Internet verbunden.

Wenn Sie über einen eingeschränkten Datentarif verfügen, können Sie dieses Netzwerk als getaktete Verbindung festlegen oder andere Eigenschaften ändern.

WLAN (mossad_mobiles_m...
Der letzten 30 Tage

So gaaaaanz einfach war es unter Linux nicht. [Heiko Richter](#) hat es dankenswerterweise relativ volkstümlich erklärt.

In die Datei `/etc/wireguard/wg0.conf` fügen wir die Konfiguration ein, die wir von der Fritz!Box erhalten haben. Die Datei, die einem die Fritzbox vorher – bei der Einrichtung von WireGuard – geruhte zu überreichen, heisst `wg_config.conf` und funktioniert sowohl für Windows und Linux (`sudo gedit`

usw.)

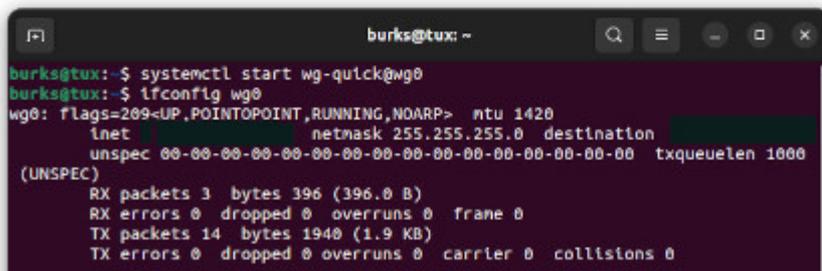
Sehr geehrte Damen und Herren Nerds aka Thomas Niedermeier !
Manuals wie [Ubuntu Desktop als WireGuard VPN Client konfigurieren](#) lese ich nur, wenn mich eine attraktive nackte Frau dazu auffordert. Ich bin mir auch nicht sicher, ob ich das Thema verstanden habe: VPN *ohne* Fritzbox o.ä.? Wer tut sich so etwas an?

```
# systemctl start wg-quick@wg0
```

Nach erfolgter Einwahl gibt es ein neues Interface mit entsprechenden Routen:

```
# ifconfig wg0
wg0: flags=209<UP,POINTOPOINT,RUNNING,NOARP> mtu 1420
    inet 10.10.10.201 netmask 255.255.255.255 destination 10.10.10.201
    unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 1000 (UNSPEC)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2 bytes 296 (296.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.10.10.0      0.0.0.0         255.255.254.0   U        0      0      0 wg0
```



```
burks@tux:~$ systemctl start wg-quick@wg0
burks@tux:~$ ifconfig wg0
wg0: flags=209<UP,POINTOPOINT,RUNNING,NOARP> mtu 1420
    inet          netmask 255.255.255.0 destination
    unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 1000
    (UNSPEC)
    RX packets 3 bytes 396 (396.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 14 bytes 1940 (1.9 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

So sieht das dann unter Jammy Jellyfish aus.

Auch [Detailprobleme](#) (Wie permanent einschalten? Wie ausschalten? Ist es überhaupt an?) kriegte ich nach einiger Zeit hingefummelt.

[x] Problem gelöst.

2. Mit WireGuard kann ich mich auch von nah und fern mit meiner Fritzbox verbinden. Wer hätte gedacht, dass das so einfach funktioniert! Was geschieht aber im [Oktober](#)?

