

RA Emanuel Schach, Kaiserstraße 37, 60329 Frankfurt/Main

Staatsanwaltschaft Wiesbaden
Mainzer Straße 124
65189 Wiesbaden

Kaiserstraße 37
60329 Frankfurt am Main
Telefon: (0 69) 91 30 34 25
Mobil: (01 72) 68 48 505
Telefax: (0 69) 28 55 41 + 28 55 71
E-Mail: info@ra-schach.de
Im Netz: www.ra-schach.de

Gerichtsfach 568

In Bürogemeinschaft mit:
Björn Vogel, Rechtsanwalt
Martin Breunig, Rechtsanwalt

Strafanzeige

Mein Zeichen (bitte immer angeben):

0311/2011 Piratenpartei Hessen - Strafanzeige
--

sta01

Datum
16. November 2011

Sehr geehrte Damen und Herren,

in der vorbezeichneten Angelegenheit zeige ich an, dass mich der Landesverband Hessen der Piratenpartei Deutschland, vertreten durch den Vorstand, mit der Wahrnehmung seiner rechtlichen Interessen beauftragt hat. Eine auf mich lautende Vollmacht füge ich in Kopie bei.

Wie Sie sicherlich der Presse- und Medienberichterstattung der vergangenen Wochen entnommen haben, hat der Chaos Computer Club (CCC) aufgedeckt, dass in einer Reihe von Bundesländern Ermittlungsbehörden, namentlich die Landeskriminalämter, im Rahmen von Ermittlungsverfahren nach der StPO ein Computerprogramm der Firma DigiTask zum Einsatz bringen, das eine grundgesetzwidrige Onlinedurchsuchung durchführt. Diese Software muss von Polizeibeamten heimlich auf dem PC/Notebook des Beschuldigten installiert werden, wozu unter anderem Beamte in die Räumlichkeiten eines Tatverdächtigen eindringen und dort dessen Computersystem heimlich mit der Schadsoftware infizieren.

Diese Erkenntnisse haben im Verlaufe der letzten Wochen zu einer bundesweiten öffentlichen und politischen Diskussion geführt. Auch das hessische Innenministerium hat mittlerweile eingeräumt, ein solches Programm der Herstellerfirma DigiTask eingesetzt zu haben.

Die Analyse des CCC zeigt, dass das von der Fa. DigiTask stammende Computerprogramm neben der Überwachung der Skype-Telefonie (also der eigentlichen Quellen-TKÜ) außerdem eine Aufzeichnung und Weiterleitung von Browser-Screenshots durchführt. Die Software ist nach den Erkenntnissen des CCC außerdem dazu in der Lage, über das Netz weitere Programme nachzuladen und ferngesteuert zur Ausführung zu bringen. Eine Erweiterbarkeit mit Blick auf das Durchsuchen, Schreiben, Lesen sowie Manipulieren von Dateien ist vorgesehen. Sogar ein digitaler großer Lausch- und Spähangriff ist möglich, da das Programm erlaubt, ferngesteuert auf das Mikrofon, die Kamera und die Tastatur des Computers zugegriffen wird.

Seit der Entscheidung des BVerfG zur sog. Onlinedurchsuchung vom 27. Februar 2008 (Az.: 1 BvR 370/07 und 1 BvR 595/07) ist es jedenfalls juristisch offensichtlich, dass derartige Maßnahmen zweifelsfrei unzulässig sind (vgl. Albrecht, JurPC Web-Dok. 59/2011).

Auch hat das Landgericht Landshut in einem bundesweit viel beachteten Beschluss vom 20. Januar 2011 (Az.: 4 Qs 346/10; Az. der StA Landshut: 45 Js 11552/08) das dargelegte Vorgehen beanstandet und für rechtswidrig erklärt. Dennoch wurde der Einsatz des Schadprogramms laut entsprechender Medienberichte offenbar unverändert fortgesetzt.

Bereits mit dem Urteil des BVerfG vom 27. Februar 2008 hätten die in der hessischen Landesregierung politisch wie auch juristisch Verantwortlichen die Pflicht gehabt, das Programm zurückzurufen oder zumindest anzuordnen, die Software nicht (mehr) einzusetzen, sollte diese bis dahin bereits eingesetzt worden sein. Offenbar ist aber genau das Gegenteil geschehen. Nach allen derzeit vorliegenden Informationen ist der Kauf des Programms sogar erst nach der Entscheidung des Bundesverfassungsgerichts erfolgt, mithin zu einem Zeitpunkt, als eindeutig und auch für die Exekutive bindend festgestanden hat, in welchem eingeschränktem Rahmen der Einsatz von solchen Spähprogrammen überhaupt nur zulässig sein kann.

Das heimliche Installieren der Software auf den Computern von Tatverdächtigen sowie das Ausspähen von Inhalten und Daten, die nicht aus einer Internettelefonie stammen, verstößt demzufolge gegen die Strafvorschriften der §§ 202a, 202b und 202c StGB.

Die Verantwortlichen, die diese Maßnahme angeordnet bzw. durchgeführt haben, haben sich unter Überwindung einer Zugangshürde zunächst Zugang zu Daten verschafft, die gegen unberechtigten Zugang besonders gesichert waren (§ 202a StGB). Eine Zugangssicherung im Sinne dieser Norm besteht bereits dann, wenn sich die Hardware in verschlossenen Räumen befindet (Fischer, StGB, § 202a, Rn. 9). Ein hohes Sicherheitsniveau ist nicht erforderlich. Es genügt ferner, dass beim Start des Betriebssystems die Eingabe eines Passwortes erforderlich ist (Schönke/Schröder, Strafgesetzbuch, § 202a, Rn. 8; Fischer, StGB, § 202a, Rn. 9a), was heutzutage bei nahezu jedem Rechner der Fall ist.

