WOZ DIE WOCHENZEITUNG

27. Mai 2010

Online-Durchsuchungen

Der Staat in deinem Computer

Von Dinu Gautier

Der Bund will mit heimlich eingeschleusten Trojanern Computer durchsuchen. Experten erklären, wie das funktioniert. Die Piratenpartei droht mit einem Referendum.

Die Strafverfolgungsbehörden wollen künftig Trojaner auf die Computer von Verdächtigen schleusen dürfen. Mithilfe dieser Überwachungsprogramme soll der Staat nicht nur verschlüsselte Mails oder verschlüsselte Internettelefonate (VoIP) mitverfolgen können, sondern sich auch gleich auf der Festplatte der überwachten Personen umsehen dürfen. «Es kann auf das ganze Datenverarbeitungsprogramm zugegriffen werden», so die offizielle Beschreibung.

Die neue Massnahme ist in einem Vernehmlassungsentwurf für ein überarbeitetes Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (Büpf) zu finden. Veröffentlicht wurde der Entwurf letzte Woche. Deutschschweizer Nachrichtenagenturen und Medien haben die neue Massnahme bisher nicht bemerkt.

Dabei betont sogar das Bundesamt für Justiz (BJ) in seinen Erläuterungen, um welch heiklen Eingriff in die Privatsphäre der Betroffenen es sich handelt: Mit dieser Technik könne auch auf Daten zugegriffen werden, welche nicht in Zusammenhang mit dem Überwachungszweck stünden und «die zur Privat- oder sogar Intimsphäre gehören». Als Beispiele werden «Fotos», «Filme» sowie «Korrespondenz» genannt.

Den geplanten Einsatz von Bundestrojanern rechtfertigt das Bundesamt für Justiz mit der zunehmend verschlüsselten Kommunikation von Verdächtigten, sei dies per Mail oder VoIP-Telefonie (beispielsweise Skype), die mit herkömmlichen Methoden nicht überwachbar sind. «Wir führen keine Statistik darüber, wie viele Personen in der Schweiz verschlüsselte E-Mails verschicken», sagt Eva Zwahlen vom Bundesamt für Justiz auf Nachfrage. Heutzutage würden aber zahlreiche Mailsysteme die Verschlüsselung standardmässig ausführen.

Passwörter mitlesen

(Bundes-)Trojaner sind Programme, die unbemerkt auf dem Rechner (oder dem Mobiltelefon) der zu überwachenden Person laufen. Einmal installiert, sind sie kaum zu entdecken. Übers Internet sendet der Trojaner Informationen an die Behörde. Diese erhält so Zugriff auf alle Dateien, kann die Tastatureingaben mitlesen (wodurch sie zu Verschlüsselungspasswörtern kommt) oder das System gar fernsteuern. Bei Laptops kann beispielsweise das Mikrofon eingeschaltet werden, was das unbemerkte Abhören von Gesprächen im Raum ermöglicht, in dem der Laptop steht.

Patrick Rohner, beim BJ zuständig für die Büpf-Revision, redet nicht gerne von Trojanern: «Der Begriff ist negativ besetzt. Der Staat ist ja kein Internetkrimineller, sondern handelt im Rahmen des Gesetzes.» Technisch sei mit den Programmen vieles möglich, räumt Rohner ein. Die Aktivierung von Laptopmikrofonen etwa hält er nicht nur technisch, sondern dank des vorgeschlagenen Gesetzes künftig auch juristisch für möglich. Rohner betont aber, dass die Untersuchungsbehörden vor dem Einsatz der Trojaner verschiedene Verfahrenshürden nehmen müssen.

Das unbemerkte Einschleusen von Trojanern auf den Computer oder das Mobiltelefon des Verdächtigten ist anspruchsvoll. Wie das gehen könnte, erklärt ein IT-Experte mit Erfahrungen auf dem Gebiet. Er möchte anonym bleiben, nennen wir ihn Pit Schürmann: «Man müsste zuerst mittels herkömmlicher Überwachung das Verhalten der Zielperson analysieren, um einen geeigneten Weg zu finden, ihr den Trojaner unterzujubeln.» Getarnt als Freund der Person, könnte man ihr dann beispielsweise ein Computerspiel zusenden, in welchem sich der Trojaner versteckt. «Eine weitere Möglichkeit ist die Installation vor Ort im Rahmen einer verdeckten Polizeiaktion», so Schürmann.