Bei der Ausreise vom Flughafen Ben Gurion aus kann es zur Einbehaltung von elektronischen Geräten, insbesondere Laptops, durch die israelischen Sicherheitsbehörden kommen. In diesen

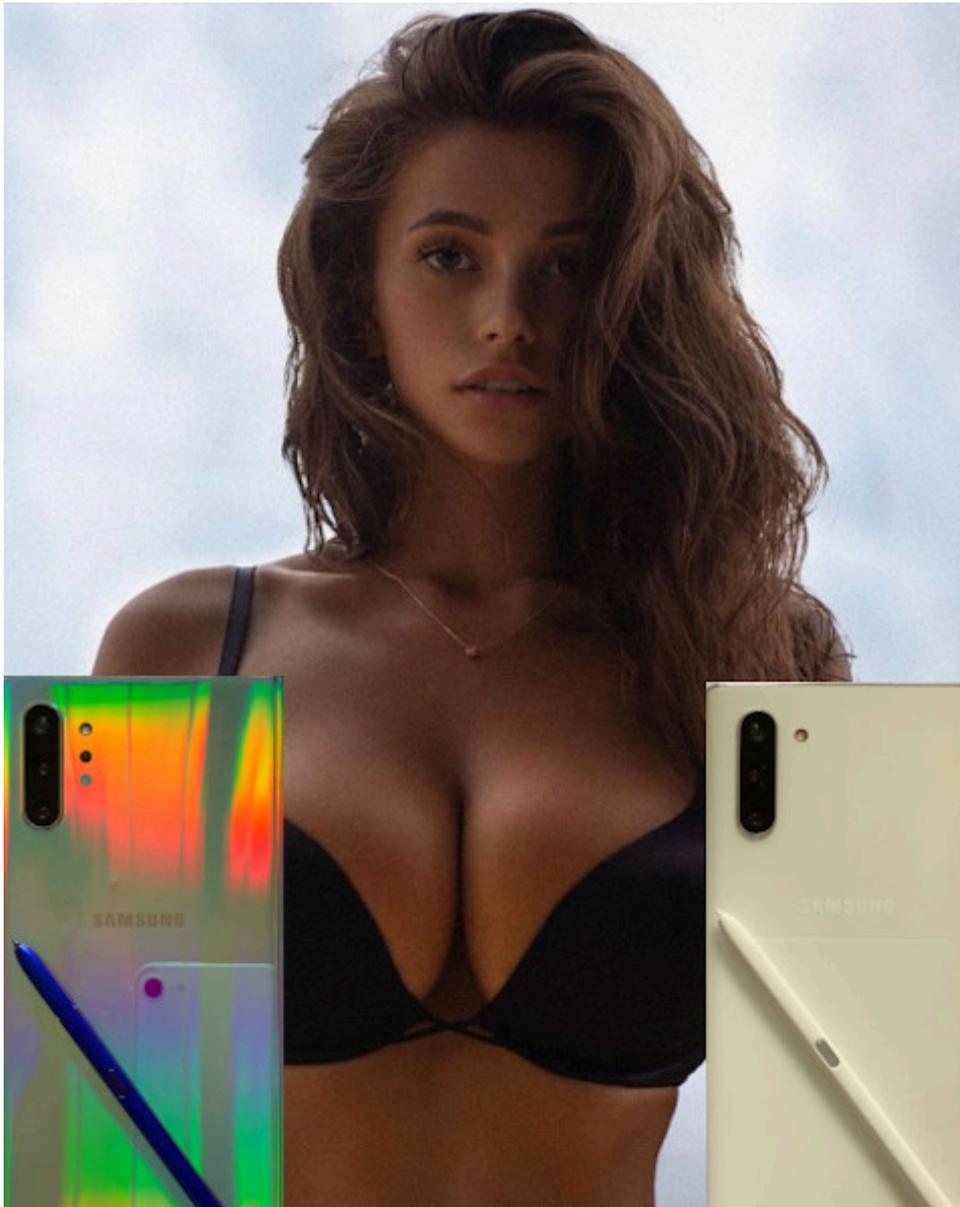
Fällen werden die Computer eingehend untersucht und dann nach ein bis drei Tagen an den Aufenthaltsort des Reisenden nachgesandt.

Hurra! Endlich eine „Online-Durchsuchung“! Das will ich sehen. Aber mein fettes Linux-Laptop nehme ich sowieso nicht mit.. Und wenn sie meine Veracrypt-Container nicht aufkriegen, behalten sie den Rechner? Da entwickle ich [sportlichen Ehrgeiz](#)... ~~ich hätte gar nichts zu verbergen.~~



Das technische Problem, sich zu entfesseln, wurde hier nur halbherzig gelöst. (Credits: [Schockwellenreiter](#))

Unter clientsidigen verdecktmaßnahmigen Cybersicheren an ihren Endgeräten



Eine Userin und ihre Endgeräte (Symbolbild)

[Netzpolitik.org](https://www.netzpolitik.org) hat die feuchten Träume des Ministeriums für Wahrheit der üblichen Verdächtigen veröffentlicht.

