Noch mehr Staatstrojaner:

Verfassungsschutz soll hacken dürfen

von Constanze

[3]

Dem Verfassungsschutz soll die Erlaubnis zum Hacken erteilt werden, wenn es nach dem Willen des Heimatministeriums geht. Wie ein Staatssekretär von Minister Horst Seehofer in einer Rede bekräftigte, soll der Geheimdienst per Gesetz zu „Online-Durchsuchungen“ ermächtigt werden.

Wer dachte, die enorme Ausweitung der Befugnisse [4] bei Staatstrojanern in der letzten Legislaturperiode sei schon das Ende der Fahnenstange, der wird nun von den neuen Plänen der schwarz-schwarz-roten Koalition zu noch mehr staatlichem Hacken überrascht. Unter der Ägide von Heimatminister Horst Seehofer (CSU) soll nun auch Geheimdiensten die Nutzung von Staatstrojanern erlaubt werden. Diesmal geht es nicht nur um die kastrierte Variante der Schadsoftware, die heimlich auf Geräten eingeschleust wird und dann ausschließlich laufende Gespräche mithören darf, sondern um die sogenannte „Online-Durchsuchung“. Dabei handelt es sich um eine Spionagesoftware, die den gesamten Inhalt von Festplatten von Computern, Smartphones und anderen informationstechnischen Geräten durchsuchen und ausleiten kann.

Anfang des Jahres war mit dem Hessentrojaner [5] bereits ein Ausbau geheimdienstlicher Befugnisse beim staatlichen Hacken diskutiert worden. Der CDU-Landesinnenminister Peter Beuth [6] hatte einen Entwurf für eine Reform des Hessischen Verfassungsschutzgesetzes (HSVG) vorgelegt, der beide Varianten des Staatstrojaners für den Landesgeheimdienst vorsah, also „Online-Durchsuchung“ und „Quellen-Telekommunikationsüberwachung“ (Quellen-TKÜ). Die schwarz-grüne Landesregierung verständigte sich nach einer mehrstündigen Sachverständigenanhörung dann aber darauf, dem Landesamt für Verfassungsschutz (LfV Hessen [7]) doch keine staatliche Erlaubnis zum Hacken zu erteilen, allerdings der hessischen Polizei den Staatstrojanereinsatz zu erlauben.

Nun geht der Streit um geheimdienstliche Trojaner in die nächste Runde, diesmal auf Bundesebene. Über die neuen Pläne zur Staatstrojaner-Ausweitung sprach der Staatssekretär im Heimatministerium, Hans-Georg Engelke, am 26. Juni auf dem „Kongress für wehrhafte Demokratie“ in Berlin. Nach einer Anfrage nach dem Informationsfreiheitsgesetz [8] haben wir sein Redemanuskript erhalten und veröffentlichen es wie immer in Gänze [9] (pdf). Das Ministerium weist allerdings darauf hin, dass Engelke in seinem mündlichen Vortrag von dem schriftlichen Manuskript abgewichen sein könnte.

► Neue Befugnisse für den Verfassungsschutz

Inhaltlich beschäftigt sich Engelke mit den aktuellen „Gefährdungslagen“, die es zu bewältigen gilt. In seinem Redemanuskript nennt der Staatssekretär drei konkrete Gefahrenbereiche: terroristische „Gefährder“, Cyber-Angriffe sowie „Police Outing“. Für Letzteres verweist er auf einen umstrittenen Protest in der Stadt Hitzacker [10] vor dem privaten Wohnhaus eines Polizisten, der in den Medien mit dem Begriff „Police Outing“ verbunden wurde.

