Staatstrojaner

<<TableOfContents>>

Ein Staatstrojaner ist ein Spionage-Programm, welches heimlich auf dem Rechner des Betroffenen von den Sicherheitsbehörden installiert wird, um dessen Computeraktivitäten auszuspionieren.

= Geschichte =

Die Diskussion über Staatstrojaner begann mit der Novellierung des Verfassungsschutzgesetzes in [[NRW]], das Einbrüche in Rechner unter recht liberalen Voraussetzung erlaubte. Das Bundesverfassungsgericht verwarf diese großzügige Regelung mit [[http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html|Urteil vom 27.2.2008 (1 BvR 370/07, 1 BvR 595/07)]]. Das Urteil machte durch die Definition eines "Grundrecht[s] auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme" fast Rechtsgeschichte, doch erlaubte es gleich einige Verletzungen des frisch geschaffenen Grundrechts.

Damit konnte im Rahmen der Novellierung des BKA-Gesetzes 2008 (<<Rellink(/gc/bkag.pdf,RHZ-Artikel dazu)>>) das BKA in §20k die Befugnis zum Einbrechen in Rechner erhalten. Einige Ländergesetze haben diesen Schritt nachvollzogen. Sowohl [[BKA]] als auch [[Länder]] dürfen den Staatstrojaner nur zur Gefahrenabwehr -- also bei Unverdächtigen -- einsetzen, nicht aber im Strafverfahren -- also bei Personen, bei denen zumindest ein Anfangsverdacht besteht. Dies mag merkwürdig erscheinen, entspricht aber der eigentlichen Rechtskonstruktion.

Tatsächlich beriefen sich bis 2012 jedoch alle öffentlich bekannten Trojanereinsätze auf Eingriffsbefugnisse aus der LawfulInterception (d.h. Überwachung der Kommunikation des Rechners und nicht von Inhalten auf dem Rechner selbst). Das war natürlich Propaganda und flog auf vgl. unten beim [[#DigiTask-Skandal]].

Wie weit die Befugnis zur eigentlichen "Onlinedurchsuchung" nach §20k tatsächlich schon eingesetzt wurde oder wird ist vorläufig unklar. In der Logik der Geheimpolizei verweigert die Regierung in <<BtDS(17/6079)>> (2011) die Auskunft zur Frage, wie weit sie bereits eingesetzt wurde (vgl. auch [[http://www.golem.de/1106/84298.html|golem.de: "Regierung verweigert Informationen..."]]).

In einem <<Doclink(2012-bfdi-trojaner.pdf,BfDI-Bericht zum Digitask-Skandal)>> steht dazu:

{{{#!blockquote Tatsächlich habe das BKA dieses Modul [des Digitask-Trojaners, nämlich zur Onlinedurchschung nach §20k] niemals abgerufen [...] Für Maßnahmen der Onlinedurchsuchung setze das BKA ohnehin eine andere Software ein" (S. 12). }}}

Damit dürfte feststehen, dass das [[BKA]] sich auch im unbegrenzten Zugriff auf Privatrechner übt.

Zur Frage, wie der Staatstrojaner auf die Maschinen gelangt, formuliert der [[BfDI]]-Digitask-Bericht, das Betreten von Wohnungen zur Installation würde gegen Art. 13 Abs. 2 GG verstoßen, und er habe keine entsprechenden Fälle feststellen können. Auch die Methode, den Trojaner bei einer offenen Maßnahme heimlich aufzuspielen (so dokumentiert in [[http://ijure.org/wp/archives/727|Patrick Schladt: Einer der Trojaner des CCC...]]) hält der BfDI für unverträglich mit StPO und Grundgesetz.

Infolge der katastrophalen Evaluationsergebnisse für den Trojaner des BKA-Hauslieferanten Digitask beschließt das BKA, selbst einen "gesetzeskonformen" Trojaner zu entwickeln und richtet, im Groben nur dafür, ein "Kompetenzzentrum Informationstechniche Überwachung" ("CC ITÜ") ein.