Ein hohes Datenschutzniveau, ein hohes Maß an Cybersicherheit,

einschließlich einer durchgängigen und sicheren Ende-zu-Ende-Verschlüsselung in der elektronischen Kommunikation sind für die Bundesregierung unerlässlich.

Dieses [Neusprech bedeutet](#):...will das Innenministerium am umstrittenen „[Client-Side-Scanning](#)“ festhalten. Der Einsatz dieser Technologie würde dazu führen, dass E-Mails, Messenger-Dienste und weitere Kommunikationsplattformen anlasslos und massenhaft überwacht werden. Beim Client-Side-Scanning werden Inhalte auf den Geräten der Nutzer vor dem Versand von Nachrichten durchsucht und somit eine spätere Ende-zu-Ende-Verschlüsselung unterlaufen.

Denglisch, Neusprech und irgendetwas mit cyber? Wait a minute. Da kann nur Bullshit-Bingo herauskommen, auch bei den Berichterstatern. Es geht um eine „Verfahrensweise, bei der versendete oder empfangene Dateien lokal auf dem Endgerät einer Person (...) durchsucht werden, bevor diese weiter verschickt beziehungsweise verarbeitet werden. Höre ich da die [Online-Durchsuchung](#) trapsen?

Ich kenne meine „Endgeräte“ (Anfangsgeräte besitze ich hingegen nicht.) Ich sitze zum Beispiel gerade vor einem. Das möchten „die“ durchsuchen, bevor ich darauf/davon/damit eine verschlüsselte E-Mail absende? Darf ich vorsichtig nach der Methode fragen, wie das gehen soll? Nein? Quod erat demonstrandum. Auch netzpolitik.org fragt nicht nach, wie schon bei der ominösen „[Online-Durchsuchung](#)“, wie „Client-Side-Scanning implementiert wird“.

Die streiten sich alle wieder um die Kleider eines nackten Kaisers. Wir lassen stattdessen Jörg Ziecke [zu Wort kommen](#), den ehemaligen Chef des BKA. Der erklärte 2007, wie das geht mit dem Onlinedurchsuchen:

Die Online-Durchsuchung ist einerseits der heimliche Zugriff auf die Festplatte, auf der anderen Seite ist es der heimliche Zugriff durch Quellen-TKÜ. Dieses Programm, was wir da

entwickeln, muss ein Unikat sein, darf keine Schadsoftware sein, darf sich nicht selbst verbreiten können und muss unter der Kontrolle dessen stehen, der es tatsächlich einbringt, wobei die Frage des Einbringens die spannendste Frage für alle überhaupt ist. Ich kann Ihnen hier öffentlich nicht beantworten, wie wir da konkret vorgehen würden. Sie können sich die abstrakten Möglichkeiten vorstellen, mit dem man über einen Trojaner, über eine Mail oder über eine Internetseite jemanden aufsucht. Wenn man ihnen erzählt hat, was für eine tolle Website das ist oder eine Seite mit ihren Familienangehörigen, die bei einem Unfall verletzt worden sind, sodass sie dann tatsächlich die Seite anklicken. Die Geschichten sind so vielfältig, dass es kaum jemanden gibt, der nicht auf irgendeine Form dieser Geschichte hereinfällt. Oder aber wir gehen den Weg über verdeckte Maßnahmen.

Wisst ihr Bescheid.



Ich habe kein Personal wie netzpolitik.org und würde mich daher mit einem Zehntel zufriedengeben.

Ein Teller bunten Quatsch



Was gibt es so?

- Noch mehr [Vereinsmeierei](#). Also noch mehr Schriftführer, Kassenwarte und Beisitzer, Ämter, um die sich Leute bewerben, die sonst nichts auf die Reihe kriegen. Braucht dieses Land nicht.
- Nein. Ich [kann den Quatsch](#) nicht mehr hören. Dann doch lieber irgendeinen russischen [Propagandakanal](#).
- ~~Warum bekommt die Ukraine keine Atomwaffen vom putinfreien Westen? Selenskij würde doch bestimmt vernünftig damit umgehen!~~

~~– Manche Leute sind so dumm, dass es sogar verschwendete Zeit wäre, versuchte man, deren gar nicht vorhandenen Argumente zu widerlegen. #deutschersatzbau~~

dpa • factchecking

Olaf Scholz war kein Mitglied der RAF

10/12/2021, 12:42 PM (CET)

Wer hätte [das gedacht](#)! Gut, dass es Faktenchecker gibt! Die kriegen wirklich alles raus.