Auf die genannten „Gefährdungslagen“ will Engelke Antworten geben und leitet im Laufe seiner Rede aus diesen Gefahren eine Politik von „Null Toleranz gegenüber Gewalt und Kriminalität“ ab. Er nennt dabei als ein Beispiel geplante neue Befugnisse für den aktuell wieder in einen Skandal verwickelten [11] Verfassungsschutz. Wörtlich steht im Redemanuskript folgende Passage:

> Wenn „Online-Durchsuchungen“ mittlerweile sogar zur Strafverfolgung zulässig sind, dann sollten sie eigentlich erst Recht zur Gefahrenabwehr zulässig sein und als typisch nachrichtendienstliche – verdeckte – Methode dabei auch für die nachrichtendienstliche Gefahrenforschung. Wir werden daher für einen breiten politischen Konsens werben, den Harmonisierungsimpuls der IMK [Innenministerkonferenz] gemäß dem Koalitionsvertrag mit wirksamen Befugnissen auch in einer Novelle des Bundesverfassungsschutzgesetzes aufzugreifen.

Die Logik von Engelke kann jedoch nicht überzeugen. Er bezieht sich auf die Ausweitung der Staatstrojanererlaubnis in der Strafprozessordnung, die nun eine Änderung des Bundesverfassungsschutzgesetzes (BVerfSchG [12]) quasi wie selbstverständlich nach sich ziehen würde. Ein Strafverfahren ist allerdings dadurch gekennzeichnet, dass verschiedene Beteiligte das Vorgehen vorab und auch im Nachhinein überprüfen können: Richter, Betroffene, Strafverteidiger. Nicht so in den Geheimbehörden: Im geheimdienstlichen Handeln bliebe das heikle staatliche Hacken weitgehend der Kontrolle entzogen.

Auch der Verweis Engelkes auf den Koalitionsvertrag ähnelt einem missglückten Taschenspielertrick: Darin findet sich zwar auf Seite 127 das Vorhaben, das Bundesverfassungsschutzgesetz „auf Grundlage eines einheitlichen Rechtsrahmens der Innenministerkonferenz novellieren“ zu wollen und bei der Datenerhebung und Datenspeicherung „die Befugnisse des Verfassungsschutzes des Bundes und der Länder [zu] vereinheitlichen“, aber geheimdienstliche Trojaner gehören gerade nicht zum Standardinstrument der Landesgeheimdienste in Deutschland – im Gegenteil.

Engelke nutzt übrigens den Begriff der „Gefahrenforschung“, die offenbar auf den Festplatten von Betroffenen stattfinden soll. Die Vorstellung scheint zu sein, mit der heimlichen Spionagesoftware in die auf Computern oder Smartphones gespeicherten Daten und damit in etwaige gefährliche Gedanken der Betroffenen hineinblicken zu wollen.

Eigenentwicklung oder kommerzielle Anbieter?

Die Bundesregierung gibt schon im polizeilichen Bereich kaum Informationen dazu heraus, mit welchen technischen Mitteln und mit kommerziellen Partnern der Staatstrojanereinsatz vollzogen wird. Angesichts dessen ist für die chronisch schlecht kontrollierten Geheimen schon jetzt absehbar, dass die Öffentlichkeit, der Bundestag und auch die Kontrollgremien keine Einsicht in deren Praxis bekommen werden. Unter dem Siegel der Geheimhaltung und mit der üblichen Begründung, dass die nationale Sicherheit bedroht sei, wenn Informationen zum Vorgehen der Staatshacker bekannt würden, werden die Behörden in weitgehender Eigenregie arbeiten können.

Erst durch unsere Veröffentlichung vormals geheimgehaltener Unterlagen ist heute öffentlich bekannt, dass die BKA-Eigenentwicklung des Staatstrojaners (Behördendeutsch: Remote Communication Interception Software (RCIS 2.0)) insgesamt 5,77 Millionen Euro [13] verschlungen hat. Ob auch die Geheimdienste Mitnutzer der Software werden, ist allerdings zweifelhaft. Es steht zu befürchten, dass weitere hohe Summen dafür aufgewendet werden, die Planungen des Ministeriums in die technische Realität umzusetzen. Wer die Funktionalität der geheimdienstlichen Software – ob als Eigenentwicklung entworfen oder bei Drittanbietern eingekauft – überblicken und vor allem überprüfen soll, erwähnt Engelke in seiner Rede nicht.

