INNERE SICHERHEIT

Trojaner im Abo

Mehr als 50-mal haben Ermittler Spezialsoftware gegen Kriminelle eingesetzt – teilweise rechtswidrig. Nun steht die Zukunft der Computer-Überwachung zur Diskussion.

Seine Freunde nannten Dmitrij A. den „Diminator“. Er schwamm auf einer Welle des Erfolgs. Geld, Freundeskreis, Muskeln, alles schien nur eine Richtung zu kennen: Es wuchs.

Anfangs war der 110-Kilo-Mann Deutscher Juniorenmeister der Bodybuilder, doch dann stieg er in den Handel mit Anabolika ein. Über den vermeintlich sicheren Mail-Anbieter „hushmail“ schrieb er seine chinesischen Lieferanten unter deren vielsagendem Namen „anabolicsteroid@hotmail.com“ an. Die Kunden des Diminators bekamen Post über „SAFe-Mail“, einen Service, der ebenfalls unknackbar schien.

Am 21. Januar 2010 ordnete das Amtsgericht Nürnberg deshalb den Einsatz einer Computer-Überwachung „im Rahmen einer Fernsteuerung“ an. Die Staatsanwaltschaft hatte den Einsatz eines Trojaners beantragt und vorsorglich darauf hingewiesen, dass „die Frage der Zulässigkeit bundesweit noch uneinheitlich gesehen wird“.

Vermutlich als E-Mail-Anhang schmuggelten die Ermittler die Software auf die Festplatte des Diminators. Sie lasen Mails mit, die der Russlanddeutsche verschlüsselt verschickte, hörten Skype-Telefonate ab und schossen „Application Shots“, mit denen sie überwachen konnten, was sich auf dem Rechner des Muskelmanns gerade tat.

Nach 13 Tagen hatten die Ermittler genügend Beweise, sie nahmen ihn fest. Mit so viel technischer Finesse seiner Verfolger hatte er offenbar nicht gerechnet.

Massiver Eingriff

Das Auge des Gesetzes

Auszug aus SPIEGEL 9/2011

Der Fall aus Nürnberg befördert eine Debatte, die seit vergangener Woche um elementare Fragen des Rechtsstaats geführt wird. Welche Technik dürfen deutsche Sicherheitsbehörden bei ihren Ermittlungen gegen Beschuldigte einsetzen? Und unterlaufen sie dabei die Vorgaben des Bundesverfassungsgerichts, das im Februar 2008 den Einsatz von Trojanern nur in engen Grenzen erlaubt hatte?

Ausgelöst wurde die Debatte durch eine Analyse des Chaos Computer Clubs (CCC), der ein in Bayern eingesetztes Schnüffelprogramm, einen sogenannten Trojaner, technisch sezierte. Über den Fall hatte im Februar der SPIEGEL (9/2011) berichtet, und die jetzt vom CCC veröffentlichte Analyse förderte so viele fachliche und juristische Mängel zutage, dass seitdem die Empörung über den offenkundig rechtswidrigen Einsatz der Überwachungssoftware groß ist.

Die Trojaner sollen eine Art Ultima Ratio der Behörden sein. Sie dürfen nur dann eingesetzt werden, wenn Beschuldigte geheim kommunizieren: verschlüsselt chatten, via Skype telefonieren oder ihre E-Mails kryptieren. Die Spähsoftware nistet sich auf dem Rechner der Zielperson ein und leitet die Daten auf Server der Ermittler. Deshalb wird die Methode „Quellen-Telekommunikationsüberwachung“ („Quellen-TKÜ“) genannt.

Doch das Verfassungsgericht hat in seinem Grundsatzurteil 2008 die „Integrität informationstechnischer Systeme“ – also von Computern – zum Grundrecht erklärt, vergleichbar der Unverletzlichkeit der Wohnung. Eingriffe bedürfen eines Richterbeschlusses.

Deutlich über 50-mal haben Gerichte diesen erteilt und Behörden solche Trojaner eingesetzt. 20-mal schmuggelte das Bundeskriminalamt (BKA) die Spähsoftware auf Festplatten von Verdächtigen, viermal das Bundesamt für Verfassungsschutz, einmal die Bundespolizei.

Allerdings sei, versicherte das Bundesinnenministerium vergangene Woche, die Anwendung anders als in Bayern stets restriktiv erfolgt, auf Basis der geltenden Rechtslage. Screenshots etwa seien damit ausgeschlossen worden. Das Zollkriminalamt setzte die Technik angeblich bislang 16-mal ein. Dazu kommt eine unbekannte Zahl von Fällen in den Ländern.

Bis sicher sei, dass die Programme nicht mehr vollbringen könnten, als rechtlich erlaubt ist, sollten die Bundesländer die Spähsoftware nicht mehr nutzen, fordert Bundesinnenminister Hans-Peter Friedrich (CSU). Dem Machtwort des Berliner

Parteifreunds beugte sich auch Bayerns Innenminister Joachim Herrmann (CSU), der trotz gegenteiliger Rechtsprechung noch immer der Meinung ist, sein Bayern-Trojaner sei sauber eingesetzt worden.

