Trojaner gegen Rechtsextremisten

Ist der gezielte Einsatz von Trojanern gegen Rechtsextremisten durch deutsche Behörden legitim oder ist dieser abzulehnen? Bernd Carstensen, stellvertretender Vorsitzender des Bundes Deutscher Kriminalbeamter (BDK), spricht sich für eine Überwachung via Trojaner aus, während der Fachanwalt für IT-Recht Thomas Stadler diese rundweg ablehnt.

Das Aufdecken der sogenannten „Zwickauer Zelle“ hat eine neue politische Diskussion über die Dimension rechtsextremistischer Gewalttaten, die Rolle des Verfassungsschutzes bei der Überwachung der rechten Szene sowie das Verbot der NPD ausgelöst. Offensichtlich wurde die rechte Gewalt jahrelang entweder massiv unterschätzt, schlicht ignoriert oder gar geduldet. Das scheint ebenso für die Aktivitäten von Rechtsextremisten im Netz zu gelten.

Als erste konkrete Maßnahme kündigte Bundesinnenminister Friedrich einen Gesetzentwurf an, der die Einführung einer zentralen Neonazi-Datei vorsieht. Könnte zu den weiteren Überlegungen möglicherweise auch das gezielte Einsetzen von Trojanern gegen Rechtsextremisten gehören? Derzeit scheint ein solches Szenario zwar ausgeschlossen – nicht zuletzt, weil der Einsatz solcher Spionagesoftware erst kürzlich mächtig in Verruf geriet.

Prominente Befürworter des Einsatzes von Trojanern gibt es aber weiterhin. Dazu zählt Bernd Carstensen, der stellvertretende Vorsitzende des Bundes Deutscher Kriminalbeamter spricht sich auf politik-digital.de für die sogenannte Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) gegen Rechtsextremisten aus. Thomas Stadler, Fachanwalt für Informationstechnologierecht und Betreiber des Blogs Internet-Law, lehnt dagegen die Strafverfolgung mithilfe von Trojanern

allein schon aus verfassungsrechtlichen Gründen ab.

Pro-Standpunkt von Bernd Carstensen

Rechtsextremistischen Rattenfängern im Netz das Handwerk legen

Die Mitglieder und Unterstützer rechtsextremistischer Gruppierungen oder deren Terrorgruppen nutzen das Netz ebenso zur verdeckten bzw. konspirativen Kommunikation wie es mittlerweile Straftäter aus allen Kriminalitätsfeldern machen. Die Protagonisten des rechtsextremistischen Terrors kommunizieren aus den unterschiedlichsten Gründen im Netz. Sie präsentieren ihre menschenverachtende Ideologie, sie entwickeln Strategien zur Publicity, sie werben für eine Unterstützung ihrer Thesen und betreiben Propaganda in vielen sozialen Netzwerken, den sogenannten Social Network Services (SNS), in Foren und Blogs. Vielfach ist die hintergründige Propaganda auf den ersten Blick, auf die erste Begegnung im Netz gar nicht sofort zu erkennen. Sie sind die modernen digitalen Rattenfänger im Netz. Diese zuletzt genannte Präsentation rechtsextremistischer Haltung im Netz ist recherchierbar und kann auch von den Sicherheitsbehörden beobachtet werden. Die offene Präsenz im Netz ist von den Betreibern dieser rechtsextremistischen Websites gewollt. Die nicht offen im Netz zu verfolgende ist die konspirative Kommunikation, die im Deep- oder Darknet stattfindet. Hier benötigen die Nutzer dieser Foren eine spezielle Zugangs- oder Verschlüsselungssoftware. Diese Kommunikation wird dann zur kriminellen Handlung, wenn sich hier zu Straftaten verabredet wird oder Straftaten vorbereitet werden. Dieser Teil einer strafbaren Handlung muss den Ermittlungsbehörden zugänglich sein. So wie in der realen Welt unter bestimmten rechtlichen Voraussetzungen und mit Beschluss einer richterlichen Anordnung Straftäter z. B. observiert oder deren Telefonate überwacht werden dürfen, muss es möglich sein, die Internetkommunikation von Mitgliedern rechtsextremistischer Gruppierungen mit technischen Mitteln vor der stattfindenden verschlüsselten Kommunikation zu überwachen. Um das zu verdeutlichen: Es geht dabei nicht um die sogenannte Online-Durchsuchung oder, wie es umgangssprachlich bezeichnet wird, das Ausspähen von privaten PCs, mit deren Hilfe über eine installierte Software die gespeicherten Daten des Betroffenen auf dessen Computer kopiert werden. Es geht um die Installation einer Software im PC-System des betroffenen Tatverdächtigen, die die Übertragung von Daten dieses PC-Nutzers überwacht, bevor diese verschlüsselt