Ruben Unteregger hat früher für die Schweizer Firma ERA IT Solutions gearbeitet. Bereits 2006 berichtete die «SonntagsZeitung», die Firma habe im Auftrag des Bundes Trojaner zur Überwachung von Skype-Gesprächen entwickelt. Letzten Sommer hat Ruben Unteregger Bausteine für solche Trojaner der Öffentlichkeit online zugänglich gemacht. Er geht davon aus, dass die Behörden zur Einschleusung von Trojanern weniger die «klassischen Hackermethoden» verwenden würden, sondern auf die Mithilfe der Provider zählten. «Nicht umsonst zwingt das neue Büpf diese ja zur Kooperation in diesem Punkt» (vgl. «Unternehmen zur Schnüffelei gezwungen» weiter unten). Mithilfe der Provider könne man sich in den Datenstrom einklinken. Wolle der Nutzer ein Programm aus dem Internet runterladen, könne man den Trojaner um das nachgefragte Programm herumwickeln, was eine «elegante Methode» und nur mittelmässig aufwändig sei, so Unteregger. «So würden zudem Antivirenprogramme umgangen, da es sich ja um einen legitimen, vom Benutzer initiierten Download handelt.»

Alles Kinderpornografie?

Für Viktor Györffy, Anwalt und Präsident von grundrechte.ch, hat der Einsatz von Trojanern einen grundsätzlich anderen Charakter als die traditionelle Kommunikationsüberwachung. «Das ist, wie wenn Sie, statt die Briefe abzufangen und zu öffnen, den Schreibtisch aufbrechen und neben dem Büro gleich auch noch das Wohn- und das Schlafzimmer durchstöbern.» Man müsse sich bewusst sein, wie zentral die Computer für die Menschen geworden sind. «In ihnen bilden sich sehr grosse Teile unseres Lebens ab.» Es handle sich hier um einen «wahnsinnig einschneidenden Eingriff» in die Persönlichkeitsrechte eines Betroffenen, so Györffy.

Betroffen von Überwachungsmassnahmen (und damit auch von Trojanerangriffen) können Personen sein, bei denen der Verdacht besteht, ein bestimmtes Delikt begangen zu haben. Die Liste der Delikte, für welche das Gesetz eine solche Überwachung zulässt, verweist auf nicht weniger als 97 Strafartikel. Darunter Klassiker wie die Finanzierung einer terroristischen Organisation, verbotene Pornografie oder Mitgliedschaft in einer kriminellen Organisation, aber auch schwerere Drogendelikte, Diebstahl, Veruntreuung, Betrug, Sachbeschädigung mit hohem Schaden, unbefugte Datenbeschaffung, gewerbsmässiger Wucher, Drohung, Schreckung der Bevölkerung oder Störung des Eisenbahnverkehrs, um nur einige Beispiele zu nennen.

Patrick Rohner vom BJ betont, dass der Trojanereinsatz nur «doppelt subsidiär» angewandt werden soll. Bereits die herkömmliche Kommunikationsüberwachung werde nämlich nur bewilligt, wenn normale Untersuchungsmethoden nicht ausreichten. Nur wenn auch die Kommunikationsüberwachung «erfolglos geblieben» sei, etwa wenn der Verdächtige Mails verschlüsselt, komme es zum Einsatz der Trojaner. «Bei allen Kommunikationsüberwachungen gilt: Es braucht eine Bewilligung eines Gerichts», so Rohner. Beim Trojanereinsatz «muss der Staatsanwalt zudem die Art der Daten, die er will, genau angeben». So soll vermieden werden, dass auf Daten zugegriffen wird, die von vornherein nutzlos sind.

IT-Experte Pit Schürmann: «Ohne sich erst einmal durch die Dateien zu ackern, kann man sich kein abschliessendes Bild machen.» Es gebe zwar Spezialprogramme, die zum Beispiel automatisiert Kinderpornografie finden würden, schliesslich könne aber nur ein Mensch eine seriöse Durchsuchung garantieren. Viktor Györffy von grundrechte.ch: «Sind die Dateien einmal durchschnüffelt, dann ist die Privatsphäre bereits verletzt - egal, was dann weitergereicht wird und was nicht.»

