

Trojaner im Computer:
Einsatz trotz fehlender
Rechtsgrundlage

«Einfach nur dreist»

Bundeskriminalpolizei und Staatsanwälte verwenden in der Praxis sogenannte «Trojaner» – rechtliche Grundlage hin oder her. Die Spionageprogramme können viel mehr, als das Gesetz erlaubt.

So hinterlistig wie die Griechen, die sich im Bauch eines Holzpferdes in die Stadt Troja eingeschlichen haben, schleust sich ein heutiger Trojaner in einen Computer ein, getarnt als scheinbar harmlose Datei. Genau so heimlich wie die Griechen öffnet er dessen Tore gegen aussen. Ohne Wissen des Computerbenützers können die ungebeten Gäste dann Passwörter oder Kreditkartennummern ausspionieren, indem sie zum Beispiel die Tastatureingaben direkt einem Dritten kommunizieren.

Von solchen Programmen machen Kriminelle und die Polizei

Gebrauch. Nach dem Skandal in Deutschland wurden jüngst auch in der Schweiz verschiedene Fälle publik: Viermal soll die Bundeskriminalpolizei in der Strafverfolgung zu diesem Überwachungsmittel gegriffen haben, dazu kommen unbekannt viele Einsätze von kantonalen Ermittlern.

«Rechtsgrundlage nicht vorhanden»

Die vier Einsätze des Bundes erfolgten vor Inkrafttreten der neuen Schweizerischen Strafprozessordnung (StPO), gestützt auf Artikel 66 der Bundesstrafrechtspflege,

der den «Einsatz technischer Überwachungsgeräte» unter bestimmten Voraussetzungen erlaubte. In der neuen StPO nimmt Artikel 280 diese Formulierung auf. Er wird laut dem Eidgenössischen Justiz- und Polizeidepartement (EJPD) von den Staatsanwaltschaften heute als Rechtsgrundlage für den Einsatz von Trojanern herangezogen.

Taugt der Artikel 280 StPO als Rechtsgrundlage? Kann ein Computerprogramm, mit dem man in ein fremdes Datensystem eindringt und es manipuliert, als «technisches Überwachungsgerät» im Sinne dieser Bestimmung gelten? Für Anwalt Martin Steiger ist eine hinreichende Rechtsgrundlage nicht nur «umstritten», sondern schlicht «nicht vorhanden». «Im Strafrecht gilt das Legalitätsprinzip: Die Strafverfolgungsbehörde darf nur Mittel gebrauchen, die ausdrücklich zugelassen sind.»

«Diese Trojaner sind ab Stange erhältlich und können jeweils viel mehr, als sie eigentlich dürften»

Thomas Hansjakob, Staatsanwalt

Umso mehr, weil die Überwachung mit Trojanern ein schwerwiegender Eingriff in die Grund-

Auch das EJPD räumt ein, dass «nur ein Teil der Lehre diese Rechtsgrundlage als ausreichend erachtet». Geht man diesem «Teil der Lehre» nach, wird das Fundament noch wackliger. Denn konkret gemeint ist damit Thomas Hansjakob, welcher im Kommentar zur Schweizerischen Strafprozessordnung zurückhaltend festhält, «dass sich Artikel 280 nur bei sehr weiter Auslegung auf den Einsatz von Government-Ware (GovWare, also staatlich entwickelte und eingesetzte Software zur Überwachung von Computern) anwenden lässt». Im persönlichen Gespräch mit dem Ersten Staatsanwalt in St.Gallen wird klar: Eine Rechtsgrundlage für den Einsatz von Staatstrojanern gibt es nach Hansjakob heute nicht. «Artikel 280 StPO kommt nicht in Frage, denn bei einem Trojaner geht es um das «Einführen von Informatikprogrammen in ein Datensystem», sagt Hansjakob.