Im Januar 2013 sickert ein <<Doclink(2012-bund-trojanersachstand.pdf,Bericht zum Sachstand)>> (vgl. auch [[https://netzpolitik.org/2013/geheimes-dokument-bundeskriminalamt-kauft-international-bekannten-staatstrojaner-finfisherfinspy-von-gamma/|netzpolitik.org dazu]]) in Sachen CC ITÜ durch, der frecherweise als VS-NfD eingestuft war. Aus ihm geht hervor, dass sich bis 10/2012 lediglich Beteiligungen aus Bayern, Hessen und vom Zollkriminalamt -- mithin also aus den schwärzesten Datenschutzhöllen der Republik -- an dem BKA-Projekt beteiligt hatten. Der Trojaner soll bis Ende 2014 fertig sein, die Eigenschaften dabei durch eine "Standardisierte Leistungsbeschreibung" beschrieben werden, wobei etwa das "Verschlüsselungsverfahren, der Schlüsselaustausch oder technische Maßnahmen zur Gewährleistung, dass ausschließlich laufende Kommunikation erfasst wird" (S. 3) spezifiziert sein sollen. Dieses Dokument ist, soweit bekannt, keinen unabhängigen und kompetenten Personen offiziell zugänglich.

Der Sachstandsbericht verkündet außerdem, das BKA habe "für den Fall eines erforderlichen Einsatzes ein kommerzielles Produkt der Firma Elaman/Gamma beschafft" (S. 4), als den FinFisher. Mehr zu diesem Hoflieferanten der Diktatoren dieser Welt unter [[Hersteller]] -- das BKA ist da in der allerbesten Gesellschaft.

2020 veröffentlichte das BMJ den [[https://www.heise.de/downloads/18/3/0/2/5/1/1/5/Uebersicht_TKUE_2019.pdf_jsessionid_BFFE11C37E1F166C1094DA87B3F7996D.2_cid393.pdf|Bericht zu Maßnahmen nach §100a StPO]] und behauptete, der Staatstrojaner sei 2019 satte 380 Mal zum Einsatz gekommen, was angesichts der Digitask-Erfahrungen extrem erschien, und schon deswegen unplausibel war, weil etwa das kleine Bremen Bremen 94 Mal Staatstrojaner beantragt haben und damit in 11 Fällen durchgekommen sein will, während sich das üblicherweise autoritäre Maßstäbe setzenden Bayern gerade mal 3 beantragte Versuche (und 3 Erfolge) berichtete.

Es stellte sich heraus ([[https://www.heise.de/news/Falsch-angekreuzt-Justiz-rudert-bei-Staatstrojaner-Statistik-zurueck-5019148.html|Heise online 2020-01-08]]):

{{{#!blockquote Die gemeldeten Fälle seien überprüft worden. Dabei habe sich herausgestellt, dass ein Dezernent "die Bögen offenbar missinterpretiert hat. Wir haben im Ergebnis keine Umsetzung." Auch in Mecklenburg-Vorpommern und Nordrhein-Westfalen teilten Staatsanwaltschaften mit, sie hätten tatsächlich keine solchen Überwachungen veranlasst. Die hessischen und sächsischen Justizressorts äußerten erhebliche Zweifel an den Zahlen und wollten eine Revision veranlassen. Aus dem Saarland hieß es, es handele sich um eine "fehlerhafte

statistische Erfassung". Die dortigen Zuständigen hatten zunächst 12 Anordnungen gemeldet, von denen 24 durchgeführt worden seien, was keinen Sinn ergibt. }}}

Die großen Erfolgszahlen wären auch insoweit bemerkenswert gewesen, als das BKA 2021 einräumte, es habe seinen für ca. 5 Millionen Euro entwickelten eigenen Staatstrojaner zwischen 2017 und 2020 nicht in einem einzigen Verfahren mit Erfolg einsetzen können ([[https://www.heise.de/news/BKA-hat-Bundestrojaner-seit-2017-kein-einziges-Mal-erfolgreich-eingesetzt-5062346.html|heise online dazu]]). Das ist bemerkenswert, weil das BKA Ermittlungskompetenzen eben in den Bereichen hat, mit denen die Menschenrechtsverletzung hauptsächlich begründet wurde, „Terrorismus“ und „organisiserte Kriminalität“ (was immer das dann auch sein mag).

