Penny

Staatstrojaner

Die Späh-Software fürs behördliche Schnüffeln

digitalcourage

KURZ&MÜNDIG

KOSTENFREI

Art d'Ameublement

Band 27

Impressum

1. Auflage 09-24, Art d'Ameublement, cc-by 4.0, ISBN 978-3934636-65-1

Autorin: Penny, 🔗at-all.org | **Redaktion:** Aiga Kornemann, 🔗aigiko.de

Layout: Isabel Wienold, 🔗iwi-design.de

Bildlizenzen: S. 2-3: john mcsporran on pxhere cc by 2.0; S.14-15: Peggy und Marco Lachmann-Anke on Pixabay; S. 12-13 Peggy on Pixabay
Alle weiteren Bilder: 🔗iwi-design.de, Isabel Wienold cc by 4.0

Den einen gilt unerkanntes staatliches Hacking als die effektivste Möglichkeit zur Bekämpfung von Terrorismus, andere sehen darin eine Verletzung von Grund- und Menschenrechten. Wir widmen uns hier grundsätzlichen Fragen zum Staatstrojaner: Was genau ist damit gemeint? Wie funktioniert er? Wer darf ihn benutzen? Wofür und wie häufig wird er eingesetzt? Damit anschließend alle für sich die Frage beantworten können: Nutzen oder Schaden – Was überwiegt?

Quellen und weiterführender Lesestoff sind über diesen QR-Code auf der Webseite 🔗digitalcourage.de/kurz-und-muendig-quellen zu finden.

Unsichtbare Übergriffe

Der Staatstrojaner ist eine Schadsoftware, die auf Geräte aufgespielt wird und unbemerkt Daten an Behörden überträgt. Sie heißt „Trojaner“, weil sie wie ein trojanisches Pferd in Mobiltelefone oder Computer eindringt.

Trojanersoftware gibt es nicht nur vom Staat. Solche Schadsoftware wird von Cyberkriminellen benutzt, um sich unbefugten Zugang zu sensiblen Daten zu verschaffen, diese missbräuchlich zu verwenden oder digitale Systeme zu beschädigen.

Wenn der Staat solche Software für Ermittlungszwecke nutzt, wird sie „Staatstrojaner“ genannt. Damit sammeln Behörden Informationen, vielleicht auch mal gegen Sie und andere, mit denen Sie in Kontakt sind oder waren.

Kurze Reflektion

Denken Sie mal an alles, was Sie so im digitalen Raum machen. Welche Seiten Sie im Internet aufsuchen. Welche Fragen Sie beschäftigen. Welche Personen Ihnen im Kopf herumschwirren. Mit wem Sie chatten oder mailen. Denken Sie an heimliche Vorlieben. Gesundheitliche Probleme. Peinliche Begebenheiten. Notlügen. Ängste. Geheimnisse.

Ist es okay, wenn all das an Dritte gelangt, ohne dass Sie es wissen?

Der Sprung aufs Endgerät

Um an höchst private Daten zu gelangen, spielt eine ermittelnde Behörde die Schadsoftware aufs Endgerät von Verdächtigten (oder auch Dritten) – auf einen Laptop, ein Smartphone, theoretisch auch auf „smarte Geräte“ wie Alexa[1] oder ein vernetztes Haushaltsgerät. Dafür werden „Exploits“ genutzt, das sind Möglichkeiten, über Sicherheitsschwachstellen in installierten Programmen und Apps in ein Gerät einzudringen.

Auch deshalb ist es so wichtig, dass Sie nicht vergessen, Ihre Software immer wieder auf den neuesten Stand zu bringen!

Das Aufspielen passiert zunehmend „zero-click“ – das heißt, ohne, dass die Besitzer.innen des Endgeräts einen Link anklicken müssten, der ihnen vielleicht schon komisch vorkommt[2]. Der Staatstrojaner wird also heimlich aus der Ferne aufgespielt, oder unauffällig dann, wenn etwa die Polizei (oder der Zoll bei der Gepäckkontrolle) ein Gerät physisch in die Hand bekommt.

