Cyberfahnder-Newsletter 7 vom 28.07.2011

Boards und Internetermittlungen

Der letzte Newsletter in dieser Form liegt acht Monate zurück. Wollte ich mit dem Cyberfahnder Geld verdienen, wäre das unverzeihlich. Zuletzt habe ich auf das Arbeitspapier ▸ Eskalationen hingewiesen, ohne aber darauf nennenswerte Reaktionen erfahren zu haben. Entweder wird man mir in ein paar Jahren nachsagen, dass ich grob, aber dennoch mit feinem Gespür wichtige Entwicklungen voraus gesagt habe, oder ich werde einfach nur ein wirrer Spinner gewesen sein, was mir im wegen meiner Parteiergreifung für die Vorratsdatenspeicherung sowieso nachgesagt wird (▸ Bestandsdatenauskünfte und Rechtsschutzverweigerung).

In der Zwischenzeit haben Anonymous und LulzSec (▸ Sponti-Hacking: LulzSec) kräftig zugeschlagen und die These vom zunehmenden Hacktivismus bestätigt. Der Cyberfahnder hat sich rarer gemacht und reagiert nicht mehr tagesaktuell. Das war – aus persönlichen Gründen – überfällig, hat aber nicht dazu geführt, dass der Aufwand, der in dem Programm steckt, wirklich weniger wurde. Im Mai erschien unter dem Druck „Können Sie nicht mal ...“ die Präsentation ▸ Ermittlungen im Internet. Sie beschäftigt sich besonders mit der Frage, was die Ermittler im Rahmen der Strafverfolgung in Hackerboards dürfen. Da stecken umfangreiche Recherchen und viel Kopfarbeit drin und das Ergebnis ist noch ein Baukasten mit Lücken. Diese füllt jetzt der Aufsatz ▸ Verdeckte Ermittlungen im Internet.

Aktive Ermittlungen in Kommunikationsdiensten

Die Cardingboards haben Paget (▸ Cybercrime und politisch motiviertes Hacking. Über ein Whitepaper von François Paget von den McAfee Labs) und vor allem Ester und Benzmüller (▸ GData Whitepaper 2009. Underground Economy, ▸ Whitepaper 04/2010. Underground Economy - Update 04/2010) ausgiebig angesprochen. Ihre Brisanz ist mir dadurch endlich deutlich geworden (▸ Basar für tatgeneigte Täter).

Um Ermittlungen in diese Richtung zu führen, bedarf es aber nicht technischer, sondern kommunikativer Ermittlungen, die anonymisiert und legendiert sind. Das ist unter rechtsstaatlichen Bedingungen ausgesprochen heikel.

Um ihre Zulässigkeit und Grenzen geht es dem Aufsatz ▸ **Verdeckte Ermittlungen im Internet**. Er gibt einen Überblick über die wichtigsten Maßnahmen, die im Zusammenhang mit den Ermittlungen im Internet von Bedeutung sind. Sie reichen von den Auskünften von Providern und Diensten (zum Beispiel wegen Bestandsdaten) über die Beschlagnahme von E-Mails, technische Überwachungsmaßnahmen (Verkehrsdaten, Überwachung der Telekommunikation, Onlinedurchsuchung) bis hin zu der längerfristigen Beobachtung und Kommunikation mit Beschuldigten in Netzwerken, Foren und geschlossenen Hackerboards.

In seinem Urteil zur Onlinedurchsuchung hat das BVerfG 2008 neben das Grundrecht auf Kommunikationsgeheimnis einen weiteren Technikschutz gestellt und das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme formuliert. Beide bilden zusammen mit dem Grundrecht auf informationelle Selbstbestimmung den Rahmen, an dem sich strafverfahrensrechtliche Eingriffsermächtigungen messen lassen müssen.

In demselben Urteil befasst sich das BVerfG aber

auch mit der Frage, welche Handlungen den Strafverfolgungsbehörden im Internet gestattet sind, ohne dass sie messbar in die Grundrechte der Kommunikationpartner eingreifen. Das gilt auf jeden Fall für die Beschaffung frei zugänglicher Informationen im Internet, die Nutzung von Informationssammlungen und -diensten, soziale Netzwerke und Foren und das ausdrücklich auch in der Weise, dass die Tatsache verschwiegen wird, ein Strafverfolger zu sein (Fake Accounts). Bis zu diesen Schwellen sind die Ermittlungsmaßnahmen auf jedem Fall von der Ermittlungsgeneralkausel des § 161 Abs. 1 StPO umfasst.

Dazu benennt das Gericht ausdrücklich zwei Grenzen: Die Dokumentation der gesammelten Informationen, ihr Quervergleich mit anderen Informationen und ihre Auswertung verlangen dann nach einer besonderen Eingriffsermächtigung, wenn *sie eine besondere Gefahrenlage für die Persönlichkeit des Betroffenen* bedeuten würden.

Die zweite Grenze ergibt sich aus der Tiefe der Kommunikation, die mit Verdächtigen und Beschuldigten unter Verschweigen der Tatsache geführt wird, dass ihr Kommunikationspartner ein Strafverfolger ist und er *dabei ein schutzwürdiges Vertrauen des Betroffenen in die Identität und die Motivation seines Kommunikationspartners ausnutzt, um persönliche Daten zu erheben, die* <er> *ansonsten nicht erhalten würde*.

Deshalb ist eine kritische Auseinandersetzung mit der kriminalistischen List im Zusammenhang mit dem Einsatz Nicht offen ermittelnder Polizeibeamter (NoeP) und ihre Abgrenzung zum Verdeckten Ermittler nötig. Ihr Ergebnis ist, dass der NoeP nur in den zeitlichen Grenzen des § 163f StPO wegen zeitlich und sachlich umgrenzter Ermittlungsaufträge tätig werden darf. Sobald er in Kommunikationsdiensten im Internet einen bestimmten Beschuldigten längerfristig beobachtet, ist das nicht mehr von der Ermittlungsgeneralklausel des § 161 Abs. 1 StPO gedeckt und bedarf es eines gerichtlichen Beschlusses. Beobachtet er passiv oder nur im Zusammenhang mit allgemeinen Wortbeiträgen, ist die längerfristige Observation einschlägig (§ 163f StPO). Wenn er aktiv mit dem Beschuldigten kommuniziert, dann bedarf es einer Zustimmung zum Verdeckten Ermittler (§ 110b StPO).

Mit dem Aufsatz und Schlüssen betrete ich wieder einmal Neuland. Einerseits zeigt er die Möglichkeiten zu aktiven Ermittlungen auf, die bislang kaum genutzt werden, und andererseits auch ihre Grenzen. So sind nachhaltige personale Ermittlungen erst ab der Schwelle der „erheblichen Straftaten“ zulässig und der Einsatz von NoeP auf Scheinkäufe, die Identifikation von Beschuldigten oder auf den Zugriff beschränkt.

Ich wünsche mir eine rege Diskussion!

Mit freundlichen Grüßen

Dieter Kochheim (Cyberfahnder)