KaPo Zürich kauft bei «Hacking Team» ein

7. Juli 2015

Die Kantonspolizei Zürich hat bei der Softwarefirma «Hacking Team» in Mailand für 486,500 Euro die Software «Remote Controlled System» (RCS 9, Codename «Galileo») gekauft. Mit diesem Trojaner können Desktops mit den Betriebssystemen Windows, OS X und Linux sowie mobile Geräte unter Android, Blackberry, iOS oder Windows Phone angegriffen werden. Mit «Remote Controlled System» wird volle Kontrolle über das Zielsystem erhalten, so können etwa Dateien, z. B. Videos, installiert oder Tastatureingaben herausgelesen werden u.s.w.

HT S.r.l.
Sede legale e operativa: Via della Moscova,13 – 20121 Milano – Tel: +39.02.29.06.06.03
e-mail: info@hackingteam.it – web: http://www.hackingteam.it – Fax: +39.02.63118946
P.IVA: 03924730967 – Capitale Sociale: € 223.572,00 i.v.
N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

KANTONSPOLIZEI ZURICH
8004 Zurich
Polizeikaserne
Kasernenstrasse 29
CH-8004 Zurich
SWITZERLAND

Milan, December 24th, 2014

Invoice no. 072/2014

Ref.: Our Offer no. 20140203-006.ES-REV06
Your Order no. # 3100/14/015

Remote Control System Galileo	€ 486.500,00
Total Amount	**€ 486.500,00**

VAT does not apply in accordance with Italian Presidential Decree 633/72, art. 7

Terms of payment:
Within 19/01/2015
Bank fees charged to the customer

By wire bank transfer to:
HT S.r.l. - Intesa San Paolo SPA - Fil. Imprese Milano Città Centro IBAN IT 78 P 03069 09420 100000000781 BIC/SWIFT Code: BCITITMMXXX

Am 14. Oktober 2013 um 13:40 Uhr hat Bernhard Weder von der Technischen Ermittlungsunterstützung TEU der Kantonspolizei Zürich per Mail mit dem «Hacking Team» Kontakt aufgenommen und den Kauf eingeleitet. Entsprechende Belege tauchten auf, nachdem am Wochenende vom 5. Juli 2015 rund 450 Gigabyte Daten aus dem Firmennetz von «Hacking Team» kopiert und im Internet veröffentlicht wurden. Neben umfangreichem E-Mail-Verkehr und Kundenlisten mit Bestellinformationen war auch der gesamte Source Code von RCS 8 (Codename «Da Vinci») und RCS 9 (Codename «Galileo») in diesem Fundus.

Durch SQL-Injection könnte im «Remote Controlled System» ein Backdoor installiert werden, wodurch das «Hacking Team» Zugriff auf alle Geräte der Strafverfolger und der überwachten Personen bekäme. Da jetzt aber alle Daten öffentlich sind, kann jedermann ein Backdoor installieren. Die Firma «Hacking Team» hat auch umgehend alle Kunden aufgefordert, «Galileo» nicht mehr zu verwenden.

Am Abend des 7. Juli 2015 wurde der Erwerb von «Galileo» bestätigt. Gemäss Medienmitteilung der Kantonspolizei Zürich habe im Jahr 2013 die zuständige Staatsanwaltschaft in zwei Verfahren von Betäubungsmittelkriminalität und Geldwäscherei die Überwachung verschlüsselter Internetkommunikation mittels einer speziellen Software angeordnet. Der Preis nur für die Software betrug somit rund 250,000 Franken pro Überwachung. Gemäss dem Sprecher des Obergerichts hat das Zwangsmassnahmengericht seit 2011 «eine kleine einstellige Zahl» von Trojanereinsätzen bewilligt. Am 9. Juli 2015 hat die Kantonspolizei Zürich mitgeteilt, dass «Galileo» nicht mehr eingesetzt werde.