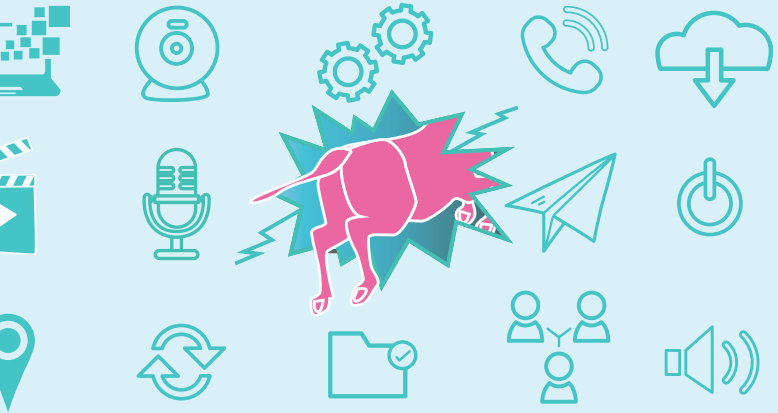
Die Software muss aufs Betriebssystem zugeschnitten sein, aber Staatstrojaner gibt es mittlerweile für ziemlich viele Betriebssysteme[3].

1, 2, 3 siehe digitalcourage.de/kurz-und-muendig-quellen

4, 5 siehe digitalcourage.de/kurz-und-muendig-quellen

Was können Staatstrojaner?

- Dateien durchsuchen und kopieren: Fotos, Videos, Musik, Chats etc.
- Adressbuch einsehen
- Chats mitlesen, bevor sie verschlüsselt werden (also auch Nachrichten, die jemand über verschlüsselte Kanäle wie Signal schickt)
- eMails lesen, auch verschlüsselte (für unverschlüsselte eMails braucht es nicht einmal einen Trojaner)
- Telefonate, auch übers Internet (Videokonferenzen), mithören und mit ansehen
- Trojaner können nahezu alles, was auch Sie mit Ihrem Gerät tun können – ferngesteuert.



6, 7 siehe digitalcourage.de/kurz-und-muendig-quellen

Im Einsatz: Gross und Klein

Um den Einsatz so mächtiger Software rechtlich zu regulieren, hat der Staat sich ein seltsames Konstrukt überlegt: Den „großen Trojaner“ und den „kleinen Trojaner“. Das sind allerdings nicht wirklich zwei Trojaner – der Unterschied besteht nur auf rechtlicher Ebene:

Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) „klein“

- Liest laufende Kommunikation mit, auch verschlüsselte Chats, Emails, etc.
- Hört laufende Gespräche mit
- seit 2021 zusätzlich als „Quellen-TKÜ Plus“[8]: Nachrichtendienste durchsuchen über laufende Kommunikation hinaus auch ab dem Zeitpunkt der Bewilligung gespeicherte Kommunikation

Erlaubt für Bundeskriminalamt (BKA), Bundespolizei, Landespolizeien (die meisten Polizeiaufgabengesetze wurden dafür schon angepasst, beispielsweise in Nordrhein-Westfalen, Bayern, Baden-Württemberg)[9] sowie die 19 Nachrichtendienste, Generalbundesanwaltschaft und Zoll.

8, 9 siehe 🔗digitalcourage.de/kurz-und-muendig-quellen

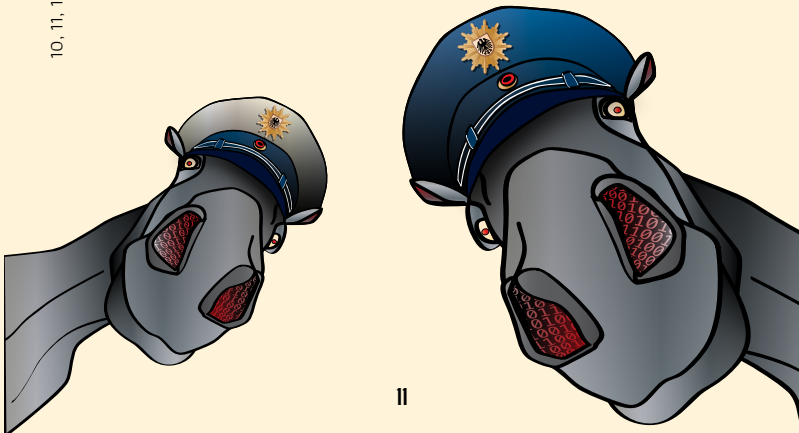
Online-Durchsuchung „groß“

- Darf alles, was der kleine Trojaner darf
- Durchsucht alle Dateien, Kontakte und Programme im Endgerät[10]