Wir dürfen gespannt sein, ob sich der Koalitionspartner SPD nun dem Wunsch des Heimatministeriums nach geheimdienstlichen Trojanern anschließen wird. Vielleicht können die Sozialdemokraten die Christenunion an das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme erinnern.

Constanze

"**Hessische Polizei wird militärisch aufgerüstet**" >> **weiter** **[14]**.

_____

Constanze Kurz ist promovierte Informatikerin, Autorin und Herausgeberin mehrerer Bücher, ihre Kolumne „Aus dem Maschinenraum“ erscheint im Feuilleton der FAZ. Sie ist Aktivistin und ehrenamtlich Sprecherin des Chaos Computer Clubs. Sie forschte an der Humboldt-Universität zu Berlin am Lehrstuhl „Informatik in Bildung und Gesellschaft“ und war Sachverständige der Enquête-Kommission „Internet und digitale Gesellschaft“ des Bundestags. Sie erhielt den Werner-Holtfort-Preis für bürger- und menschenrechtliches [15] Engagement, den Toleranz-Preis für Zivilcourage und die Theodor-Heuss-Medaille für vorbildliches [16] demokratisches Verhalten.

Kontakt: constanze(at)netzpolitik.org (OpenPGP), Telefon: +49-30-92105-9846.

netzpolitik.org ist eine Plattform für digitale Freiheitsrechte. Die Betreiber und deren Autoren thematisieren die wichtigen Fragestellungen rund um Internet, Gesellschaft und Politik und zeigen Wege auf, wie man sich auch selbst mithilfe des Netzes für digitale Freiheiten und Offenheit engagieren kann. Mit netzpolitik.org beschreiben sie, wie die Politik das Internet durch Regulation verändert. Und wie das Netz Politik, Öffentlichkeiten und alles andere verändert. Sie verstehen sich als journalistisches Angebot, sind jedoch nicht neutral. Ihr Haltung ist: Engagement für digitale Freiheitsrechte und ihre politische Umsetzung.

[3]

► **Quelle:** Erstveröffentlicht am 01. August 2018 auf NETZPOLITIK.org >>Artikel [17]. **Lizenz:** Die von NETZPOLITIK verfassten Inhalte stehen, soweit nicht anders vermerkt, unter der Lizenz Creative Commons (Namensnennung - Nicht-kommerziell - Weitergabe unter gleichen Bedingungen 4.0 International (CC BY-NC-SA 4.0 [18]). Die Bilder im Artikel sind nicht Bestandteil des Originalartikels und wurden von KN-ADMIN Helmut Schnug eingefügt. Für sie gelten ggf. andere Lizenzen, s.u..

► Bild- und Grafikquellen:

1. Horst Seehofer. Das Foto von Horst Seehofer entstand am 17.07.2012 im Bayerischen Landtag. **Foto:** © Michael Lucan [19], München. (Pixeldost Bildagentur, Inh. Michael Lucan). **Quelle:** Wikimedia Commons [20]. Diese Datei ist

unter der Creative-Commons [21]-Lizenz „Namensnennung – Weitergabe unter gleichen Bedingungen 3.0 nicht portiert“ [22] lizenziert. (Lizenz: CC-BY-SA 3.0).

ACHTUNG: Dieses Werk steht unter einer (oder mehreren) freien Lizenz(en) [23], die mit den Nutzungsbedingungen von Youtube, Facebook, Twitter und anderen sozialen Netzwerken nicht vereinbar sind. Eine Verwendung auf Facebook oder in anderen "sozialen" Medien wie Youtube, Twitter etc. ist daher nicht zulässig, sondern wäre eine Schutzrechtsberühmung [24] und Urheberrechtsverletzung [25]. Bitte vermeiden Sie im eigenen Interesse das Teilen/Sharen, sowie Dritten das Teilen/Sharen des Werkes bei Facebook oder in anderen "sozialen" Medien wie Youtube, Twitter etc. anzubieten.