Der Einsatz von «Galileo» ist problematisch, weil es in der Schweiz noch keine gesetzlichen Grundlagen für Staatstrojaner gibt und weil Telefonüberwachungen über den Dienst ÜPF abgewickelt werden müssten. Gemäss Art. 1 BÜPF gilt dieses Bundesgesetz für die Überwachung des Post- und Fernmeldeverkehrs, die angeordnet und durchgeführt wird im Rahmen eines Strafverfahrens des Bundes oder eines Kantons. Der vorgeschriebene offizielle Weg über den Dienst ÜPF wird aber offensichtlich umgangen, wenn Staatsanwaltschaften oder gar die Polizei selbständig und heimlich Trojaner beschaffen und einsetzen.

Ganz generell scheint man in Zürich bei der Fernmeldeüberwachung eigene ungesetzliche Wege zu gehen. Am Frühjahrstreffen 2015 der «Digitalen Gesellschaft Schweiz» wurde die «Überwachung Server» vorgestellt, bei welcher Echtzeitüberwachungen ohne Genehmigungsverfahren durchgeführt werden. Diesbezügliche Fragen an das Obergericht des Kantons Zürich vom 20. März 2015 wurden nur dahingehend beantwortet, dass keine Auskunft erteilt werden könne.

Eine Woche nach dem Super-GAU für «Hacking Team» hat die Sonntagspresse am 12. Juli 2015 eine erste Bilanz aus Schweizer Sicht gezogen: Schon 2011 interessierte sich ein Vertreter der Waadtländer Kantonspolizei für den Trojaner der Mailänder. Später bekundete auch die Genfer Kriminalpolizei Interesse. Der Dienst Überwachung Post- und Fernmeldeanlagen (Dienst ÜPF) lud Im Juli 2011 das «Hacking Team» für eine Präsentation der Software ein. Vor allem auch Private wollten mit den Mailändern ins Geschäft kommen. Ein Lausanner Unternehmen etwa schloss mehrere Geschäfte mit «Hacking Team» ab, ein Broker aus Zug, eine kleine Dienstleistungsfirma im Bereich Sicherheit und Verteidigung, suchte den Kontakt mit Hacking Team, um die Spionage-Software zusammen mit einem Partner nach Macau zu verkaufen. Eine Privatdetektei an der Zürcher Bahnhofstrasse wollte sich 2011 die Spionage-Software zulegen. Pikant ist, dass sich auch der in die Kasachstan-Affäre verwickelte private US-Geheimdienst Arcanum mit Sitz in Zürich um das Spionage-Produkt bemühte. Am 19. Juli 2015 zitierte die «Schweiz am Sonntag» ein Protokoll von «Hacking Team», wonach vier Anbieter von Trojanern ihre Produkte bei der Kantonspolizei Zürich präsentieren konnten.

Zwei wichtige Erkenntnisse offenbart diese Geschichte: Wird der Telefon- oder E-Mail Verkehr einer Zielperson gehackt, egal ob durch Private oder durch den Staat, gibt es jede Menge Dritte, welche ebenfalls mitgehackt werden und zu Schaden kommen können. Aus den Unterlagen des «Hacking Team» geht nicht hervor, welche Interessenten Trojaner von anderen Anbietern beschafft haben. Das Interesse ist auf jeden Fall gewaltig.

Zürich evaluierte mehrere Trojaner

Wer heute schon Trojaner einsetzt, verspottet unseren Rechtsstaat

Aushorchen nur mit Bewilligung

Galileo entdeckt gar nichts mehr

Alle Mails von Hacking Team

Erster E-Mail Kontakt

Polizei kauft Spionagesoftware bei Firma, die gehackt wurde

Dubiose Deals und teure Trojaner

Medienmitteilung Kantonspolizei Zürich

Folien Vortrag «Digitalen Gesellschaft Schweiz»

Möglichkeiten und Grenzen der digitalen Forensik

Unbekannte veröffentlichen Daten von Spionagesoftwarefirma