



2012/11 Lifestyle

<https://jungle.world/artikel/2012/11/krieg-der-hacker>

Die Verhaftung von Mitgliedern der Hacker-Gruppe LulzSec

Krieg der Hacker

Von **Elke Wittich**

Nach der Verhaftung von Mitgliedern der Gruppe LulzSec stellt sich heraus, dass das FBI Informanten in der internationalen Hacker-Szene hat. In dem Spionagethriller, in dem es um gehackte Daten, Geheimdokumente, Verrat und Verschwörung geht, taucht wieder der Name von Julian Assange auf.

Unauffällig und ein bisschen heruntergekommen – wer wollte, konnte sich schon im Juli 2011 per Google Streetview das in der New Yorker Lower Eastside gelegene 14-stöckige Mietshaus ansehen, in dem AnonymouSabu, wie sich der Anführer der Hacker-Gruppe LulzSec nannte, lebte. Kurz zuvor hatte eine Hacker-Gruppe namens TeaMp0isoN eigenen Angaben zufolge Sabus persönliche Daten gedoxt, also zusammengetragen und veröffentlicht. Vom Klarnamen über die besuchte Highschool bis hin zur Wohnadresse war die Identifizierung nach dem, was man heute weiß, vollständig gelungen. Sabu, der in Wirklichkeit Xavier Hector Monsegur heißt, zeigte sich jedoch vollkommen unbeeindruckt: Stoisch erklärte er wieder und wieder, es handele sich um eine Verwechslung und es sei höchst verwerflich, irgendwelche Namen willkürlich zu nennen und damit Unschuldige zu gefährden.

Als nun vergangene Woche führende Mitglieder von LulzSec verhaftet wurden, zeigte sich rasch, dass TeaMp0isoN recht gehabt hatte mit dem Verdacht, Sabu sei ein Informant des FBI. Klar wurde auch, dass der aus Puerto Rico stammende Monsegur im realen Leben nicht viel gemein hatte mit dem bekannten Hacker, der zu sein er vorgab. Der geheimnisumwitterte AnonymouSabu erwies sich nicht etwa als der weitgereiste Kosmopolit, den er so gern in seinen Tweets verkörperte, sondern als Sozialhilfeempfänger mit einer traurigen Lebensgeschichte. Als Hector 14 war, wurden sein Vater und seine Tante Iris wegen des Handels mit Heroin verhaftet. Der Jugendliche zog zu seiner Großmutter. Nachdem Iris 2010 erneut inhaftiert wurde, beantragte und erhielt Monsegur das Sorgerecht für seine beiden kleinen Nichten, das er auch nach der Freilassung ihrer Mutter behielt.

In der Nachbarschaft war Monsegur als rücksichtsloser Partymacher und gleichzeitig als hilfsbereiter Computernerd bekannt, der gern seine Hilfe anbot und unter anderem

behauptete, schlechte Kredit-Ratings ganz einfach in gute umwandeln zu können. Im Juni war er festgenommen worden. Zwei Fehler hatten das FBI laut einer Pressemitteilung schließlich auf Monsegurs Spur gebracht: Einmal hatte er sich in einem Online-Chat eingeloggt, ohne einen Anonymizer zu benutzen – und zusätzlich hatte er eine Website genannt, die er unter Kontrolle hatte. Als das FBI Monsegur einen Deal anbot, nahm der Hacker ihn ohne langes Zögern an. Von nun an lieferte er den Behörden Informationen über die Aktivitäten seiner ehemaligen Hacker-Kollegen. Die Alternative für den LulzSec-Anführer wären 124 Jahre und sechs Monate Gefängnis gewesen, sowie der Entzug des Sorgerechts für seine Nichten.

Sabu hatte in seinen Tweets immer wieder geschworen, das verhasste System mit allen Konsequenzen bekämpfen zu wollen. Vielleicht waren auch deswegen so wenige LulzSec-Mitglieder misstrauisch geworden, als er – nach seiner Verhaftung, wie man heute weiß – für rund zwei Monate verschwand. Dass Sabu, der normalerweise rund um die Uhr Tweets veröffentlichte, plötzlich schwieg, hatte zwar immer wieder zu Spekulationen geführt, zumal einige Personen festgenommen wurden, die mutmaßlich LulzSec angehörten, aber offenbar fühlten sich die restlichen Gruppenmitglieder sicher. Als Sabu dann wieder auftauchte, gab er sich radikaler und kompromissloser als je zuvor. Seine Behauptungen, er könne durch US-Ermittler nicht gefasst werden, weil er im Ausland wohne, untermauerte er durch Tweets in Fremdsprachen, unter anderem auf Deutsch, was bei seinen Freunde von LulzSec womöglich das Gefühl verstärkte, sicher vor Strafverfolgung zu sein.

Warum aber bot das FBI dem Spiritus Rector der Gruppe einen Deal an, statt einfach alle Beteiligten auf der Stelle zu verhaften? Eine mögliche Antwort könnte in einem zunächst weitgehend als lächerlich geltenden Hack vom Dezember vergangenen Jahres liegen. Betroffen davon war Stratfor, ein 1996 gegründetes US-Unternehmen, das sich auf die Auswertung von Nachrichten spezialisiert hat und Journalisten sowie internationalen Unternehmen gegen Gebühr geopolitische Analysen, Daten und einen kostenlosen Newsletter anbietet.