Im August 2022 urteilt das fürs BKA zuständige VG Wiesbaden (6 K 924/21.WI), dass eine IFG-Auskunft zum finfisher-Trojaner viel zu stark geschwärzt war. Damit ist klar, dass im BKA-Etat 325.666 Euro für den Trojaner auftauchen (die Arbeitszeit, die mit dem Ding verspielt wurde, wird das wohl nicht dabei sein).

== Staatstrojaner zur Lawful Interception ("Quellen-TKÜ") ==

In der zweiten Hälfte der 2000er Jahre setzten verschiedene Polizeibehörden Staatstrojaner unter dem Vorwand der Überwachung der Telekommunikation ein. Ziel war wohl vor allem die proprietäre VoIP-Software Skype, was der Operation angesichts einer vermutlich authentischen [[http://cryptome.org/isp-spy/skype-spy.pdf|Anleitung von Skype für "Bedarfsträger"]] zusätzlichen Vorwands-Hautgout gibt.

Zur (propagandistisch interessanten) Frage der Abhörschnittstelle von Skype vgl. auch [[http://ijure.org/wp/archives/808|Ulf Buermeyer: Skype dürfte eine Abhörschnittstelle bieten]] sowie die Aussage des BfDI <<Doclink(2012-bfdi-trojaner.pdf,seinem Bericht zum Digitask-Skandal)>> 2012, Italien hätte mit Skype einen Vertrag zur LawfulInterception. Wie auch ein [[http://www.internet-law.de/2011/10/die-quellen-tku.html|Blogeintrag des Anwaltes Thomas Stadler]] erläutert, würde damit insbesondere jeder Angriff mit dem Ziel, Skype-Gespräche abzuhören, unverhältnismäßig. Dementsprechend leugnet auch die niedersächsische Regierung in [[http://www.landtag-niedersachsen.de/Drucksachen/Drucksachen_16_5000/4501-5000/16-4545.pdf|Landtagsdrucksache 16/4545]] (2012) die Fähigkeit von Skype selbst, eine Abhörschnittstelle bereitzustellen.

Die Anordnung der Maßnahmen erfolgt nach §100a/b StPO (vgl. LawfulInterception). Allerdings können diese Normen eigentlich lediglich Eingriffe in die Telekommunikationsfreiheit (Art. 10 Abs. 1 GG) rechtfertigen, nicht aber in die Integrität und Vertraulichkeit informationstechnischer Systeme, wie etwa der Richter Ulf Buermeyer in [[http://ijure.org/wp/archives/756|"Quellen-TKÜ – ein kleines Einmaleins"]] darlegt.

Da nicht zu erkennen ist, wie ein Trojaner auf einen Rechner gebracht werden und dort laufen kann, ohne Integrität und Vertraulichkeit es Gesamtsystems zu verletzen, hat die [[http://www.humanistische-union.de/aktuelles/aktuelles_detail/back/aktuelles/article/instrumente-zeigen-humanistische-union-fordert-stopp-der-onlineueberwachung-und-offenlegung-aller-

ue/|Humanistische Union im Oktober 2011 erklärt]], sämtliche Anordnungen und ihre Umsetzungen in der vom CCC bekannt gemachten Form einer "Quellen-TKÜ" rechtswidrig und strafbar seien.