Dieses Vorgehen war auch unbefugt. Die handelnden Beamten können sich selbst dann nicht auf eine richterliche Gestattung berufen, wenn ein Ermittlungsrichter eine sog. Quellen-TKÜ angeordnet haben sollte. Denn die Besonderheit des eingesetzten Programms besteht gerade darin, dass es sich nicht auf den im Rahmen einer allenfalls zulässigen Quellen-TKÜ erlaubten Zugriff auf die Internettelefonie beschränkt, sondern gerade über diese (und damit die richterlicher Anordnung) hinausgeht.

Zusätzlich ist auch der Tatbestand der Vorschrift des § 202b StGB erfüllt, der allerdings gegenüber § 202a StGB subsidiär ist. Der vom LKA eingerichtete Trojaner überträgt jedenfalls Daten, die nicht Gegenstand einer richterlichen Anordnung sein können, weshalb auch das Merkmal des Sich-Verschaffens erfüllt ist.

Besonders schwer wiegt allerdings, dass bereits der Ankauf einer Software, die die dargelegten und offensichtlich gesetzlich nicht erlaubten Überwachungsmöglichkeiten eröffnet, zudem den Tatbestand des § 202c StGB erfüllt. Damit haben sich gerade auch diejenigen strafbar gemacht, die den Ankauf des Computerprogramms bei der Fa. DigiTask angeordnet und genehmigt haben, weil von vornherein klar war, dass diese Software in der Lage ist, eine rechtswidrige Onlinedurchsuchung zu ermöglichen und der Einsatz dieser Software im Rahmen von Ermittlungsverfahren auch deutlich macht, dass von Anfang an die Intention bestanden hat, die Software gezielt auch für gesetzlich nicht zulässige Überwachungszwecke einzusetzen.

In diesem Zusammenhang ist vor allem auf die Berichterstattung der Frankfurter Rundschau in ihrer Online-Ausgabe (<http://www.fr-online.de/politik/bundestrojaner-die-privaten-hinterdem-bundestrojaner,1472596,10985154.html>) hinzuweisen. Dort wird vom der Zeitung vorliegenden Schriftverkehr zwischen der Herstellerfirma DigiTask, dem bayerischen Innenministerium, den Oberlandesgerichtspräsidenten und den Generalstaatsanwälten über das hier interessierende Programm berichtet. Danach soll die Leistungsbeschreibung ausdrücklich alle jetzt als rechtswidrig gebrandmarkten Spionagefähigkeiten umfasst haben. Daraus folgt, dass die Leistungsbeschreibung die Rechtswidrigkeit des Programms ausdrücklich aufzeigt. Hieraus folgt der nahe liegende Verdacht, dass neben der Herstellerfirma in Hessen offenbar auch der seinerzeitige Innenminister, Volker Bouffier, sowie sämtliche sonst in Entwicklung, Erwerb und Einsatz involvierten Personen von den verfassungswidrigen Überwachungsfunktionen des Trojaners wussten.

Dabei wird nicht verkannt, dass diese Erkenntnisse unmittelbar nur die Verantwortlichen in Bayern betreffen. Indes hat das Landeskriminalamt Hessen mittlerweile eingeräumt, ein Spähprogramm des gleichen Herstellers, DigiTask, verwendet zu haben. Dies jedenfalls teilte der hessische Datenschutzbeauftragte auf eine Nachfrage meiner Mandantschaft mit. Eine Kopie dieser E-Mail füge ich anliegend bei. Im Weiteren kann als sicher unsterstellt werden,

dass die Firma DigiTask auch gegenüber den hessischen Behörden eine umfassende und anschauliche Beschreibung sämtlicher Möglichkeiten des verwendeten Programms vorgelegt hat. Für diese Annahme spricht bereits die allgemein bekannte Tatsache, dass bei allen Herstellern von Produkten derartige Beschreibungen gang und gäbe sind. Zudem kann es nach allgemeiner Lebenserfahrung als nahezu sicher ausgeschlossen gelten, dass ein Unternehmen gegenüber unterschiedlichen Kunden unterschiedliche Präsentationsmethoden nutzt.

Nach alledem besteht ein erheblicher Tatverdacht dahingehend, dass diejenigen Personen, die am Einsatz des Trojaners mitgewirkt haben, diejenigen, die ihn angeordnet haben, sowie diejenigen, die den Erwerb dieses Computerprogramms angeordnet haben, sich strafbar gemacht haben.

Zum Kreis der mutmaßlichen Täter gehören deshalb insbesondere der damalige Innenminister Volker Bouffier, die beteiligten Beamten des Innenministeriums und des Landeskriminalamts.

Namens und in Vollmacht meiner Mandantschaft erstatte ich daher Strafanzeige und bitte um die Einleitung eines Ermittlungsverfahrens und die Aufnahme sachdienlicher Ermittlungen im Hinblick auf alle in Betracht kommenden Personen unter allen denkbaren rechtlichen Aspekten.

Sollten Ermittlungen nicht aufgenommen werden, obwohl ohne Zweifel ein hohes Maß an Tatverdacht besteht, würde meine Mandantschaft davon ausgehen, dass die Justiz in Hessen nicht ohne Ansehung der Person ermittelt, sondern vielmehr nach politischen Kriterien bzw. Vorgaben.

Ich darf Sie in jedem Fall bitten, mich über den Verlauf des Ermittlungsverfahrens zu unterrichten.

Mit freundlichen Grüßen

Emanuel Schach
-Rechtsanwalt-