Miszellen zum Überwachungsstaat Deutschland

Die Medien in Deutschland stecken immer noch voller Vodoo, sobald es um Computer und Internet geht. Das macht manchmal selbst vor IT-affinen Portalen wie Heise oder Golem nicht halt. Die Nutzer tun ihr Übriges, um den jeweiligen Quatsch zu perpetuieren. „Regret the Error“ ist ohnehin kaum vorgesehen.

Man lese die folgenden Sätze: „Deutsche Geheimdienste können PGP entschlüsseln“ (Golem). Ein Nutzer hat im Golem-Forum gleich kommentiert: „Vermutlich eine Ente“.

Genau so ist es. Es geht um eine Antwort der Bundesregierung auf eine Anfrage mehrere Abgeordneter der Linken, ob die Technik deutscher Übewachungsbehörden in der Lage sei, „verschlüsselte Kommunikation (etwa per SSH oder PGP) zumindest teilweise zu entschlüsseln und/oder auszuwerten?“

So fragt man natürlich nicht: Man kann nicht SSH oder PGP in einem Atemzug nennen. Das sind Äpfel und Gummibärchen. Dementsprechend dämlich und missverständlich ist die Antwort der Bundesregierung: „Ja, die eingesetzte Technik ist grundsätzlich hierzu in der Lage, je nach Art und Qualität der Verschlüsselung.“

Das kriegen natürlich Leute mit einem geplegten IT-Halb- und Viertelwissen gleich in den falschen Hals. Fefe schreibt dazu: „Weil mir hier gerade vermehrt gemailt wird, die Geheimdienste könnten PGP entschlüsseln: nein, können sie nicht. Was sie tun können ist Passwörter durchprobieren. Die sind direkt gefragt worden, ob sie PGP entschlüsseln können, und die Antwort war „im Prinzip haben wir die nötige Software dafür“. Die nötige Software kann man kaufen, die probiert Passwörter durch. Bessere Angriffe auf PGP sind nicht bekannt. Insofern haltet mal bitte alle die Füße still.“

Quod erat demonstrandum. Genau das Gegenteil der Überschrift von Golem ist richtig: Deutsche Geheimdienste können PGP *nicht* entschlüsseln. Golem hat mittlerweile einen klärenden Artikel nachgeschoben: „Symantec hat sich zu den Aussagen der Bundesregierung geäußert, nach denen Geheimdienste in der Lage seien, SSH oder PGP zu knacken oder zu umgehen. Mathematisch gesehen sei kein wirksamer Angriff bekannt.“

Hemker: „Wir hatten in der Vergangenheit ja schon oft Meldungen, laut denen PGP angeblich geknackt wurde. Das waren aber meistens Brute-Force-Attacken, bei denen schwache Passphrases für den Schlüsselzugriff geknackt wurden. Es war niemals ein mathematischer Angriff auf die Kryptografie selbst.“

Auch der Heise-Artikel zum Thema war zunächst missverständlich; dort aber bekommen die Autoren meistens gleich jeden falschen Punkt von den Lesern um die Ohren gehauen.

Man kann dem von Golem befragten Mathematiker Thomas Hemken nur zustimmen: „Unklar bleibe, was sie [die Bundesregierung] genau meinten.“ Die Bundesregierung wirft in diesem Fall genauso Nebelkerzen wie im Fall der sogenannten „Online-Durchsuchung“ oder hat einfach keine Ahnung. Vermutlich sogar beides.