= Zahlen =

Über die Trojaner-Einsätze nach StPO muss die Regierung jährlich berichten; Anfang der der 2020er Jahre sind das eignige Dutzend pro Jahr, die zu vielleicht 2/3 erfolgreich sind. Da inzwischen diverse Ländergesetze ihren Polizeien Trojanereinsatz mit anderen Rechtsgrundlagen erlauben, könnten die wahren Zahlen etwas höher liegen. Es ist allerdings wahrscheinlich, dass die Ländergesetze meist eher als Submissionsgeste gegenüber der Polizei erlassen wurden und der präventive Einsatz von Staatstrojanern sehr überschaubar ist.

- 2021: 55 Versuche, 33 erfolgreich; 35 (23 erfolgreich) waren „Quellen-TKÜ“, 20 (9 erfolgreich) „Online-Durchsuchung“ ([[https://www.bundesjustizamt.de/DE/ServiceGSB/Presse/Pressemitteilungen/2023/20230822.html?nn=39384|Erklärung des BMJ]])
- 2020: 50 Versuche, 22 erfolgreich. Besonders unterhaltsam: das Bundesamt für Justiz hat [[https://netzpolitik.org/2022/justizstatistik-2020-polizei-setzt-staatstrojaner-alle-zwei-wochen-ein/|die Auskunft völlig vermurkst]]
- 2019: 52 Versuche, 15 erfolgreich ([[https://netzpolitik.org/2021/justizstatistik-2019-polizei-nutzt-staatstrojaner-vor-allem-bei-erpressung-und-drogen/|Netzpolitik vom 18.2.2021]])

= DigiTask-Skandal =

In einer [[http://www.ccc.de/de/updates/2011/staatstrojaner|Pressemitteilung vom Oktober 2011]], berichtet der CCC, ihm sei der Binärcode eines Trojaners zugespielt wurde. Der CCC hat die Software analysiert und einerseits festgestellt, dass der Trojaner nicht nur Web-Browser und IM-Programme per Screenshot ausspäht und Code zum Zugriff auf das Rechner-Mikrofon enthält, sondern auch das Nachladen beliebigen weiteren Codes unterstützt. Dies alles war gegen jeglichen Zugriff praktisch nicht gesichert.

Der Trojaner sei von der Firma [[Hersteller#Digitask|Digitask]] gekauft worden. Hinweise auf fallspezifische Anpassungen ergaben sich nicht.

Das Bundesinnenministerium dementierte zunächst, Ausgangsort des Trojaners zu sein ([[http://www.faz.net/aktuell/politik/nach-enttarnung-des-staatstrojaners-innenministerium-trojaner-nicht-eingesetzt-11487583.html|FAZ-Bericht vom 9.10.2011]]).

Nach und nach gaben dann etliche Bundesländer den Einsatz des Trojaners durch ihre LKA zu, etwa [[Bayern]], [[Baden-Württemberg]], [[Niedersachsen]], [[Brandenburg]], [[Hessen]], [[Rheinland-Pfalz]], [[NRW]] und [[Schleswig-Holstein]] (vgl [[http://blog.fefe.de/?ts=b06d8be5|fefes Blog]]).

Eine [[http://www.presseportal.de/polizeipresse/pm/35235/2128673/pol-hb-nr-0418-informationen-zum-einsatz-einer-bundestrojaner-software/|Pressemitteilung der Polizei in Bremen (12.10.2011)]] räumt ein, der Trojaner sei 2007 in einem [[129a Verfahren]] verwendet haben.

[[http://www.heise.de/tp/blogs/8/150615|Peter Mühlbauer berichtet am 12.10.2012 auf telepolis]] weiter, der Digitask-Trojaner sei auch in [[Österreich]] und der [[Schweiz]] im Einsatz gewesen. Weiter gibt er an, deutsche Behörden hätten ihn in Vefahren gegen eine Online-Apotheke und gegen Betrug beim Online-Verkauf eingesetzt.