2. HIER WACHT DER BUNDESTROJANER. **Grafik**: Wilfried Kahrs (WiKa).

Regelmäßig wurde auf den möglichen Einsatz von staatlicher Schadsoftware, eine Art Trojanisches Pferd, verwiesen. Umgangssprachlich werden für diese Software deshalb auch die Begriffe „Polizeitrojaner“, „staatlicher Trojaner“, „Staatstrojaner“ und der in Deutschland am weitesten verbreitete Begriff „Bundestrojaner“ verwendet. In der Sicherheitsbranche werden solche Arten von (Schad)Software auch als Govware [26] (von englisch *government* ‚Regierung‘ bzw. *to govern* ‚lenken‘, ‚steuern‘, ‚beeinflussen‘) bezeichnet.

Offiziell wird die Software als *Remote Forensic Software (Fernforensische [27] Software)* (RFS) bezeichnet. Nach Angaben von Beamten des Bundeskriminalamtes soll es sich dabei um einen spezifischen Keylogger [28] handeln. Dieser soll entweder voll elektronisch oder aber von Observanten persönlich in der Wohnung direkt am Rechner des Tatverdächtigen installiert werden. (Text: Wikipedia).

3. Staatshacker: Im geheimdienstlichen Handeln bliebe das heikle staatliche Hacken weitgehend der Kontrolle entzogen. **Foto:** geralt / Gerd Altmann, Freiburg. **Quelle**: Pixabay [29]. Alle bereitgestellten Bilder und Videos auf Pixabay sind gemeinfrei (Public Domain) entsprechend der Verzichtserklärung Creative Commons CC0 [30]. Das Bild unterliegt damit keinem Kopierrecht und kann - verändert oder unverändert - kostenlos für kommerzielle und nicht kommerzielle Anwendungen in digitaler oder gedruckter Form ohne Bildnachweis oder Quellenangabe verwendet werden. >> Bild [31].

4 . Staatstrojaner (Behördendeutsch: Remote Communication Interception Software (RCIS 2.0). **Foto:** geralt / Gerd Altmann, Freiburg. **Quelle**: Pixabay [29]. Alle bereitgestellten Bilder und Videos auf Pixabay sind gemeinfrei (Public Domain) entsprechend der Verzichtserklärung Creative Commons CC0 [30]. Das Bild unterliegt damit keinem Kopierrecht und kann - verändert oder unverändert - kostenlos für kommerzielle und nicht kommerzielle Anwendungen in digitaler oder gedruckter Form ohne Bildnachweis oder Quellenangabe verwendet werden. >> Bild [32].

5. Spionagesoftware kann den gesamten Inhalt von Festplatten von Computern, Smartphones und anderen informationstechnischen Geräten durchsuchen und ausleiten. **Bild:** Zaadii / Sadi Yigit, Ludwigsburg. **Quelle**: Pixabay [29]. Alle bereitgestellten Bilder und Videos auf Pixabay sind gemeinfrei (Public Domain) entsprechend der Verzichtserklärung Creative Commons CC0 [30]. Das Bild unterliegt damit keinem Kopierrecht und kann - verändert oder unverändert - kostenlos für kommerzielle und nicht kommerzielle Anwendungen in digitaler oder gedruckter Form ohne Bildnachweis oder Quellenangabe verwendet werden. >> Bild [33].

