Weiter privat über Liebe

Staatstrojaner im Jahr 2 nach ozapftis

> Im Oktober 2011 veröffentlichte der CCC eine Untersuchung eines vom BKA verbreiteten Schadprogramms, das der Ausspähung privater Rechner diente: der Staatstrojaner trat aus dem Reich der Bond-Legende ins Licht einer freundlich interessierten Öffentlichkeit. Selbst die FAZ breitete genüßlich die Stümperei der BKA-Zulieferer aus. Nun, anderthalb Jahre später, rüttelt immer noch niemand an den lästerlichen §§20k, l BKAG und ihren Pendants in den Polizeigesetzen der Länder, während das BKA Menschen mit Charakterdefiziten und Programmierkenntnissen sucht, die ihnen „bessere" Programme für den Angriff auf die Untertanen-IT schreiben. Zeit also für einen zweiten Blick.

Die ersten konkreten Pläne für das, was mal der „Staatstrojaner" werden sollte, kamen aus Nordrhein-Westfalen. Dort winkte der Landtag 2006 ein neues Verfassungsschutzgesetz durch, das den Schlapphüten recht beliebige Einbrüche auf den Rechnern ihrer Feinde erlaubt hätte. Die Herrscher in Düsseldorf hatten den Text aber in der üblichen Mischung aus Machtbesoffenheit und Unfähigkeit so dumm geschrieben, dass das Bundesverfassungsgericht diese Regelungen schon 2008 wieder kassierte.

Wenn allerdings solche Zumutungen vom Verfassungsgericht (statt durch, sagen wir, Latschdemos oder Straßenschlachten) zurückgewiesen werden müssen, kommt meist ein dickes Ende hinterher, denn die Beamten aus Karlsruhe liefern mit der Zurückweisung gerne Rezepte, wie der staatliche Übergriff trotz Verfassung doch hinzukriegen sei.

In diesem Fall boten sie an, der Zugriff auf die Rechner der ungewaschenen Massen und damit die Verletzung der Menschenwürde – denn ja, bei diesen Dingen gehts immer gleich um Artikel 1 Grundgesetz – könne in Ordnung gehen, wenn es entweder um nur durch universelle Überwachung zu rettende Rechtsgüter geht (der narkotisierende „Bestand des Staates" und sowas halt) oder es nur um Kommunikation geht, denn an der ist in diesem Staat ohnehin nicht mehr viel geheim.

Lügen mit 18 und 37 Zeichen

So kam zu dem Propagandawort „Onlinedurchsuchung" der noch fürchterlichere Terminus „Quellen-Telekommunikationsüberwachung". „Onlinedurchsuchung" ist eine Ein-Wort-Lüge, weil sie suggeriert, es würden ja nur bestehende Mittel modernisiert. Eine Durchsuchung aber hat offen stattzufinden, die Opfer wissen also sofort davon, die panoptische Paranoia („Ist da wer in meinem Notebook?") kommt nicht auf. Dazu wird sich die Staatsgewalt nach einer tatsächlichen Durchsuchung nicht für die nächsten Wochen oder Monate in der Wohnung verstecken und weiter zugucken, was alles passiert. Nein, ehrliche Menschen sagen nicht „Onlinedurchsuchung", sie sagen Computerwanze und Totalüberwachung.

Das womöglich noch wieseligere Gerede von der „Quellen-TKÜ" kam aufgrund des erwähnten höchstrichterlichen Zugeständnisses auf, Einbrüche zur Kommunikationsüberwachung seien irgendwie harmloser als die zur Durchsuchung von Platte oder Bildschirms und könnten daher in Anlehnung an den Schnüffelparagraphen 100a StPO fürs halbe Strafgesetzbuch in Anschlag gebracht werden.

Was das Gericht nicht erklärt hat: Wie sieht mensch Daten an, dass sie „Kommunikation" sind? Ob ich einen Mailentwurf dann auch rausschicke, ist ja nicht vorherzusehen. Und wenn ich ihn rausschicke und er durch die Netz-Schnittstelle geht, ist er schon verschlüsselt, der Einbruch in den Computer würde mithin nichts helfen. „Quellen-TKÜ" ist also ein fieser Propagandabegriff auf der Basis richterlicher Technikinkompetenz; mehr als auf der Leitung (da sitzt der Staat ja leider eh schon) kommt nur raus, wenn

der Schadcode eben nicht die tatsächliche Kommunikation, sondern irgendwas ausforscht, das *vielleicht irgendwann* Kommunikation wird.