Im Februar 2012 hat der BfDI einen <<Doclink(2012-bfdi-trojaner.pdf,Bericht zum Digitask-Skandal)>> vorgelegt (vgl. [[http://linksunten.tachanka.org/de/node/54960|linksunten.indymedia.org von 2012]] zu dessen etwas obskurem Weg an die Öffentlichkeit), der leider aufgrund von Geheimhaltungsrechten des BKA stark unvollständig ist. Auch lag nicht einmal dem BfDI der Quellcode des Digitask-Trojaners vor, und da die Mehrzahl der Einbrüche im Auftrag von Länder-Staatsanwaltschaften nach StPO vorgenommen wurden, waren sie nicht Gegenstand der Untersuchung. Dennoch gibt der Bericht einige Einsichten, etwa:

(1) Das BKA hat 23 Einbrüche verübt, davon vier in Amtshilfe (für Hessen und Rheinland-Pfalz, in Verfahren wg. Drogen, Diebstahl und Raub). Von den BKA-eigenen Einbrüchen waren 11 und damit die Mehrheit gegen Menschen gerichtet, gegen die kein hinreichender Anfangsverdacht bestand ("zur Gefahrenabwehr"). Das Zollkriminalamt hat 16 Einbrüche vorgenommen, davon 12 für die Zollfahndungsämter. Von den ZKA-Einbrüchen fanden nur drei zur Gefahrenabwehr statt, die anderen nach StPO, und es ging bei allen um Skype. Die Bundespolizei hat nur einen Einbruch vornehmen lassen, und zwar vom Bayrischen Landeskriminalamt in einem Fall von "Menschenhandel" (§97 Abs. 2 Aufenthaltsgesetz).

(2) Für die Einbrüche ist eine BKA-Abteilung namens KI 25 zuständig, die die Bedarfsträger "berät". Über den Modus Operandi der Einbrüche will das BKA nichts berichtet wissen (wahrscheinlich ist ihnen die [[http://ijure.org/wp/archives/727|Amtshilfe des Zolls]] peinlich).

(3) Die strafrechtlichen Maßnahmen orientierten sich in der Tat an §100a/b StPO; es ging bei den Verfahren um §129 (wohl etwas konstruiert, sie waren hinter Phishern her), §129b (no surprises), §89a ("staatsgefährdende Gewalttat", der Gedanke an Anti-Bundeswehr-Aktionen liegt nicht fern) und §263 (Betrug) StGB sowie zwei Mal §29a BtMG (also Drogenkisten). Bei der Gefahrenabwehr (Befugnis nach §20l BKAG (Abhören), ''nicht'' §20k (Einbruch)) waren es "Hinweise auf Gefahrenlagen aus dem Phänomenbereich des internationalen Terrorismus". Die ZKA-Verfahren gingen um Schmuggel von Arzneimitteln, Zigaretten und anderen Drogen.

(4) Es wurden Tonaufzeichnungen von Gesprächen (nicht aber eigenständig vom Raum-Mikrofon) sowie Mitschnitte von Chats gespeichert. Screenshots hat der BfDI weder beim BKA noch beim ZKA gefunden.

(5) Zitat aus dem Bericht (es geht um ein Ermittlungsverfahren in einer BTM-Kiste des BKA):

{{{#!blockquote Anhand der von uns eingesehenen schriftlichen Aufzeichnungen der Gespräche fanden sich u.a. folgende Zusammenfassungen zu Gesprächen zwischen dem Beschuldigten und seiner Freundin in Südamerika:

- "kurzes erotisches Gespräch...", 20.11.09, 14:31:54
- "Gespräch übers Wetter und initime Angelegenheiten", 20.11.2009, 15:43:24

- "..Liebesbeteuerungen...", 4.12.2009, 15:46:31; weiterer Wortlaut: "...Danach Sexgespräch (Anm. Übers. Ab 15:52:20 bis 16:01:00 finden offensichtlich Selbstbefriedigungshandlungen statt)...", "...weiter privat über Liebe..."