Erlaubt ist das dem BKA bei internationalem Terrorismus. Bundespolizei und Landespolizeien (hier nach Änderung ihrer Aufgabengesetze, bereits geschehen unter anderen in Bayern, Hessen, Rheinland-Pfalz), Bundesnachrichtendienst (BND) bei Ausländern im Ausland, Generalbundesanwalt und Zoll. Noch nicht erlaubt ist es dem Verfassungsschutz und Militärischen Abschirmdienst (MAD).[12]

Die Bundespolizei[11] und zum Beispiel die Landespolizei in Bayern darf auch präventiv hacken, das heißt, wenn jemand nichts Strafbares getan hat, sich aber möglicherweise irgendwann in der Zukunft strafbar machen könnte.

10, 11, 12 siehe 🔗digitalcourage.de/kurz-und-muendig-quellen



Staatstrojaner oder Grundrechte?

§ Der Staat darf nicht auf meine Geräte zugreifen. Das Grundrecht dazu heißt: „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“ (kurz: IT-Grundrecht).

§ Das Recht auf Privatsphäre, abzuleiten aus Artikel 1 und 2 im Grundgesetz, ist zu wahren.

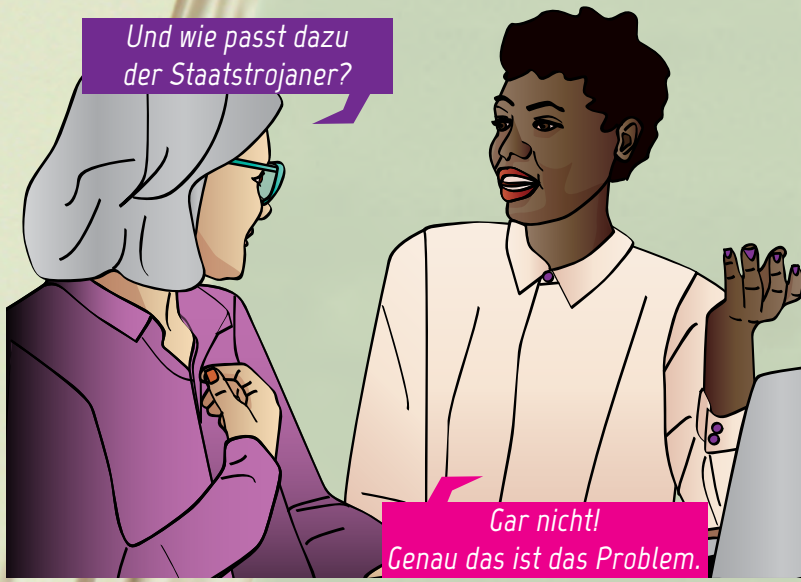
Auch das noch ... Die Forderung nach informationstechnischer Überwachung wird oft mit Terrorismus und Kinderpornografie begründet. In der Praxis werden Staatstrojaner primär für andere Ermittlungen eingesetzt.

Stellen Sie sich vor, Faschisten kommen an die Macht. Gibt es etwas in Ihrem Leben, das Personen mit faschistischer Gesinnung sauer aufstößt? Was meinen Sie, um welche „Straftaten“ die Liste erweitert würde?

§ Wer darf an meine Daten? Das regelt mein „Recht auf informationelle Selbstbestimmung“. Ich entscheide, welche Daten ich freigebe und wofür.

§ Das Recht auf Brief-, Post- und Fernmeldegeheimnis (Artikel 10 Grundgesetz)

§ Das Recht auf Unverletzlichkeit der Wohnung (Artikel 13 Grundgesetz), in der beispielsweise ein Computer steht.



Ein Sicherheitsdialog

Das mit den Grundrechten ist ja schön und gut, aber es gibt eben keine Alternative, um verschlüsselte Kommunikation auszulesen!

Gut so! Vielen ist eben nicht egal, ob sie überwacht werden. Nachdem dank Edward Snowden rauskam, wie viel Behörden überwachen, haben sie immer mehr Apps benutzt, die Ende-zu-Ende verschlüsseln.

Unter diesen vielen sind aber auch gefährliche Leute …

Das stimmt. Es kann aber nicht sein, dass die Sicherheit von Millionen Endgeräten gefährdet wird, um einer vergleichsweise winzigen Gruppe nachzustellen.

Das ist natürlich unverhältnismäßig. Aber wie denn sonst?