Von solchen Details unbelastet sind die BKA-Leute mit der Karlsruher Steilvorlage bei der Regierung aufgeschlagen und haben sich im BKA-Gesetz von 2009 (vgl. dazu auch „Sicherheit in Zeiten des Spin“, RHZ 1/09) den §20l geben lassen, dessen Absatz 2 sagt, das Amt dürfe in Computer einbrechen, um „die Überwachung und Aufzeichnung der Telekommunikation insbesondere auch in unverschlüsselter Form zu ermöglichen„ dürfe dann aber “ausschließlich laufende Telekommunikation überwach[en]“ und aufzeichnen. Dabei ist die Eingriffsschwelle relativ niedrig; im Groben reicht es, dass eine Gefahr für eine Sache „von bedeutendem Wert“ vorliegt und das Opfer vielleicht was mit dieser Gefahr zu tun haben könnte. Einschlägige Anordnungen unterschreibt, damit es einfach bleibt, der Haus-Ermittlungsrichter des BKA.

Dazu tritt dann in §20k das Recht, den kompletten Computer auf den Kopf zu stellen und abzuschnorcheln, und zwar wieder zur „Gefahrenabwehr“ (was anderes regelt das BKAG ja nicht), also lange bevor, sagen wir, wirklich ein Bundeswehrjeep brennt. Dabei versucht der Text den Eindruck zu erwecken, die abzuwehrende Gefahr müsse durch ihre schiere Größe die Menschenverunwürdigung insignifikant erscheinen lassen, kommt dann aber mit dem folgenden Stück atemberaubender Prosa heraus:

> [Totalüberwachung] ist auch zulässig, wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass ohne Durchführung der Maßnahme in näherer Zukunft ein Schaden eintritt, sofern bestimmte Tatsachen auf eine im Einzelfall durch bestimmte Personen drohende Gefahr [für den Staat oder sonstwen] hinweisen.

Ähnliche Regelungen zogen dann nach und nach in die Polizeigesetze der Länder ein (oder werden mit den nächsten Novellierungen einziehen). Pikanterweise sieht die Strafprozessordnung – die ja regelt, was passiert, wenn was passiert ist und nicht nur „Gefahr“ in der Luft liegt – den vollen Computereinbruch noch nicht vor. Die Menschenverunwürdigung, die also bei nach staatlicher Einschätzung Unschuldigen unabweisbar sein soll, geht nicht mehr, wenn der Jeep im Gedankenspiel oben nur noch ein qualmender Haufen Schrott ist.

Der Einbruch „zum Abhören“ wird allerdings auch nach StPO schon gemacht. Zwar schweigt sich der in diesen Fällen bemühte §100a StPO zum Thema „Computer kaputtmachen“ eigentlich aus, bisher hat jedoch auch noch niemand die Logik, „Quellen-TKÜ“ sei ja auch „nur“ TKÜ, ernsthaft kritisiert, juristisch oder sonstwie.

Der Kernbereich

Zu den eher traurigen Konstrukten des Bundesverfassungsgerichtes gehört die Nummer mit dem „Kernbereich der persönlichen Lebensgestaltung“. Dessen Wahrung nämlich bestimmt in der jüngeren Rechtsprechung im Wesentlichen die Schranken beim Verwanzen, Durchsuchen oder Bewegungsprofilieren. Konkret hat das Gericht meist ausgeführt, noch so haarsträubende Überwachung sei in Ordnung, solange sie unterbrochen wird, wenn Gespräche, Standort, Bilder oder Texte Richtung „Kernbereich“ rutschen.

Das Konstrukt ist traurig aus zwei Gründen: Erstens, weil jedenfalls aus Sicht einer linken Solidaritätsorganisation das Problem voyeuristischer Cops gegenüber der tatsächlichen Ausforschung widerständiger Strukturen doch stark zurücktritt. Zweitens ist aber auch die Vorstellung monty-pythonesk, alles sei gut, wenn der Bulle sich zur rechten Zeit gerade noch denkt: „Hups, Kernbereich, das muss ich gleich wieder vergessen“. Nein – entweder, der Staat darf Menschen, Computer, Telefone, Zentren und Wohnungen verwanzen, dann wars das eben mit den persönlichen und noch mehr politischen Kernbereichen, oder er darf es nicht. Schade, dass die einschlägigen Entscheidungen aller deutschen Verfassungsorgane seit vielen Jahren recht klare Prioritäten gesetzt haben.