Die Tondateien zu diesen Gesprächen lagen noch vor. Das BKA führte aus, die Staatsanwaltschaft habe verfügt, die Dateien nicht zu löschen. Begründet wurde dies damit, dass eine Teillöschung technisch nicht möglich gewesen sei. }}}

(6) Nur bei sieben der 12 Einbrüche im Auftrag der ZFÄ hat der Trojaner am Ende auch Daten geliefert. Bei keinem der drei Verfahren zur Gefahrenabwehr durch das [[ZKA]] hat der Trojaner Daten geliefert.

(7) Das Nachladen von Software durch die von staatlicher Seite aufgebrachte Malware war integraler Bestandteil der Einbrüche des BKA. Zitat:

{{{#!blockquote [Nach einer durch konventionelle TKÜ gelieferten Systemübersicht] wird [von Digi Task] eine Software ohne Aufzeichnungsfunktion geliefert. Diese hat nur die Nachladefunktion und eine Funktion zur Auflistung der Software des infizierten Rechners. Mit einem ebenfalls von Digi Task bezogenen Programm werden die IP-Adresse eines externen Proxy-Systems und ggf. die sogenannte U-Nummer [...] als Identifizierungsmerkmal in die Binärdatei eingefügt. [...] Anschließend wird diese erste Komponente der Überwachungssoftware auf den bzw. die Zielrechner aufgebracht. [...] Nach der Rückmeldung des Zielrechners mit seiner MAC-Adresse [..] prüft das BKA per Fernzugriff die Softwarekonfiguration des Zielrechners [...] Anschließend wird Software mit den eigentlichen Überwachungsfunktionen [...] in Form eines Updates nachgeladen. }}}

Das ZKA hingegen hat gleich einen Trojaner mit Vollüberwachung aufgebracht.

(8) Die Prüfung des BfDI war erstaunlich oberflächlich. Immerhin hat er sich die Mühe gemacht, die vom CCC angegebenen Schlüssel bzw. Kennungen in der BKA-Software zu identifizieren. Zur Möglichkeit der Aufzeichnung von Raumgesprächen sagt der BfDI nur:

{{{#!blockquote Ich habe die Funktionsweise der Quellen-TKÜ-Software mit Skype kurz getestet. Hinweise darauf, dass die Überwachungssoftware zur Überwachung von Raumgesprächen bei nicht aktivier Skype-Kommunikation erfolgen kann, haben sich bei der Prüfung nicht ergeben. }}}

(9) Auch der BfDI ist entsetzt über die erkennbare technische Stümperei sowie über die Wurstigkeit der Behörden, die nicht mal den Versuch unternommen haben, die Software zu auditieren oder auditieren zu lassen.

= Trojaner-Einsätze durch Landesbehörden =

== Niedersachsen ==

[[http://www.landtag-niedersachsen.de/Drucksachen/Drucksachen_16_5000/4501-5000/16-4545.pdf|Landtagsdrucksache 16/4116 aus Niedersachsen]] beschreibt drei Trojanereinsätze zum Angriff auf Skype mittels einer Angriffssoftware der Firma Syborg.

== Berlin ==

Laut einer [[http://www.datenschutz.de/news/detail/?nid=5256|Meldung des Virtuellen Datenschutzbüros vom 2.2.12]] hat Berlin für 280000 Euro Einbruchs- und Spähsoftware von Syborg gekauft (vermutlich "Hermes"). In dem Artikel wird Innensenator Henkel Folgendes in den Mund gelegt:

{{{#!blockquote Die Software soll heimlich auf dem Rechner des Nutzers installiert werden und könne alles aufzeichnen, was auf dem Gerät gemacht werde. Mit dem Gesetz zur Quellentelekommunikationsüberwachung soll dies möglich sein. }}}

Wenn Henkel irgendetwas in der Art gesagt haben sollte, hat er klar dokumentiert, dass er selbst überhaupt nicht versteht, wo der Trick bei der Propaganda von Quellen-TKÜ wäre.

Version #1
Erstellt: 2025-10-27 22:34:52 UTC von Datenschmutz Migration Bot
Zuletzt aktualisiert: 2025-10-27 22:34:52 UTC von Datenschmutz Migration Bot