

# Bundestrojaner beim Afghanen?



Stefan Krempl schreibt bei [Heise](#): „Der Bundesnachrichtendienst (BND) hat Berichten zufolge eine heimliche Online-Durchsuchung beim afghanischen Handels- und Industrieminister [Amin Farhang](#) durchgeführt, bei der auch die Kommunikation mit einer Spiegel-Reporterin erfasst worden sein soll.“ Ich glaube vorsichtshalber erst einmal gar nichts. Weiter heißt es: „Nach Informationen der Nachrichtenagentur ddp war es dem BND gelungen, mit Hilfe eines Trojaners auf der Festplatte von Farhang ein Spähprogramm zu installieren.“ Was sagen die Quellen?

Krempl zitiert sich in [typischer Manier](#) selbst: „Die monatelange Observation der Journalistin zwischen Juni und November 2006, die das Nachrichtenmagazin am Wochenende bekannt machte, war demnach offenbar ein ‚Nebenprodukt‘ der Bespitzelung des Spitzenpolitikers“. Das – der zweite Satz des Artikels – suggeriert, als sei die Observation eine „Online-Durchsuchung“ gewesen. Das war aber mitnichten so. Hinter dem verlinkten [„bekannt geworden“](#) verbirgt sich ein Artikel von Spiegel Online, in dem es lediglich heißt: „Der Bundesnachrichtendienst (BND) hat monatelang die E-Mail-Korrespondenz der 42-jährigen SPIEGEL-Reporterin mit dem afghanischen Politiker überwacht und mitgeschnitten.“ Das

Abhören des Kommunikation hat mit einer Online-Durchsuchung nichts zu tun und ist ein Kinderspiel, wenn die Beteiligten ihre Korrespondenz nicht verschlüsseln. Typisch für das Niveau deutscher Recherche ist auch, dass das „Opfer“ [Susanne Koelbl](#) meinte, an einen afghanischen Politiker Postkarten schreiben zu müssen und „nicht ahnte“, dass auch andere Leute die lesen wollten – und das natürlich getan haben. Die Kollegin antwortet übrigens nicht auf meine E-Mails zum Thema.

Die [Welt online](#) berichtet: „...wurde zum Abschöpfen des E-Mail-Verkehrs zwischen der „Spiegel“-Journalistin Susanne Koelbl und dem Politiker aus Kabul zwischen Juni und November 2006 ein ‚Trojaner‘ eingesetzt. Das Spionageprogramm, für dessen Einsatz das Bundesverfassungsgericht unlängst hohe Hürden gesetzt hat, sei auf der Festplatte des Computers des Afghanen installiert worden, hieß es. Dabei seien auch ‚intime Bereiche‘ der persönlichen Lebensführung der Journalistin ausgespäht worden.“

Da haben wir's. Jede Wette, dass der BND den physischen Zugriff auf den Rechner hatte und entweder einen Keylogger oder so etwas wie [EnCase® Field Intelligence Model](#) eingesetzt hat. [Vgl. c't: [Der weisse Spion](#)]. Die [Stattzeitung für Südbaden](#) erwähnt ein weiteres interessantes Detail: Der heutige afghanische Wirtschaftsminister, ein ehemaliges Mitglied der deutschen Grünen und „langjährig in Nord-Rhein-Westfalen ansässig,... (...) Die Ausspähung geschah ab 2006 per Trojaner. Also existiert schon ein funktionsfähiges Modell. Dabei wurde offiziell immer wieder geächzt, wie teuer so was sei und wie schwer zu installieren.“ Und genau das ist die Pointe: Der berüchtigte „Bundestrojaner“ wird im öffentlichen Diskurs als heimlicher Zugriff über das Internet verstanden. Darum geht es hier aber gar nicht, sondern um ein Spionageprogramm, dass auf der Festplatte installiert worden war. Und so etwas ist gar nicht teuer und auch nicht kompliziert und existiert natürlich schon in verschiedenen Varianten.

Farhang hat das selbst bestätigt, wie die [FTD](#) meldet: „Er habe erfahren, dass der BND *seinen Computer im Büro* manipuliert habe. Er gehe davon aus, dass nicht nur einer seiner Computer für wenige Monate überwacht worden sei, wie der BND behauptete. „Ich habe das Vertrauen verloren und nehme an, dass deutsche Agenten alle meine Telefonate und E-Mails noch immer überwachen.“ Quod erat deminstrandum.

Falsch im Heise-Bericht ist definitiv: „Im Januar war bekannt geworden, dass der Geheimdienst bereits rund 60 Mal heimlich Zielrechner Verdächtiger im Ausland über das Internet ausgeschnüffelt haben soll“. Soll. Nicht hat. Dass das gar nicht stimmt und auch im damaligen [Focus-Artikel](#) falsch war, hat man mir mir telefonisch bestätigt. Es soll damals – durch den BND – nur *eine* „Online-Durchsuchung“ gegeben haben, und dafür auch nur eine Quelle. Es ist also gar nichts verifizierbar.