KEYSTONE

rechte sei. «Weil der Betroffene nichts von der Überwachung weiss, kann er sich nicht dagegen wehren.» Dazu kommt, dass die Schweiz bedauerlicherweise kein absolutes Beweisverwertungsverbot kenne, so Steiger. «Selbst wenn die Überwachung mittels Trojaner nachträglich als rechtswidrig erklärt wird, könnten die dadurch erlangten Beweise im Strafprozess allenfalls verwertet werden.»

Diese Formulierung findet sich im geplanten Artikel 270^{bis} StPO, welcher mit der Revision des Bun-

desgesetzes zur Überwachung des Post- und Fernmeldeverkehrs (BÜPF) eingeführt werden soll. Auch der Bundesrat hat offenbar erkannt, auf welcher dürftigen Rechtsgrundlage der heutige Einsatz von Staatstrojanern basiert.

In der Vernehmlassung stiess die «Trojaner-Vorlage» auf herbe Kritik, quer durch alle politischen Lager und Interessenverbände. Neben grundrechtlichen Bedenken wird kritisiert, dass der eindringende Trojaner das System nicht unverändert lässt. Er schafft nämlich eine Lücke, um die gewünschten Informationen nach aussen zu schleusen. Diese Lücke, so die Kritiker, könne aber neben dem Staat auch von anderen Angreifern genutzt werden.

«Staatsanwalt muss genaue Auflagen machen»

Thomas Hansjakob scheint dieses Szenario eher unwahrscheinlich. Das eigentliche Problem der Trojaner sieht er anderswo: «Der Punkt ist, dass diese Trojaner ab Stange erhältlich sind und jeweils viel mehr können, als sie eigentlich dürften.» Also nicht nur ein Gespräch via Internet-Telefon abhören, sondern zum Beispiel auch die gesamte Festplatte durchsuchen, mittels Screenshots das aktuelle Geschehen auf dem Rechner überwachen oder gar die Kontrolle über die Kamera übernehmen und das Mikrofon als elektronische Wanze nutzen.

Die Trojaner werden immer raffinierter und die Wissenslücke zwischen den Technikern bei der Polizei und den altgedienten Staatsanwälten immer grösser. «Die meisten Staatsanwälte und Zwangsmassnahmengerrichte können gar nicht mehr nachvollziehen, was die Polizei mit einem Trojaner genau macht», sagt Hansjakob. «Wichtig ist darum, dass von Seiten der Polizei mit offenen Karten gespielt wird und der Staatsan-

Zur Rechtsgrundlage der Strafprozessordnung

Einzelne Strafverfolgungsbehörden stützen sich beim Einsatz von Staatstrojanern auf Artikel 280 der StPO:

Artikel 280: Zweck des Einsatzes

Die Staatsanwaltschaft kann technische Überwachungsgeräte einsetzen, um:

- a. das nicht öffentlich gesprochene Wort abzu- hören oder aufzuzeichnen;
- b. Vorgänge an nicht öffentlichen oder nicht allgemein zugänglichen Orten zu beobachten oder aufzuzeichnen;

c. den Standort von Personen oder Sachen festzustellen.

Im Rahmen der BÜPF-Revision will der Bundesrat eine klarere Regelung und schlägt folgenden Artikel in der StPO vor:

Artikel 270^{bis}: Abfangen und Entschlüsselung von Daten

1. Sind bei einer Überwachung des Fernmeldeverkehrs die bisherigen Massnahmen erfolglos geblieben oder wären andere Überwachungsmassnahmen

aussichtslos oder würden die Überwachung unverhältnismässig erschweren, so kann die Staatsanwaltschaft auch ohne Wissen der überwachten Person das Einführen von Informatikprogrammen in ein Datensystem anordnen, um die Daten abzufangen und zu lesen. Die Staatsanwaltschaft gibt in der Anordnung der Überwachung an, auf welche Art von Daten sie zugreifen will.

2. Die Anordnung bedarf der Genehmigung durch das Zwangsmassnahmengericht.

walt in seiner Verfügung genaue Auflagen macht, wie weit die Überwachung gehen darf.»