Umstritten ist vor allem, welche Computeraktivitäten von dem Begriff „Kommunikation“ noch abgedeckt sind. Das Landgericht Landshut hat dazu bereits im Januar 2010 einen Beschluss gefasst und das Schießen von Bildschirmfotos im Rahmen einer Quellen-TKÜ als rechtswidrig eingestuft.

In dem Verfahren, das noch nicht abgeschlossen ist, wird einem Geschäftsmann aus Landshut vorgeworfen, er habe unerlaubt Betäubungsmittel gehandelt. Im Auftrag der Behörden hatte offenbar ein Trojaner der hessischen Firma DigiTask alle 30 Sekunden einen Screenshot des überwachten Computers gemacht.

Genau diese Screenshot-Funktion stufte das Gericht als illegal ein: „Nach Auffassung der Kammer besteht für das Kopieren und Speichern der grafischen Bildschirminhalte keine Rechtsgrundlage, weil zum Zeitpunkt dieser Maßnahmen noch kein Telekommunikationsvorgang stattfindet.“

Die in Bayern eingesetzte Software, fand der CCC heraus, kann freilich noch viel mehr – etwa weitere Programme nachladen. Zudem sicherte das Programm den Datentransfer zu den Ermittlern nur unzureichend ab.

DigiTask habe in den Verkaufsgesprächen „ihren Instrumentenkoffer gezeigt und damit geprahlt, was sie alles können“, sagt ein Beamter. Offensichtlich kauften einige Behörden mehr als andere. Einige Beamte müssen sich jetzt den Vorwurf gefallen lassen, mit Geschäftsleuten zusammengearbeitet zu haben, die eine dubiose Geschichte haben.

Denn die Ermittler kennen die hessischen Unternehmer auch aus eigenen Akten. Ein damals führender Mitarbeiter wurde 2002 wegen Bestechung von Beamten des Zollkriminalamts zu einer ungewöhnlich hohen Geldbuße von 1,5 Millionen Euro und 21 Monaten Haft auf Bewährung verurteilt. Im Jahr 2000 war es zudem gleich in diversen Landeskriminalämtern zu Durchsuchungen wegen des Verdachts der Korruption im Zusammenhang mit den Hessen gekommen.

Dass die Nachfolgefirma DigiTask bei den Bundesbehörden und diversen Landeskriminalämtern wieder zum Zuge kam, hat offenbar vor allem einen Grund. Als das BKA 2007 damit begann, den Markt für diese sensible Technik zu sondieren, boten zwar einige Firmen komplette Überwachungslösungen an – bis hin zu einer vollständigen Kopie der Festplatte, der sogenannten Online-Durchsuchung.

Die meisten Firmen, heißt es in Ermittlerkreisen, hätten allerdings die Sicherheitsüberprüfung nicht bestanden. Nur DigiTask ließ die deutschen Fahnder in den Quellcode schauen, jenen Bauplan eines Programms, an dem Profis ablesen können, was genau eine Software tut.

Die vertrauensbildende Maßnahme öffnete DigiTask einen Millionenmarkt – und widerlegt gleichzeitig Aussagen, wonach die Behörden nicht genau gewusst hätten, zu was der Trojaner technisch in der Lage ist. Ihre Verträge schlossen Bund und Länderbehörden jeweils separat ab.

Die Bayern abonnierten den Trojaner gleich jahresweise, für eine Pauschale von rund 220 000 Euro. Das BKA dagegen ließ sich für jeden Fall eine abgespeckte Trojaner-Version maßschneidern, testete sie vorab und bezahlte pro Nutzung. Drei Monate schlugen dort mit 15 000 Euro zu Buche.

An diesem Donnerstag wollen die Innenminister von Bund und Ländern in einer Telefonkonferenz über die Zukunft der Trojaner beraten. Dabei werden sie wohl auch einen Vorschlag diskutieren, der derzeit intern erörtert wird: die Entwicklung einer eigenen, unabhängig überprüfbaren und rechtlich einwandfreien Software.

Denn anders als bei der Quellen-TKÜ wendet das BKA bei der Online-Durchsuchung, also bei der Abwehr terroristischer Gefahr, bereits ein eigenes Programm an, für dessen Entwicklung die Behörde allein bis 2010 etwa 680 000 Euro ausgab – es kam seither siebenmal gegen militante Islamisten zum Einsatz.

Das staatliche Spähprogramm für die Online-Durchsuchung funktioniere „technisch ähnlich“ wie die anderen Programme, heißt es in einem vertraulichen BKA-Bericht. Es könne also ohne allzu große Mühen auch für die Quellen-TKÜ umgewidmet werden.

Für Dmitrij A., der derzeit im Gefängnis Rothenfeld seine Strafe von vier Jahren und sechs Monaten absitzt, könnte die Debatte eine unverhoffte Folge haben. Die bayerischen Ermittler hatten den Trojaner gegen den Bodybuilder eingesetzt, obwohl das Landgericht Landshut bereits seine Bedenken geltend gemacht hatte.

Sein Anwalt Jürgen Schwarz überlegt nun, eine Wiederaufnahme des Verfahrens anzustreben. „Hier wurden offenbar Beweismittel widerrechtlich erlangt“, sagt er, „das kann nicht ohne Folgen bleiben.“

Marcel Rosenbach,
Holger Stark, Steffen Winter