Am 24. Dezember 2011 hatten Hacker unter dem Codenamen »LulzXmas« insgesamt 200 Gigabyte Daten, unter anderem Passwörter und Kreditkarteninformationen, von den Stratfor-Servern gestohlen. Die Erklärung für den Hack war jedoch mindestens eigenartig: Stratfor sei eine Firma, die sich mit Datensicherheit beschäftige und deren Sicherheitsvorkehrung bestenfalls lax seien, daher sei es folgerichtig, das Unternehmen anzugreifen. Die gehackten Bankdaten werde man benutzen, um im Rahmen einer »Operation Robin Hood« eine Million Dollar an Wohltätigkeitsorganisationen zu spenden. Dabei hätte auch LulzSec klar sein müssen, dass eine solche Umverteilungsaktion für die Empfänger durch Rückbuchungen und Stornogebühren lediglich große Kosten verursachen würde.

Die Hacker von Anonymous distanzierten sich umgehend von dem Hack, und nicht nur aufgrund der eigenartigen Spendenpraxis: Sie erklärten Stratfor darüber hinaus zu einem Nicht-Ziel. Kurz nach dem Angriff veröffentlichten sie eine Erklärung, in der es hieß, für Stratfor als Medienunternehmen gelte die Pressefreiheit, »ein Prinzip, dem Anonymous hohen Wert beimisst«. Journalistische Projekte dürften nicht angegriffen werden. LulzSec und insbesondere AnonymouSabu wurden als »attention whores« und »möglicherweise agents provocateurs« bezeichnet. Was genau LulzSec mit dem Angriff auf Stratfor

bezwecken wollte, blieb rätselhaft.

Bis zum 27. Februar, als Wikileaks die aus dem Stratfor-Hack stammenden Informationen veröffentlichte. Dass sie ausgerechnet von der Whistleblower-Plattform in Umlauf gebracht wurden, könnte an einer E-Mail gelegen haben. Fred Burton, Vizepräsident von Stratfor und führender Sicherheits- und Terrorismusexperte der USA sowie Special Agent der mit dem Schutz von im Ausland lebenden Amerikanern beauftragten US-Bundesbehörde Diplomatic Security Service (DSS), hatte sich im Januar 2011 in einer E-Mail damit gebrüstet, Stratfor sei im Besitz von Dokumenten über ein Geheimverfahren gegen Julian Assange in den USA. Unter anderem liege einer Grand Jury ein »sealed indictment« vor, in dem Assange mehrere Straftaten vorgeworfen würden. Genau solche Beweise dürften für Julian Assange von größtem Interesse gewesen sein, der seit seiner Verhaftung immer wieder öffentlich erklärt hatte – zuletzt gegenüber dem italienischen Magazin L'Espresso –, in den USA werde im Geheimen daran gearbeitet, ihn auszuliefern und vor Gericht zu stellen. Beweise für diese Theorie hatte er jedoch nie liefern können.

Falls die E-Mail mit dem Text »Not for pub – We have a sealed indictment on Assange. Pls protect.« an Assange weitergeleitet worden wäre, wäre er sicher höchst alarmiert gewesen. Selbst wenn die Betonung des geheimen Charakters der Nachricht im Nachhinein so wirkt, als wolle man damit unbefugte Mitleser davon überzeugen, dass es sich um einen Vorgang von exorbitanter Brisanz handele, dürfte Assange nicht an der Echtheit der E-Mail gezweifelt haben. Der mutmaßlich von Assange persönlich betriebene Twitter-Account von Wikileaks hatte, so berichtete wired.com, LulzSec am 30. Dezember in einem kryptischen Tweet mit dem Text »rats for donavon.« darüber informiert, dass die Stratfor-Daten erfolgreich auf einen sicheren Server überspielt worden seien. Warum es dann noch fast zwei Monate bis zur Veröffentlichung dieser Daten dauerte, ist unklar. Stratfor gab lediglich eine Erklärung heraus, wonach Teile der publizierten Daten verändert worden sein könnten – ansonsten werde man sich zu dem Thema nicht weiter äußern. Bereits einen Tag nach der Veröffentlichung durch Wikileaks hatte die Bloggerin Rev. Magdalen ganz eigene Überlegung über den Stratfor-Hack verfasst: »Was würden Sie tun, wenn Sie Julian Assange wären und gerüchteweise davon erfahren hätten, dass Stratfor eine Kopie einer Anklage oder von Dokumenten, in denen dieses Schriftstück im Detail diskutiert wird, auf einem unsicheren Server verwahrt? Würden Sie nicht Ihre alten Freunde von Anonymous um Hilfe bitten, damit es in ihren Besitz kommt?«

Wie viele andere Unternehmen der Branche ist auch Stratfor dafür bekannt, hin und wieder gezielt falsche Informationen zu streuen, um beispielsweise die Verbreitungswege von Nachrichten studieren zu können. Dass die E-Mail mit der sensationellen Mitteilung von irgendeinem der zahlreichen Wikileaks-Unterstützer an Assange weitergeleitet werden könnte, hätte jemandem wie Burton eigentlich klar sein müssen – vielleicht wollten er oder das FBI auch genau das erreichen.

In den Anklageschriften gegen die verhafteten LulzSec-Mitglieder wird deutlich, dass das FBI die gesamte Kommunikation der Gruppe lückenlos verfolgt und dokumentiert hat, wobei teilweise nicht ausgeschlossen werden kann, dass die Beamten sogar selbst unter dem Namen von AnonymouSabu twitterten oder chatteten. So dürfte das FBI auch über den Stratfor-Hack im Voraus informiert gewesen sein und genau wissen, wer der Auftraggeber war – falls es einen gab.