

XXIV. GP.-NR

9518 /J

19. Okt. 2011

**Anfrage**

der Abgeordneten Vilimsky, Herbert  
und weiterer Abgeordneter  
an die Bundesministerin für Inneres  
betreffend deutsche Spionagesoftware in Österreich

Der Zeitung "Die Presse" vom 13.10.2011 konnte entnommen werden:

*„Entwickler sagt: "Staatstrojaner" auch in Österreich*

*Affäre. Entwickler der Spionagesoftware will seine Produkte auch hierzulande an Behörden verkauft haben.*

*(Wien/Köln) Die Firma DigiTask ist der Urheber jener Spionagesoftware, die deutsche Behörden als sogenannten "Staatstrojaner" zur Überwachung der Computer von Verdächtigen einsetzen. Nun bestätigte die Firma der "Presse" eine Meldung der "Deutschen Welle", dass die Produkte des Hauses nicht nur für die Regierung des eigenen, sondern auch für jene von Nachbarländern zum Einsatz kommen.*

*"Ja, wir beliefern Behörden im Einflussbereich Wiens", sagt DigiTask-Sprecher Winfried Seibert zur "Presse". Der prominente Kölner Anwalt, der Ex-Siemens-Chef Heinrich von Pierer in der Schmiergeldaffäre vertrat, berät nun die ins Schussfeld geratene Softwareschmiede aus der hessischen Kleinstadt Haiger. Er, Seibert, könne jedoch nicht sagen, ob die nach Österreich verkauften Überwachungssysteme mit jenen aus Deutschland ident seien oder nicht. Auch an wen man in Österreich verkauft hatte, wollte er nicht sagen: Betriebsgeheimnis.*

*Interessant ist das unter anderem deshalb, weil Mitglieder der deutschen Hacker-Gruppe Chaos Computer Club (CCC) zuletzt behaupteten, das Programm könne weit mehr, als es das Gesetz eigentlich erlaube. Zusätzlich zur Überwachung des Online-Telefondienstes Skype fertige das Programm nämlich Bildschirmkopien ("Screenshots") an und sei zudem in der Lage, weitere Schadsoftware, etwa zur Spionage, ferngesteuert auf den infizierten Computer zu laden. Der "Presse" sagte Seibert, dass das Unternehmen nur Funktionen in die Programme implementiere, die zum Zeitpunkt der Entwicklung rechtlich gedeckt sind. "Wir lassen uns das von den beauftragenden Behörden sogar schriftlich geben. Darauf müssen wir dann vertrauen." Unausgesprochener Nebensatz: Sagt der staatliche Auftraggeber dabei nicht die Wahrheit, sei das dessen Angelegenheit.*

*In Österreich gibt es nur sehr wenige Einheiten, die als Auftraggeber für solch eine Software infrage kommen. Neben den Nachrichtendiensten des Heeres sind das die Sondereinheit Observation (SEO) des Innenministeriums, das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT) sowie das Bundeskriminalamt (BK). Ebendort jedoch schließt man den Einsatz von Produkten der Firma DigiTask aus. "Dafür gibt es keine rechtliche Grundlage."*

*Mehr als nur abhören*

*Wie in Deutschland argumentieren Datenschützer und Grundrechtsexperten auch hierzulande, dass Online-Überwachung mithilfe von heimlich eingebrachten Computerprogrammen weit über die richterlich genehmigbare Telekom-Überwachung hinausgehe. Hans Zeger von der Arge Daten: "Das ferngesteuerte Durchstöbern eines Computers erlaubt dem Staat Einblicke in die intimsten Gedanken und Bereiche seiner Bürger.""*