Gesetz hinkt technischer Entwicklung hinterher

Die Bundesanwaltschaft will trotz der mangelnden gesetzlichen Regelung den Einsatz eines Staatstrojaners nicht ausschliessen. «Das Gesetz überlässt die Wahl der technischen Mittel bewusst und völlig zu Recht den Strafverfolgungsbehörden, denn die technologischen Mittel verändern sich laufend», lässt Jeannette Balmer, Mediensprecherin der Bundesanwaltschaft, wissen. Auch Martin Bürgisser, Oberstaatsanwalt im Kanton Zürich, würde nicht zögern, gestützt auf Artikel 280 StPO einen Trojaner-Einsatz anzuordnen: «Die Fälle sind selten, aber die Rechtsgrundlage genügt unserer Ansicht nach.»

Die genaue Auslegung der Rechtsnorm liege bei den Gerichten. In diesem Fall bei den Zwangsmassnahmerichtern, welche für jede virtuelle Überwachung eine Genehmigung erteilen müssen. Im Kanton Bern hätte Bürgisser mit einem begründeten Antrag gute Chancen. Zwar gab es dort bis anhin keinen konkreten Fall, aber Jürg Zinglé, Präsident des kantonalen Zwangsmassnahmerichters in Bern, schliesst eine Genehmigung in schweren Fällen wie organisierter Kriminalität oder Kinderpornographie nicht aus: «Aufgrund der aktuellen Diskussion wären wir aber zurückhaltend und würden die Voraussetzungen besonders genau prüfen.»

Unbestritten ist: Das Gesetz hinkt der technischen Entwicklung hinterher. Darf man die Polizei in ihrem Handlungsspielraum wegen mangelnder gesetzlicher Grundlagen trotzdem einschränken? «Man muss», meint Niklaus Ruckstuhl, Anwalt und Professor für Strafprozessrecht an der Universität Basel. «Neue technische

Möglichkeiten fordern neue gesetzliche Grundlagen.» Und diese fehlen im Moment für den Einsatz von Trojanern in der Strafverfolgung. «Man darf neue Technologien nicht einfach mit Gewalt unter bestehendes Recht subsumieren. Dieses Vorgehen ist undemokratisch, einer solchen Überwachung fehlt jegliche Legitimation.» Wolle man dafür eine Rechtsgrundlage schaffen, müsse man

sich die Voraussetzungen genau überlegen. Ruckstuhl: «Braucht es eventuell ein spezielles Genehmigungsverfahren für die Überwachung mittels Computerprogrammen? Oder vielleicht eine andere Regel für Zufallsfunde, weil solche beim Einsatz von Trojanern sehr wahrscheinlich sind?» Besonderheiten dieser Art von Überwachung müssten beachtet werden.

Überwiegend Kritik in der Vernehmlassung

Am 23. November 2011 hat der Bundesrat das EJPD mit der Ausarbeitung der Botschaft zur BÜPF-Revision beauftragt. Der Bundesrat befürwortet die Schaffung einer gesetzlichen Grundlage für Trojaner, will deren Einsatz aber nur bei Delikten erlauben, zu deren Verfolgung die verdeckte Ermittlung zulässig ist. Zudem soll die Überwachung auf Daten aus dem Fernmeldeverkehr beschränkt bleiben. Anwalt Martin Steiger ist gespannt auf die kommende Diskussion. Er sagt aber klar: «Angesichts der laufenden BÜPF-Revision, in der die gesetzliche Grundlage erst diskutiert wird, ist die heutige Verwendung von Bundestrojanern in der Schweiz einfach nur dreist.»

Corinne Stöckli

Trojaner

«Trojaner» ist die Abkürzung für «Trojanisches Pferd».

Ein Trojaner ist ein Computerprogramm, das im Hintergrund ohne Wissen des Nutzers schädliche Aktionen durchführt. Es gelangt meist über einen E-Mail-Anhang, eine infizierte Webseite oder austauschbare Datenträger auf den Computer.

So können zum Beispiel Spionageprogramme auf den Computer gelangen, die Tastatureingaben aufzeichnen, Daten durchsuchen oder sogar Mikrofon und Kamera eines Laptops einschalten.