[29]

Anhang	Größe
Koalitionsvertrag 2018 zwischen CDU, CSU und SPD - 179 Seiten - Ergebnis einer Zwangsheirat, Betrug am Wahlvolk [34]	2.8 MB

Quell-URL: https://kritisches-netzwerk.de/forum/noch-mehr-staatstrojaner-verfassungsschutz-soll-hacken-duerfen

Links
[1] https://kritisches-netzwerk.de/user/login?destination=comment/reply/7355%23comment-form
[2] https://kritisches-netzwerk.de/forum/noch-mehr-staatstrojaner-verfassungsschutz-soll-hacken-duerfen
[3] https://netzpolitik.org/
[4] https://netzpolitik.org/2017/staatstrojaner-bundestag-beschliesst-diese-woche-das-krasseste-ueberwachungsgesetz-der-legislaturperiode/
[5] https://netzpolitik.org/2017/schwarz-gruen-in-hessen-will-staatstrojaner-fuer-verfassungsschutz/
[6] https://de.wikipedia.org/wiki/Peter_Beuth_(Politiker)
[7] https://lfv.hessen.de/
[8] https://fragdenstaat.de/anfrage/redemanuskript-vom-26-juni-2018/
[9] https://cdn.netzpolitik.org/wp-upload/2018/07/engelke26.juni_.pdf
[10] http://taz.de/!5507937/
[11] https://www.sueddeutsche.de/politik/maassen-petry-afd-1.4076324
[12] http://www.gesetze-im-internet.de/bverfschg/
[13] https://netzpolitik.org/2018/geheime-dokumente-das-bundeskriminalamt-kann-jetzt-drei-staatstrojaner-einsetzen/
[14] https://kritisches-netzwerk.de/forum/hessische-polizei-wird-militaerisch-aufgeruestet
[15] http://www.faz.net/aktuell/feuilleton/debatten/datenschutz-das-vergessene-grundrecht-12095331.html?printPagedArticle=true

