Galileo entdeckt gar nichts mehr

10. Juli 2015

Die Kantonspolizei Zürich verzichtet auf die Überwachungssoftware

von Philipp Lenherr, Limmattaler Zeitung

Nachdem der Programmcode der Überwachungssoftware Galileo, welche unter anderem die Zürcher Kantonspolizei gekauft hat, ins Internet gestellt wurde, steht die Frage im Raum, ob sich die Software zur Überwachung der Computer von Verdächtigen nun überhaupt noch einsetzen lässt. «Wir haben keine Hinweise auf Probleme», wurde Kripochefin Lentjes Meili in der Mittwochausgabe des «TagesAnzeigers» auf die entsprechende Frage hin zitiert.

Gestern folgte dann die Kehrtwende: Die Kantonspolizei verwendet die Software nicht mehr. Mit ein Grund dafür dürfte die Mitteilung sein, die der Hersteller von «Galileo», die in Mailand ansässige Firma «Hacking Team», gestern auf ihrer Website veröffentlicht hat: Praktisch alle Kunden hätten auf ihren Hinweis hin den Einsatz der Software eingestellt. Dies sei ein wichtiger Schritt zum Schutz laufender Untersuchungen. Das Unternehmen geht davon aus, dass die Anti-Virus-Programme von überwachten Personen «Galileo» schon bald erkennen werden. Damit wären diese gewarnt, dass ihnen die Behörden auf den Fersen sind.

«Katz-und-Maus-Spiel»

«Hacking Team» arbeitet gemäss Mitteilung nun an Änderungen am Programm, um dieses wieder einsetzbar zu machen. Ein einfaches Unterfangen wird das jedoch nicht, wie Marc Ruef, IT-Sicherheitsexperte bei der Zürcher Firma Scip, auf Anfrage sagt. «‹Hacking Team› müsste zuerst herausfinden, anhand welcher Merkmale Anti-Virus-Programme ihre Software erkennen», sagt er. Danach könne «Galileo» entsprechend verändert werden - und die Anti-Virus-Programme könnten danach ebenfalls wieder angepasst werden. «Es ist ein Katz-und-Maus- Spiel», sagt Ruef.

Den Schaden, den «Hacking Team» durch die Veröffentlichung seiner Programmcodes und Geschäftsunterlagen erleidet, hält er für sehr gross. «Wahrscheinlich wird die Firma deswegen eingehen.» Die Kunden würden dann ohne jeglichen Support und Updates für ihre teure eingekaufte Überwachungssoftware dastehen.

Gemäss dem Mailverkehr zwischen der Kantonspolizei Zürich und «Hacking Team» sollte für die Software ein Vertrag über drei Jahre abgeschlossen werden. Rund ein halbes Jahr nach der Lieferung ist nun fraglich, was damit geschehen wird.

«Galileo» hat Hintereingang

Ruef hat sich einzelne Teile des veröffentlichten Programmcodes näher angeschaut und dabei Hinweise auf eine sogenannte Backdoor festgestellt, die dem Hersteller der Software den Fernzugriff auf «Galileo» ermöglicht. Die Mailänder Firma hätte also die Möglichkeit gehabt, die Zürcher Kantonspolizei und andere Kunden bei ihrer Überwachungstätigkeit zu überwachen.

«Hacking Team» weist diesen Vorwurf in ihrer Mitteilung klar zurück. Für Ruef ist klar: «Der Einsatz dieser Software ist eines Rechtsstaates unwürdig und technologisch bedenklich. Überwachungssoftware, die polizeilich eingesetzt wird, muss einer sehr strengen Qualitätskontrolle unterliegen.» Bei einer ausländischen Firma sei dies für Schweizer Behörden jedoch kaum möglich. Genau diese Erfahrung hat die Zürcher Kantonspolizei nun gemacht, und dafür teuer Lehrgeld bezahlt. «Mit dieser Anschaffung wurden 500,000 Euro in den Sand gesetzt», sagt Ruef.

Erledigt haben dürfte sich das Thema der Überwachung von PCs von Personen, die im Verdacht stehen, schwere Verbrechen zu begehen, jedoch nicht. Mit der vom Parlament beschlossenen Revision des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs (Büpf) soll dafür eine saubere rechtliche Grundlage geschaffen werden. «Ich bin nicht komplett gegen den Einsatz von Trojanersoftware durch die Behörden. Aber die technischen, rechtlichen und ethischen Anforderungen sind in diesem Bereich enorm hoch», sagt Ruef. Staatstrojaner müssten aus seiner Sicht deshalb zwingend im Inland programmiert werden, und von staatlichen Stellen sehr genau überprüft werden, bevor sie eingesetzt werden.