– Die Briten [spielen mit dem Feuer](#). Doch halt! [die Russen haben das schon gemerkt](#): „Laut BBC würden die ukrainischen Truppen nur drei dieser Kettenkampffahrzeuge erhalten. Wie britische Militärexperten bemerken, gibt es im Prinzip gar nicht sehr viele M270 im britischen Arsenal, die an Kiew geliefert werden könnten.“

– Nein, ich bin auf jeden Fall *für* die [Chatkontrolle](#). Das funktioniert wie bei der „Online-Durchsuchung“: Wenn man fragt, wie das denn technisch umgesetzt werden soll, erntet man betretendes Schweigen. (Chat – was war das noch mal? [IRC](#)? [Signal](#)? Oder auf Suaheli in Second Life?) Vielleicht lernen dann einige Leute, wie man Kontrollen umgeht.



Erdbeer- und Rhabarbermarmelade – man gönnt sich ja sonst nichts.

They Regret the Error

Der [Chaos Computer Club](#) hat heute auf einer Pressekonferenz mehrere Statements des Vereins widerrufen. 14 Jahre nach dem Tod des Hackers „[Tron](#)“ sei es unter anderem an der Zeit, die vom CCC auch öffentlich geäußerten Verschwörungstheorien, [Tron sei „ermordet“ worden](#), zu kritisieren. Der damalige Pressesprecher [Andy Müller-Maguhn](#) habe sein Gesicht nicht verlieren wollen und deshalb den Unsinn zum Tode Trons nie zurückgenommen. CCC-Pressesprecherin Constanze Kurz sagte angesichts der anwesenden internationalen Presse in englischer Sprache: „We regret the error.“ Der CCC sein eben ein Verein, zu dem „quite a number of conspiracy theory enthusiasts“ gehöre.

Der Journalist Burkhard Schröder, so [Constanze Kurz](#), habe 1998 [ein Buch geschrieben](#) und angesichts der Faktenlage suggeriert,

dass Tron den Freitod gewählt habe. Schröder sei seit damals immer wieder von CCC-Mitgliedern wüst beschimpft und verleumdet worden. Der CCC distanzieren sich mittlerweile von [Andreas Bogk](#), der sich dabei besonders unrühmlich hervorgetan habe. Auch sei Schröder jetzt nicht mehr, wie [der CCC noch 2008 offiziell verlautbart habe](#), „Persona non grata“.

„Wir können aber nicht ausschließen“, so Kurz, dass Journalisten, die sich kritisch über den CCC äußerten, „in Zukunft wieder gemobbt werden“. Zum Glück werde das aber nur auf sehr wenige Journalisten beschränkt sein, da die Presse ohnehin alles unkritisch wiedergebe, was der CCC behaupte. Viele Journalisten hätten so wenig Ahnung von technischen Themen – wie etwa von der so genannten ‚Online-Durchsuchung‘ - , dass sie „jeden Quatsch“ veröffentlichten, „wenn wir das publizieren“, sagte Kurz. Unter dem Gelächter der anwesenden Pressevertreter fügte sie hinzu: „Auch wenn Sie das nicht glauben: Der Chaos Computer Club ist nicht unfehlbar. Auch wir können irren.“