Hohe Kosten

Bezüglich Aufwand rede man bei einem Trojanerangriff nicht von fünf Stunden, sondern eher von fünfzig Stunden Arbeit - «bei Stundenansätzen von rund 250 Franken wird das schnell sehr teuer», sagt Pit Schürmann. Ruben Unteregger betont, dass man einen Trojaner nicht einfach schreiben und dann ewig einsetzen könne. «Die Programme müssen ständig gepflegt und erweitert werden, um mit der technischen Realität auf den Rechnern mitzuhalten.»

Patrick Rohner vom BJ zu den Kosten: «Es ist teuer, weil es A-la-carte-Lösungen braucht. Die genauen Kosten kenne ich nicht. Wir reden in einem Fall vielleicht von 10 000, in einem anderen vielleicht von nur 1000 Franken.» Die Kosten würden für die Staatsanwälte ein weiterer Grund sein, diese Art der Überwachung sorgfältig zu prüfen, so Rohner.

Politischer Widerstand gegen die Büpf-Revision ist abzusehen. Zur Wehr setzen will sich etwa die Piratenpartei. Deren Präsident Denis Simonet zur WOZ: «Nützt Aufklärung nichts, so halten wir uns die Möglichkeit offen, das Referendum zu ergreifen.» Simonet weist darauf hin, dass laut Gesetzesentwurf nicht nur Verdächtige betroffen wären, sondern auch Leute aus dem engeren Umfeld der Verdächtigten. «Man findet in jedem Umfeld jemanden, den man eines Deliktes verdächtigen kann.» Wichtig sei es, nun eine Debatte über Überwachung an sich zu lancieren. «Schuldig ist man erst, wenn man verurteilt wurde», sagt der Piratenpräsident. «Das nennt sich Unschuldsvermutung.»

Unternehmen zur Schnüffelei gezwungen

Heute bekommen Kommunikationsdienstleister für Überwachungen eine Entschädigung ausbezahlt. In der Praxis betrifft das vor allem Telefon- und Mobilfunkdienstleister sowie Anbieter von Internetzugängen (Access-Provider). Letztere müssen seit April dieses Jahres in der Lage sein, den gesamten Datenverkehr ihrer KundInnen bei Bedarf in Echtzeit mitzuschneiden, wie die WOZ letzten Sommer enthüllte (siehe WOZ Nr. 29/09). Neu müssen die sogenannten Randdaten aller Internet-, Mobil- und TelefonnutzerInnen während zwölf statt sechs Monaten gespeichert werden.

Die staatlichen Entschädigungen für Kommunikationsüberwachungen hingegen sollen wegfallen. Grössere Firmen protestieren bereits dagegen. Gegenüber der «Aargauer Zeitung» sprach etwa die Cablecom von «Zusatzkosten im sechsstelligen Bereich». Die Swisscom befürchtet, dass künftig auch die Anzahl der Behördenanfragen steigen wird.

Kommt der vorliegende Entwurf für das Gesetz zur Überwachung des Post- und Fernmeldeverkehrs (Büpf) durch, erweitert sich zudem der Kreis jener beträchtlich, die auf eigene Kosten die Überwachungsarbeit für den Staat erledigen müssen. Betroffen wären neu alle sogenannten «reinen Serviceprovider», darunter auch Kleinstbetriebe oder Privatpersonen, die Speicherplatz für Webseiten anbieten (Webhosting), sofern sie dies beruflich tun.

Das stellt gerade kleine Betriebe vor grosse Probleme: Silvan Gebhardt ist 23-jährig, Inhaber eines Start-up-Unternehmens in Frauenfeld und spezialisiert auf Kommunikationslösungen für Unternehmen, die dank Gebhardts Firma OpenFactory über Internettelefonie kommunizieren können. «Was dieses Gesetz von mir verlangt, kostet mich zwei bis drei Monatsumsätze - noch bevor überhaupt eine Überwachung angeordnet wird.» Für seine GmbH mit zwei Angestellten sei dies «existenzbedrohend». Der Jungunternehmer, der schon als Dreizehnjähriger IT-Dienstleistungen angeboten hat, sagt: «Sollte das Gesetz so durchkommen, könnte ich es einfach ignorieren - und dabei eine Busse in ebenfalls existenzbedrohender Höhe riskieren.» Wer den Weisungen nicht Folge leistet, kann laut Büpf-Entwurf mit bis zu 100 000 Franken gebüsst werden.