Es gibt alternative Ermittlungsmethoden, zum Beispiel Beschlagnahmung mit forensischer Analyse. Das ist auch sicherer in Prozessen – denn eigentlich ist das per Trojaner erlangte Material nicht rechtssicher, weil technisch nicht festgestellt werden kann, ob eventuell etwas von außen auf das Gerät nachgeladen wurde![13]

13 siehe 🔗digitalcourage.de/kurz-und-muendig-quellen

Wir leben eben in unsicheren Zeiten, mit Terrorismus und Allem, da braucht man doch Behörden mit ausreichenden Befugnissen!

Das Sicherheitsargument wird gern benutzt, um demokratische Freiheiten abzubauen. Dabei geht die Kriminalität kontinuierlich zurück[14] – es wird uns also nur vorgegaukelt, dass alles immer unsicherer werde.

Aber Terroristen sind real!

In der Realität ist der Staatstrojaner aber vor allem gegen Drogendelikte im Einsatz.[15] Da stimmt doch was nicht!

14, 15 siehe 🔗digitalcourage.de/kurz-und-muendig-quellen

Tatsächlich wurde das Grundgesetz in einer sehr unsicheren Zeit geschrieben. Mord- und Totschlag waren an der Tagesordnung, die Schwarzmärkte blühten. Und trotzdem schrieben die Väter und Mütter den Begriff „Freiheit“ 36 mal ins Grundgesetz. Das Wort „Sicherheit“ steht dort nur sechs mal.

Bei welchen Straftaten dürfen Staatstrojaner eingesetzt werden?

Unter anderem bei

- ✓ Kriegsverbrechen
- ✓ Mord
- ✓ Verbreiten kinderpornografischer Inhalte
- ✓ Landesverrat
- ✓ Bildung krimineller Vereinigungen
- ✓ Geldfälschung
- ✓ Verstöße gegen BTM- und Cannabisgesetz
- ✓ Verleitung zur missbräuchlichen Asylantragstellung
- ✓ Gewerbsmäßige Hehlerei
- ✓ Einschleusen von Ausländern
- ✓ Computerbetrug

Der Fall Letzte Generation

2022/23 wurden Umweltaktivisti der Letzten Generation durch die Bayrische Polizei abgehört – auf gleich 13 verschiedenen Telefonanschlüssen, darunter das Pressehandy der Bewegung. Der Tatvorwurf: Vielleicht hätten sie eine kriminelle Vereinigung (§129) gebildet. Bisher streiten Gerichte noch darüber, ob die Straßenblockaden der Letzten Generation überhaupt strafrechtlich relevant sind[16].

Der Fall Pegasus

Auch das BKA besitzt diesen Trojaner. Doch während in Deutschland noch kontrovers diskutiert wird, zeigen andere Beispiele in Europa, wie Regierungen Staatstrojaner einsetzen, wenn die Zivilgesellschaft nicht genau hinguckt:

In Ungarn ließ Orbans Regierung Handys von kritischen Medienschaffenden mit „Pegasus“ überwachen. In Spanien wurden Journalist.innen im Umfeld der katalonischen Unabhängigkeitsbewegung mit dem Trojaner attackiert. Und in Griechenland ging es gegen Presse, die Finanzskandale enthüllte. Das alles, obwohl journalistische Arbeit EU-weit per Gesetz besonders geschützt ist.

16 siehe 🔗digitalcourage.de/kurz-und-muendig-quellen

Woran sich deutsche Behörden halten müssen[17]

Strafverfolgungsbehörden nach StPO §100

- Eine richterliche Anordnung (die fast nie verweigert wird)
- Die Erlaubnis gilt immer für einen Monat.
- Danach darf immer für einen Monat verlängert werden – bis zu sechs Monaten.
- Ein Oberlandesgericht kann auch eine Verlängerung darüber hinaus erlauben.
- Innerhalb von sechs Monaten nach der Maßnahme müssen Betroffene informiert werden.
- Ein Gericht kann diese Benachrichtigung auch verzögern und auch beschließen, niemals Bescheid zu geben – wenn die Voraussetzungen dafür „auch in Zukunft nicht eintreten werden“[18].

Kann also sein, dass ich überwacht werde oder wurde, und mir hat einfach keiner Bescheid gesagt – unheimlich.

Ergo können Sie sich auch nicht gerichtlich dagegen wehren. Ob das noch rechtsstaatlich ist?