[16] https://nowyouknow.eu/
[17] https://netzpolitik.org/2018/noch-mehr-staatstrojaner-verfassungsschutz-soll-hacken-duerfen/
[18] https://creativecommons.org/licenses/by-nc-sa/4.0/deed.de
[19] http://www.lucan.org/
[20] https://commons.wikimedia.org/wiki/File:2012-07-17_BYL_135.JPG?uselang=de
[21] https://en.wikipedia.org/wiki/de:Creative_Commons
[22] https://creativecommons.org/licenses/by-sa/3.0/deed.de
[23] https://commons.wikimedia.org/wiki/Commons:Licensing/de
[24] https://de.wikipedia.org/wiki/Schutzrechtsber%C3%BChmung
[25] https://de.wikipedia.org/wiki/Urheberrechtsverletzung
[26] https://de.wikipedia.org/wiki/Govware
[27] https://de.wikipedia.org/wiki/Forensik
[28] https://de.wikipedia.org/wiki/Keylogger
[29] https://pixabay.com/
[30] https://creativecommons.org/publicdomain/zero/1.0/deed.de
[31] https://pixabay.com/de/bin%C3%A4r-h%C3%A4nde-tastatur-tippen-2372130/
[32] https://pixabay.com/de/monster-blau-internet-angriff-426995/
[33] https://pixabay.com/de/virus-wurm-computer-trojaner-2019480/
[34] https://kritisches-netzwerk.de/sites/default/files/koalitionsvertrag_2018_zwischen_cdu_csu_und_spd_-_179_seiten_-_ergebnis_einer_zwangsheirat_betrug_am_wahlvolk_6.pdf
[35] https://kritisches-netzwerk.de/tags/big-data
[36] https://kritisches-netzwerk.de/tags/bka-trojaner
[37] https://kritisches-netzwerk.de/tags/bundesverfassungsschutz
[38] https://kritisches-netzwerk.de/tags/bundesverfassungsschutzgesetz
[39] https://kritisches-netzwerk.de/tags/bverfschg
[40] https://kritisches-netzwerk.de/tags/cyber-angriff
[41] https://kritisches-netzwerk.de/tags/datenerhebung
[42] https://kritisches-netzwerk.de/tags/datenkrake
[43] https://kritisches-netzwerk.de/tags/datenschutz
[44] https://kritisches-netzwerk.de/tags/datenspeicherung
[45] https://kritisches-netzwerk.de/tags/gefahrder
[46] https://kritisches-netzwerk.de/tags/gefahrenabwehr
[47] https://kritisches-netzwerk.de/tags/gefahrenforschung
[48] https://kritisches-netzwerk.de/tags/gefahrdungslage
[49] https://kritisches-netzwerk.de/tags/geheimdienst
[50] https://kritisches-netzwerk.de/tags/geheimdienstliche-trojaner
[51] https://kritisches-netzwerk.de/tags/govware
[52] https://kritisches-netzwerk.de/tags/hacken
[53] https://kritisches-netzwerk.de/tags/hackerbehorde
[54] https://kritisches-netzwerk.de/tags/hans-georg-engelke
[55] https://kritisches-netzwerk.de/tags/harmonisierungsimpuls
[56] https://kritisches-netzwerk.de/tags/heimatministerium
[57] https://kritisches-netzwerk.de/tags/hessendata
[58] https://kritisches-netzwerk.de/tags/hessen-data
[59] https://kritisches-netzwerk.de/tags/hessentrojaner
[60] https://kritisches-netzwerk.de/tags/horst-seehofer
[61] https://kritisches-netzwerk.de/tags/ifg
[62] https://kritisches-netzwerk.de/tags/ifg-bund
[63] https://kritisches-netzwerk.de/tags/informationsfreiheitsgesetz
[64] https://kritisches-netzwerk.de/tags/keylogger
[65] https://kritisches-netzwerk.de/tags/landesgeheimdienst
[66] https://kritisches-netzwerk.de/tags/lfv-hessen
[67] https://kritisches-netzwerk.de/tags/malware
[68] https://kritisches-netzwerk.de/tags/massenuberwachung
[69] https://kritisches-netzwerk.de/tags/nationale-sicherheit
[70] https://kritisches-netzwerk.de/tags/online-durchsuchungen
[71] https://kritisches-netzwerk.de/tags/peter-beuth
[72] https://kritisches-netzwerk.de/tags/police-outing
[73] https://kritisches-netzwerk.de/tags/quellen-tku-software
[74] https://kritisches-netzwerk.de/tags/rcis-20
[75] https://kritisches-netzwerk.de/tags/remote-communication-interception-software
[76] https://kritisches-netzwerk.de/tags/remote-forensics-software
[77] https://kritisches-netzwerk.de/tags/rfs
[78] https://kritisches-netzwerk.de/tags/schadprogramme
[79] https://kritisches-netzwerk.de/tags/schadsoftware
[80] https://kritisches-netzwerk.de/tags/spahsoftware
[81] https://kritisches-netzwerk.de/tags/spionagesoftware
[82] https://kritisches-netzwerk.de/tags/staatliches-hacken

[83] https://kritisches-netzwerk.de/tags/staatshacker
[84] https://kritisches-netzwerk.de/tags/staatstrojaner
[85] https://kritisches-netzwerk.de/tags/staatstrojanereinsatz
[86] https://kritisches-netzwerk.de/tags/strafverfolgung
[87] https://kritisches-netzwerk.de/tags/tasten-protokollierer
[88] https://kritisches-netzwerk.de/tags/telekommunikationsuberwachung
[89] https://kritisches-netzwerk.de/tags/tku
[90] https://kritisches-netzwerk.de/tags/uberwachung
[91] https://kritisches-netzwerk.de/tags/uberwachungssoftware
[92] https://kritisches-netzwerk.de/tags/uberwachungsstaat
[93] https://kritisches-netzwerk.de/tags/verfassungsschutz
[94] https://kritisches-netzwerk.de/tags/verfassungsschutzgesetz