Entsprechend sieht das in der Praxis aus. Als der Bundesbeauftragte für Datenschutz und Informationsfreiheit sich mal die 23 Einbrüche angesehen hat, die das BKA mit dem Digitask-Trojaner verübt hat, war noch ein Mitschnitt verfügbar, der in der Transskription so dargestellt war:

> „. . . Danach Sexgespräch (Anm. Übers. Ab 15:52:20 bis 16:01:00 finden offensichtlich Selbstbefriedigungshandlungen statt). . . “, „. . . weiter privat über Liebe. . . “

Der BfDI führt dazu trocken aus: “Begründet wurde dies damit, dass eine Teillöschung technisch nicht möglich gewesen sei.“ Hat das Verfassungsgreicht

ernsthaft damit gerechnet, sowas könne anders laufen? Und auch wenn der Kram gelöscht worden wäre: Hätte das die Menschenwürde des Opfers gerettet?

Deep Impact

Der 2012er Bericht des BfDI, aus dem dieses Beispiel kommt, hätte übrigens geheim bleiben sollen, wenn auch lediglich „nur für den Dienstgebrauch". Um so bezeichnender ist, dass die Gretchenfrage selbst noch vor diesem Geheimbericht geheim gehalten wird: Wie genau kommt die Schnüffelsoftware auf die Zielcomputer? Zum grundsätzlichen Ärger über einen Sicherheitsapparat, der noch die kleinste Kontrolle seiner Arbeit erstickt, tritt hier der dringede Verdacht, das BKA könne sich etwa auf dem Schwarzmarkt geheimgehaltene Lücken in Computersystemen beschaffen. Damit würde sich der Staat an einem Geschäft beteiligen, das die Funktionsfähigkeit der gesamten Computertechnik jedenfalls schädigt, eben weil Programmfehler Ware und damit regelrecht erhaltungswürdig werden.

Nicht aus dem Bericht, sondern aus der Praxis bestätigt sind derweil zwei Einbruchstechniken. In der ersten hat der Zoll Amtshilfe geleistet und den Computer des Opfers bei einer Grenzkontrolle unter einem Vorwand in einen anderen Raum verbracht, manipuliert und dann zurückgegeben. Die zweite Technik war ein plumper und gescheiterter Versuch, sich am Rande einer der üblichen willkürlichen Hausdurchsuchungen am Rechner des Opfers zu schaffen zu machen. Allein unter Hinweis auf diese Geschichten sollte mensch die Polizei nie freiwillig mit Hardware allein lassen und der Technik misstrauen, wenn sich die Polizei vertraulichen Umgang mit ihr erzwungen hat.

Um nun die Panik vor dem Staatstrojaner ein wenig zu dämpfen: Trotz direkten Zugriffs auf die Hardware und ggf. der vollen Kooperation der Internet-Provider (die fordert das BKAG natürlich auch ein) hat der Digitask-Trojaner nur in sieben von 12 untersuchten Fällen überhaupt Daten geliefert.

Blutige Amateure

Dabei ist eher überraschend, dass die Erfolgsrate offenbar über 50% lag, denn das verwendete Programm war ausgesprochen stümperhaft geschrieben. So war der Trojaner spielend leicht zu kapern – nebenbei: was die Digitask-Leute vergessen haben ist eng verwandt mit dem Grund für unsere Empfehlung aus RHZ 4/09, sich doch mit dem feinen Web of Trust im PGP zu beschäftigen –, das Ziel der abgeschnorchelten Daten war ein (für alle Opfer gemeinsam verwendeter) Mietserver in den USA und mithin kaum getarnt, und insbesondere hat Digitask komplett versagt, sollten sie überhaupt versucht haben, die (zugegebenermaßen nicht umsetzbaren) Beschränkungen für die „Quellen-TKÜ" aus dem BKAG irgendwie in Code zu gießen. Da konnte der Trojaner Screenshots machen, hier schien etwas auf eventuell am Rechner hängende Mikrofone zugreifen zu wollen, und vor allem erlaubte das Programm, einmal installiert, ganz nach Trojanerart das Nachladen beliebigen weiteren Schadcodes.

Das folgende PR-Desaster hat zu einer spürbaren Trübung des Verhältnisses des BKA zu seinem ehemaligen Hauslieferanten geführt. Das Amt verkündete, für seine Voll-Überwachungen (zu denen ansonsten nichts bekannt ist) habe es eh eine andere Software verwendet, der Digitask-Trojaner werde nicht mehr eingesetzt, man wolle selbst einen schreiben, und bis der, voraussichtlich Ende 2014, fertig sei, sehe man sich nach Alternativen um.