17, 18 siehe digitalcourage.de/kurz-und-muendig-quellen

Nachrichtendienste nach Zustimmung der G10:

- Braucht eine Genehmigung durch die „G10-Kommission“ – die trifft sich mindestens einmal im Monat.
- Wird kontrolliert durchs „Parlamentarische Kontrollgremium (PKGr)“ – maximal alle sechs Monate
- Das wiederum berichtet dem Bundestag einmal im Jahr davon.
- Ob die gesammelten Daten noch gebraucht werden, soll maximal alle sechs Monate geprüft werden – wenn nicht mehr gebraucht, dann löschen.
- Die Daten dürfen zur Verhinderung, Aufklärung, Verfolgung von Straftaten und zum Vorbereiten und Durchführen eines Verfahrens weitergeleitet werden.
- Betroffene müssen nach Abschluss der Maßnahme informiert werden.
- Aber auch hier kann die G10-Kommission entscheiden, das nicht zu tun, wenn ihrer Einschätzung nach der „Zweck“ der Beobachtung dadurch gefährdet werden könnte oder das „Wohl des Bundes oder eines Landes“ absehbar ist.
- Sie kann auch entscheiden, wenn das nach fünf Jahren noch der Fall ist und wahrscheinlich in Zukunft so bleibt, den Betroffenen niemals etwas zu sagen.

Wie oft werden Staatstrojaner eingesetzt?

Zunehmend.[19] Doch die Zahlenlage ist dünn. Die neusten Zahlen aus dem Jahr 2022 (Stand 2024):

- Quellen TKÜ = 49 mal (vor allem für Drogendelikte)
- Online-Durchsuchung = 4 mal[20]
- Verfassungsschutz = ???

Zahlen aus dem Jahr 2022 gibt es für die Geheimdienste noch nicht. Zwar wird die Anzahl solcher Maßnahmen durchs „Parlamentarische Kontrollgremium“ bekanntgegeben – aber immer erst drei Jahre später.

19, 20 siehe digitalcourage.de/kurz-und-muendig-quellen

Transparenz dient immer auch dazu, dass die Zivilgesellschaft der Regierung auf die Finger gucken und gegebenenfalls korrigierend wirken kann. Das wird erschwert, wenn Zahlen erst Jahre später veröffentlicht werden, weil man dann erst Jahre später die Stimme dagegen erheben kann. Und dann ist’s fürs Gericht vielleicht „nicht mehr aktuell“ genug.

Mit welcher Software?

Niemand sagt gern, welche Software benutzt wird[21]. Trotzdem sind einige Programme bekannt[22]:

RCIS – Remote Communication Interception Software. Deutsche Eigenmarke, hat aber Jahre gedauert mit der Entwicklung. Gibt es für Laptops (RCIS 1.0) und Smartphones (RCIS 2.0), Android und iOS.

Pegasus – eine Software der israelischen NSO Group, wurde vom BKA eingekauft und anscheinend auch bereits genutzt.[23] Kam in den Medien groß raus, weil Regierungsbehörden sie in vielen Ländern, auch in der EU, gegen Menschenrechtsinitiativen, Opposition und Journalist.innen eingesetzt haben.

Finspy von FinFisher – einer britisch-deutschen Firma. Gelangte zu unfreiwilligem Ruhm, weil sie ihre Software an autoritäre Staaten verkaufte, worauf sie nach Klagen Insolvenz anmeldete.

R2D2, auch bekannt als Ozapftis oder Bayerntrojaner von DigiTask. Eine Software, die durch den CCC analysiert und für unsicher und verfassungswidrig befunden wurde. Seitdem fürs erste ad acta gelegt.

21, 22, 23 siehe digitalcourage.de/kurz-und-muendig-quellen

Zusammengefasst:

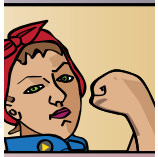
- Der Staat hält Einfallstore für Hacker offen und Geräte seiner Bürgerschaft unsicher, damit er diese Schwachstellen selbst nutzen kann, obwohl er eigentlich gesetzlich verpflichtet ist, sie zu schließen.
- Der Staatstrojaner verletzt alle möglichen Rechte, zum Beispiel das „IT-Grundrecht“, das besagt, dass Geräte „vertraulich“ bleiben sollen.
- Dass der Staatstrojaner gebraucht werde, wird mit der Gefahr von Terrorismus und dem Schutz des Kindeswohls begründet; in der Praxis wird er für Drogendelikte und auch gegen politisch Aktive eingesetzt.
- Immer werden auch Daten von Unschuldigen mitgesammelt.
- Durch all das kann der sogenannte „Chilling Effect“ einsetzen: Man sagt lieber nicht, was man denkt, aus Angst, überwacht zu werden. Das ist Gift für offene Gesellschaften.
- Die vom Staatstrojaner genutzten Sicherheitslücken können auch für kriminelle Zwecke missbraucht werden.
- Die Gesetze sind so gestaltet, dass Betroffenen oft nicht mitgeteilt wird, dass sie überwacht wurden – damit entfällt auch deren Möglichkeit, sich rechtlich dagegen zu wehren.
- Die Anzahl der durchgeführten Überwachungen wird erst Jahre später veröffentlicht, daher bleibt der Umgang der Behörden mit Staatstrojanern für die Öffentlichkeit intransparent.
- Bekannte Software, wie Pegasus und FinSpy, ist durch Menschenrechtsverletzungen sowie Export an Diktaturen berühmt geworden.

Der Staat sagt „Freiheit durch Sicherheit“ – deshalb Staatstrojaner.

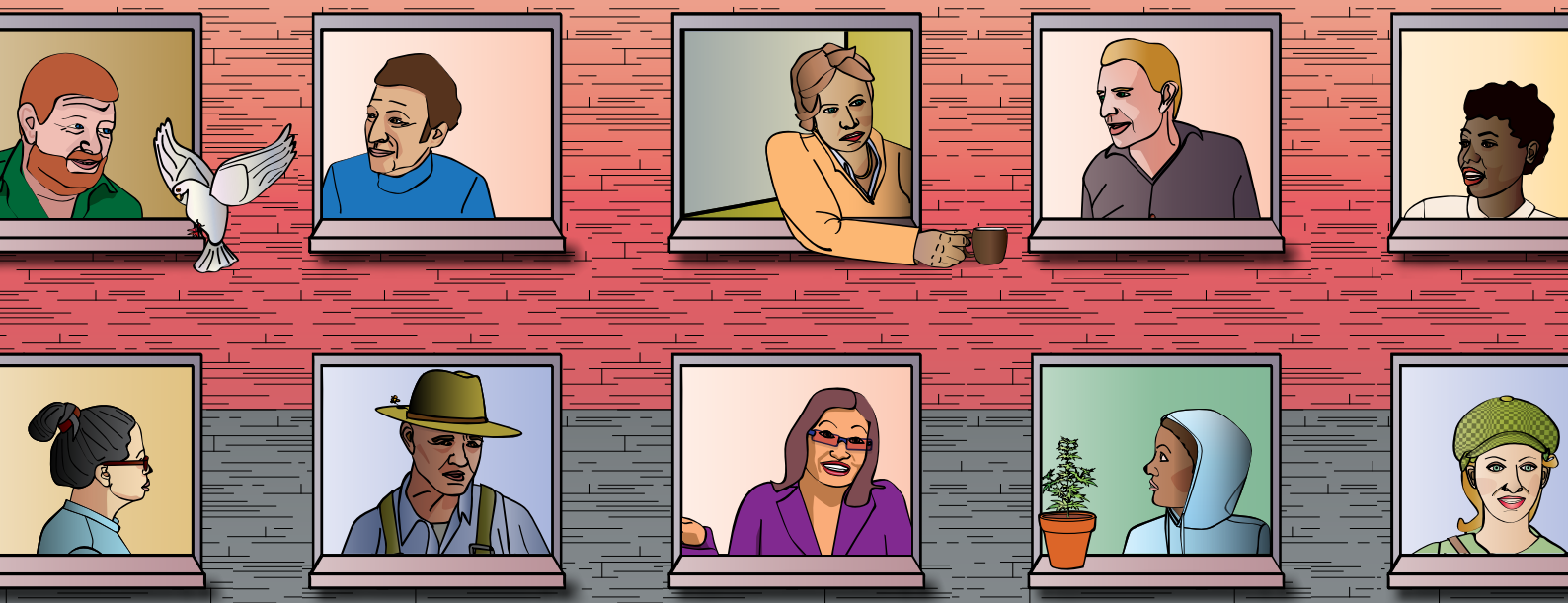
Wir sagen: Dieser Trojaner bringt „Unsicherheit und Unfreiheit“ für alle.