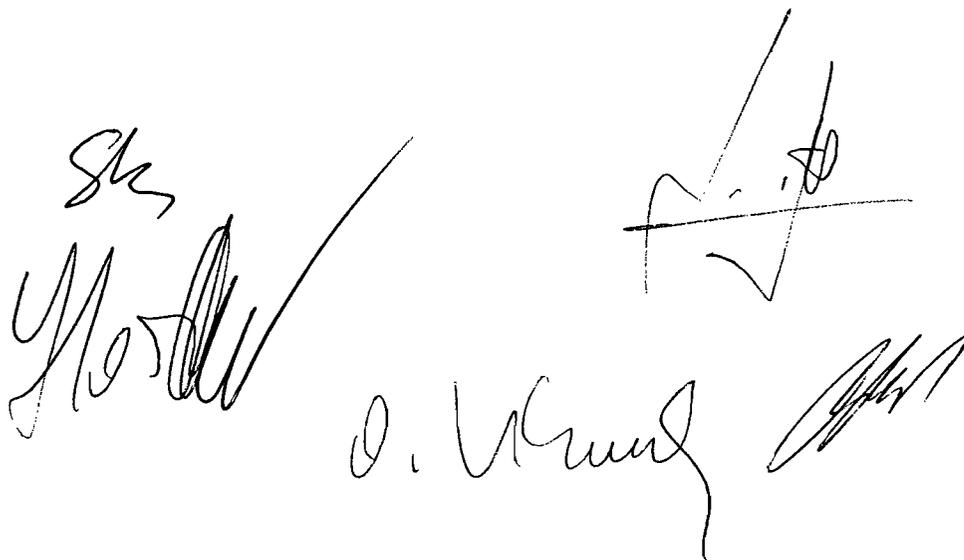
Die „Frankfurter Allgemeine“ berichtete am 8.10.2011 dazu folgendes:  
(<http://www.faz.net/aktuell/chaos-computer-club-der-deutsche-staatstrojaner-wurde-geknackt-11486538.html>)

„ (...) Für besonders gefährlich halten die Hacker eine Funktion, mit der derjenige, der die Befehlsgewalt über den Trojaner hat, ein beliebiges Programm über das Internet auf den infizierten Computer laden und ausführen lassen kann, ohne dass der Nutzer davon etwas mitbekommt. Gerade diese Funktion aber darf es in der Quellen-TKU nicht geben. „Mit dem Nachladen von Programmteilen lassen sich zum Beispiel Mikrofon oder Kamera am Computer als Raumüberwachungswanze nutzen.“ Zudem könnten durch die Nachlade-Funktion nicht nur die Festplatte durchsucht und Dateien heruntergeladen werden, sondern es könnten sogar Dateien über das Netz auf den Computer geschoben werden. Bilder oder Filme, die belastendes Material zeigten, könnten auf diesem Weg auf Computern plaziert werden. Die Beweissicherheit sei, sobald ein Computer infiziert sei, somit nicht mehr gegeben. (...)“

In diesem Zusammenhang richten die unterfertigten Abgeordneten an die Bundesministerin für Inneres folgende

### Anfrage:

1. Hat Ihr Ressort diese Spionagesoftware angekauft?
2. Wenn ja, wann?
3. Wenn ja, wie hoch waren die Kosten dafür?
4. Gab es eine Ausschreibung für dieses Projekt?
5. Wenn ja, wann?
6. Wenn ja, wer hat sich beworben?
7. Was kann diese von Ihrem Ressort erworbene Spionagesoftware?
8. Aus welchen Gründen wurde diese Spionagesoftware angekauft?
9. Welche Einheiten, Dienste und sonstige Stellen Ihres Ressorts haben die Spionagesoftware erhalten?
10. Wer hat diese Spionagesoftware getestet?
11. Wurde diese Spionagesoftware bereits verwendet?
12. Wenn ja, in wie vielen Fällen?
13. Wenn ja, in welchem Zusammenhang?
14. Wenn ja, auf welcher rechtlichen Basis?
15. Welche Einheiten, Dienste und sonstige Stellen Ihres Ressorts haben die Spionagesoftware in Verwendung?

The image shows four handwritten signatures in black ink. The signatures are written in a cursive style. The first signature on the left is the most prominent and appears to be 'G. H. ...'. The second signature is smaller and less legible. The third signature is also smaller and less legible. The fourth signature is the most legible and appears to be 'D. ...'.