versandt bzw. nachdem verschlüsselte Daten empfangen werden. Wir sprechen hier von der sogenannten Quellen-Telekommunikationsüberwachung (Quellen-TKÜ). Vielleicht werden die Ermittlungen zur Aufklärung der Aktivitäten der rechtsextremistischen Terrorgruppe aus Zwickau zu der Erkenntnis führen, dass dieses Trio mit ihren Unterstützern der NSU (Nationalsozialistischer Untergrund) schon über Jahre konspirativ übers Netz kommuniziert hat. Eigentlich aus kriminalistischer Sicht schwer vorstellbar, da die stattgefundene Kommunikation wegen des Speicherverbots nicht vorhanden sein dürfte. Grund genug aber allemal, sich Gedanken über eine Anwendung einer rechtlich einwandfreien Online-Beweissicherung in der Bekämpfung des rechtsextremistischen Terrors zu machen.

Contra-Standpunkt von Thomas Stadler

Bereits kurze Zeit nach dem Bekanntwerden der Morde der sogenannten Zwickauer Zelle setzte die übliche sicherheitspolitische Diskussion ein. Forderungen nach Wiedereinführung der Vorratsdatenspeicherung und nach einer Onlinedurchsuchung wurden laut. Es waren allerdings nicht fehlende rechtliche Möglichkeiten, die verhindert haben, dass die Morde der sogenannten NSU aufgeklärt bzw. überhaupt in einen rechtsradikalen Kontext eingeordnet worden sind. Vielmehr waren mangelhafte Polizeiarbeit und die fehlende Abstimmung zwischen den Polizei- und Verfassungsschutzbehörden sowie ein völlig außer Kontrolle geratenes V-Mann-Wesen die Hauptgründe für das behördliche Versagen, über das wir seit Wochen diskutieren. Während diese Mängel relativ offensichtlich sind, besteht kein Grund zu der Annahme, dass beispielsweise der Einsatz von Trojanern im Rahmen von Onlinedurchsuchungen zu besseren Ermittlungsergebnissen geführt hätte. In diesem Zusammenhang muss man auch berücksichtigen, dass die Ermittlungsbehörden gerade im Bereich der Telekommunikationsüberwachung bereits über eine Fülle von Befugnissen und Möglichkeiten verfügen. Ein Umstand, der gerne verschwiegen wird, wenn wieder einmal neue Überwachungsbefugnisse gefordert werden. Der Einsatz von Trojanern durch Polizei- und Sicherheitsbehörden setzt voraus, dass der Rechner eines Tatverdächtigen heimlich mit einer Schadsoftware infiltriert wird, die anschließend Daten an die Behörden schickt oder gar das vollständige Durchsuchen und Auslesen der Festplatte erlaubt. Das Bundesverfassungsgericht sieht in solchen Maßnahmen einen schwerwiegenden Grundrechtseingriff, der nur in ganz engen Grenzen erlaubt ist, vor allem dann, wenn Leib, Leben und

Freiheit einer Person konkret gefährdet sind oder wenn solche Rechtsgüter der Allgemeinheit bedroht sind, die den Bestand des Staates oder die Grundlagen der Existenz der Menschen berühren. Wegen dieser enorm hohen Eingriffshürde gibt es im Bereich der Strafverfolgung, also zur Erforschung bereits begangener Straftaten, derzeit überhaupt keine Rechtsgrundlage für Onlinedurchsuchungen mittels Trojanern. Es dürfte in diesem Bereich auch kaum möglich sein, eine verfassungskonforme rechtliche Grundlage zu schaffen. Lediglich im BKA-Gesetz und in einigen Polizeigesetzen der Bundesländer existiert eine Vorschrift, die den sogenannten verdeckten Eingriff in informationstechnische Systeme erlaubt, allerdings nur im präventiven Bereich und unter den genannten engen Voraussetzungen. Als Instrument der Strafverfolgung ist die heimliche Onlinedurchsuchung mithilfe von Trojanern bereits aus verfassungsrechtlichen Gründen nicht geeignet.

Alle zukünftigen Netzstandpunkte sind hier nachzulesen. Für politik-digital.de habe ich unter der Creative Commons Lizenz CC BY-NC-SA 3.0 bis Januar 2012 folgende Netzstandpunkte erarbeitet und zusammengestellt:

Netzstandpunkte

Merkels YouTube-Fragestunde


PRO


CONTRA

PRO
Stephan Eisel

CONTRA
Marie Legrand

Netzstandpunkte

Post Privacy vs. Privatsphäre


PRO


CONTRA

PRO
Sebastian Westermayer

CONTRA
Peter Schaar

Netzstandpunkte

Brauchen wir einen Internetminister?


PRO


CONTRA

PRO
Jimmy Schulz

CONTRA
Juliane Witt