Von denen gibt es einige, denn im Misstrauen gegen die Untertanen sind sich die Machthaber_innen aller Länder gleich. So bedient sich das BKA dem Vernehmen nach derzeit der Software FinFisher, dessen bayrische Hersteller schon die Mubarak-Regierung offenbar nicht wirklich hatten retten können. Für wie viele blutige Nasen von deren Feinden ihr „Produkt" gut war, ist Geschäfts- wie Staatsgeheimnis, ebenso wie schon die Frage, ob Mubarak das hilfreiche Angebot aus München überhaupt angenommen hat.

In den Bundesländern herrscht unterdessen ebenfalls Post-Digitask-Notstand. Von Berlin und Niedersachsen ist bekannt, dass sie in ihrer Not auf die Firma Syborg setzen, was sich diese im Fall Berlin mit 280000 Euro hat vergüten lassen. In diesem Zusammenhang soll Innensenator Henkel gesagt haben, die Software solle „alles aufzeichnen, was auf dem Gerät gemacht" werde, und dieses Wirken sei durch die „Quellentelekommunikationsüberwachung" gedeckt. Die Offenheit, mit der der Senator persönlich die durch Verfassungsgerichts-Subtilität aufgemachte Unterscheidung zwischen Vollausforschung und „Quellen-TKÜ" planiert, würde in einer besseren Welt doch das eine oder andere Richter_innenhirn beschäftigen.

Mühen der Ebene

Das klassische Szenario des massenhaften Polizei-Angriffs aus dem Netz halten wir indes nach wie vor für eher unrealistisch – auf ein halbwegs ordentlich gewartetes System mit wachem_r Nutzer_in aus der Ferne einzubrechen ist nicht einfach und geht schon gar nicht per Knopfdruck. Insofern mag mensch sich fragen, ob sich viel Aufregung um den Staatstrojaner eigentlich lohnt, zumal er vergleichsweise wenig eingesetzt wurde; mehr als einige Dutzend Fälle im Jahr gab es bisher fast sicher nicht (die erwähnten 23 mit Digitask des BKA, plus nochmal ein paar von Bundespolizei und Zoll, wahrscheinlich eine Handvoll Volleinbrüche plus noch ein paar Sachen aus den Ländern), und da sind schon Phisher, Drogis, Nordkorea-Händler und Fluchthelfer_innen dabei.

Umgekehrt liegt durchaus ein klarer Schwerpunkt beim Einsatz im politischen Bereich, in der BKA-Praxis beispielsweise bei 129b und 89a („staatsgefährdende Gewalt“). Außerdem ist die staatliche Selbstermächtigung zum Rumgeistern in unseren Rechnern (und in der Folge Kaputtmachen derselben, von der Hehlerei mit eventuellen „Sicherheitslücken“ ganz zu schweigen) jedenfalls kollektivemotional eine recht harte Nummer, mit der doch eigentlich in Sachen „Entlarven“ oder sonstiger Propaganda was zu machen sein sollte.

Warum unterblieb also eine spürbare gesellschaftliche Mobilisierung nach dem Digitask-Skandal, der ja doch verglichen mit anderen Überwachungsthemen recht breites Echo fand? Vielleicht ja, weil alle den Eindruck hatten, der CCC wache schon über unsere Freiheit?

Aber tatsächlich: Verglichen mit Vorratsdatenspeicherung, Biometrie, PNR, TKÜV und all den anderen Schrecklichkeiten, die wir in den letzten Jahren auf diesen Seiten diskutiert haben, gibt es im Hinblick auf den Staatstrojaner zusätzlich zum überschaubaren Einsatz noch eine gute Nachricht: Selbsthilfe wirkt. Wer die Polizei nicht mit seinem/ihrem Rechner bzw. Telefon allein lässt, ein jeweils halbwegs aktuelles offenes System mit aktivierter Kontrolle der Paketsignaturen laufen hat und nicht einfach Software (oder, wenn es denn sein muss, Äpps) von irgendwoher installiert, wird noch lange Zeit keine großen Sorgen bezüglich der staatlichen Cracker haben müssen.

Richtig viel Trost ist das angesichts der totalen Selbstermächtigung eines offenbar der Paranoia völlig verfallenen Staates aber auch nicht.

Datenschutzgruppe der Roten Hilfe Heidelberg

Kontakt und Artikel-Archiv: https://datenschmutz.de
PGP Fingerprint: a3d8 4454 2e04 6860 0a38 a35e d1ea ecce f2bd 132a