Und nun?

Wir finden: Niemand sollte mit Staatstrojanern überwacht werden! Deshalb hat die Grundrechteorganisation Digitalcourage 2018 eine Beschwerde beim Bundesverfassungsgericht eingelegt, die bis zum Redaktionsschluss im Juli 2024 noch nicht verhandelt war.



Was denken Sie darüber? Halten Sie den Staatstrojaner für ein nötiges Übel, oder einen zu großen Eingriff in unsere Grundrechte? Diskutieren Sie mit Ihren Freundinnen und Freunden, informieren Sie sich weiter und bleiben Sie auf dem Laufenden! Denn eines ist klar: Wir sollten solche grundsätzlichen Entscheidungen nicht unhinterfragt allein der Politik überlassen.



Über die Autorin

Penny ist großer Fan von einer Gesellschaft ohne Überwachung. Mit dem @all-Kollektiv unterrichtet sie Jugendliche und Erwachsene zu Digitalisierung und Datenschutz. Im Kollektiv Skills for Utopia organisiert sie Workshops für Aktivist.innen, zum Beispiel zu Digitaler Selbstverteidigung. Nebenbei arbeitet sie für den Lehrstuhl für Recht und Ethik in der digitalen Gesellschaft an der European New School for Digital Studies.

Kontakt: heypenny@riseup.net

Weitere kurz&mündig-Ausgaben passend zum Thema:

Versammlungsfreiheit – Gelebte Demokratie [Band 11]

Nichts zu verbergen? – Ein gefährlicher Irrglaube [Band 12]

Datenschutzbeschwerden richtig einreichen [Band 19]

Die kurz&mündig-Reihe wird herausgegeben von:

digitalcourage e.V. engagiert sich seit 1987 für Grundrechte, Datenschutz und eine lebenswerte Welt im digitalen Zeitalter. Seit 2000 verleihen wir die BigBrotherAwards. Digitalcourage ist gemeinnützig, finanziert sich durch Spenden und lebt von viel freiwilliger Arbeit.

Mehr zu unserer Arbeit finden Sie auf digitalcourage.de und bigbrotherawards.de

In der kurz&mündig-Reihe sind bisher erschienen:

01 **Digitale Mündigkeit**
02 **Datenschutzrechte in Schulen durchsetzen**
03 **Faire Websites**
04 **Leitlinien für digitale Bildung in Schulen**
05 **Uploadfilter**
06 **Stalking, Hass, Kontrolle**
07 **Homeoffice**
08 **Digitale Bildungsangebote selbst erstellen**
09 **Digitale Angiffe im Büro**
10 **Digitale Sicherheit für Frauenhäuser**
11 **Versammlungsfreiheit**
12 **Nichts zu verbergen?**
13 **Apps selbst prüfen und bewerten**
14 **Überwachung in China**
15 **Solidarität im Netz**
16 **Fediverse. So geht Social Media**
17 **Einfach. Linux.**
18 **Smart Toys und Kinder-Tracking-Apps**
19 **Datenschutzbeschwerden richtig einreichen**
20 **Datenschutz in Kirchengemeinden**
21 **Videoüberwachung an Schulen**
22 **Digitale Selbstverteidigung für Mädchen***
23 **Workshops clever planen**
24 **Bodyshaming**
25 **Umgang mit Fotos**
26 **Künstliche Intelligenz**
27 **Staatstrojaner**

Dieses KURZ&MÜNDIG-Minibuch ist auch als komfortables interaktives PDF erhältlich. Es kostet nur 5,00 Euro und ist wie alle KURZ&MÜNDIG-Ausgaben (auch als Printversion) erhältlich unter: digitalcourage.de/kum

Das Bundesverfassungsgericht wird sich mit etlichen Beschwerden befassen, die unter anderen Digitalcourage gegen den Einsatz von Staatstrojanern eingereicht hat. Das Thema wird also immer wieder für Schlagzeilen sorgen. Informieren Sie sich jetzt schon!

Digitalcourage e.V.
Marktstraße 18 | 33602 Bielefeld
mail@digitalcourage.de
digitalcourage.de
T: +49 521 1639 1639

9 783934 636651 >
5,00 Euro
5,00 CHF
ISBN 978-3934636-65-1

digitalcourage
k&m 27 Staatstrojaner