They regret the error

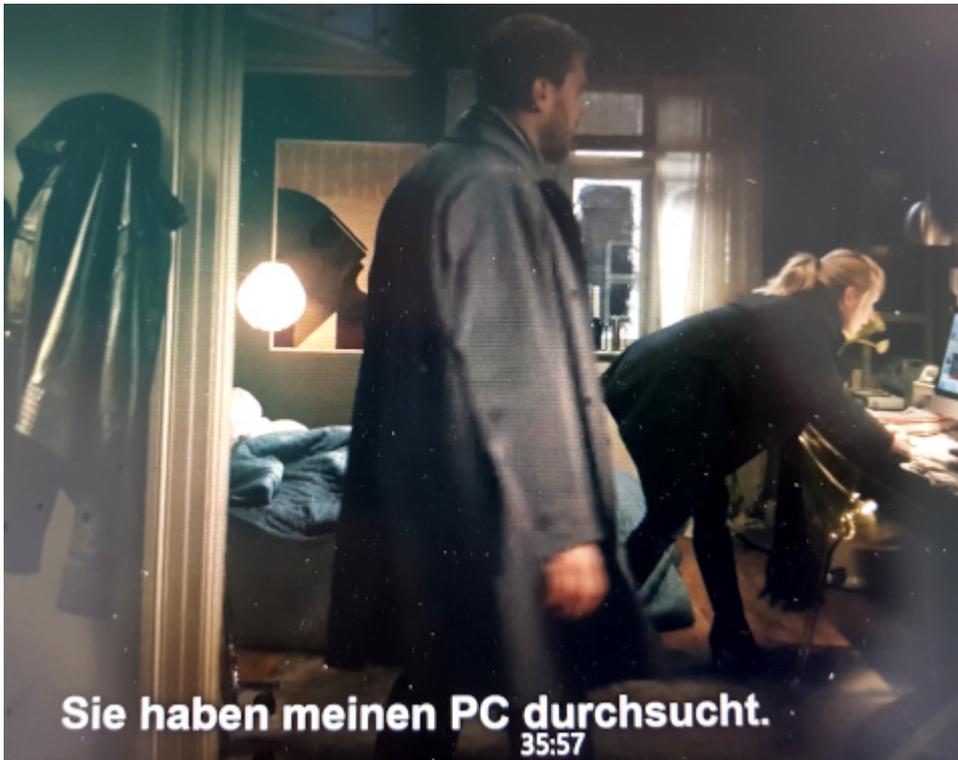
Der [Chaos Computer Club](#) hat heute auf einer Pressekonferenz mehrere Statements des Vereins widerrufen. 23 Jahre nach dem Tod des Hackers „Tron“ sei es unter anderem an der Zeit, die vom CCC auch öffentlich geäußerten Verschwörungstheorien, Tron [sei „ermordet“ worden](#), zu kritisieren. Der damalige Pressesprecher [Andy Müller-Maguhn](#) habe sein Gesicht nicht verlieren wollen und deshalb den Unsinn zum Tode Trons nie zurückgenommen. CCC-Pressesprecherin Constanze Kurz sagte angesichts der anwesenden internationalen Presse in englischer Sprache: „We regret the error.“ Der CCC sein eben ein Verein, zu dem „quite a number of conspiracy theory enthusiasts“

gehöre.

Der Journalist Burkhard Schröder, so [Constanze Kurz](#), habe 1998 [ein Buch geschrieben](#) und angesichts der Faktenlage suggeriert, dass Tron den Freitod gewählt habe. Schröder sei seit damals immer wieder von CCC-Mitgliedern wüst beschimpft und verleumdet worden. Der CCC distanzieren sich mittlerweile von [Andreas Bogk](#), der sich dabei besonders unrühmlich hervorgetan habe. Auch sei Schröder jetzt nicht mehr, wie [der CCC noch 2008 offiziell verlautbart habe](#), „Persona non grata“.

„Wir können aber nicht ausschließen“, so Kurz, dass Journalisten, die sich kritisch über den CCC äußerten, „in Zukunft wieder gemobbt werden“. Zum Glück werde das aber nur auf sehr wenige Journalisten beschränkt sein, da die Presse ohnehin alles unkritisch wiedergebe, was der CCC behaupte. Viele Journalisten hätten so wenig Ahnung von technischen Themen – wie etwa von der so genannten ‚Online-Durchsuchung‘ - , dass sie „jeden Quatsch“ veröffentlichten, „wenn wir das publizieren“, sagte Kurz. Unter dem Gelächter der anwesenden Pressevertreter fügte sie hinzu: „Auch wenn Sie das nicht glauben: Der Chaos Computer Club ist nicht unfehlbar. Auch wir können irren.“

Sie sind schon drin



Screenshot aus [Borgen](#), Staffel

1

Was soll man da machen? Vielleicht hätte eine ~~Cyber~~[Online-Durchsuchung](#) geholfen? Dann hätte niemand etwas bemerkt...(Vorsicht! Ironie!)

Merke: Man muss den größten Stuss nur oft und lange genug wiederholen, bis ihn alle für wahr halten.

**Nichtschwimmer im
extremistischen Auffangbecken**