Medieninformation

TECHNISCHE UNIVERSITÄT DARMSTADT

Vorratsdatenspeicherung wohl nicht zur Prävention geeignet

Speicherung erstmals mit mathematischer Simulation wissenschaftlich untersucht

Kommunikation und Medien
Corporate Communications

Karolinenplatz 5
64289 Darmstadt

Ihre Ansprechpartnerin:
Gerda Kneifel
Tel. 06151 16 - 70 966
Fax 06151 16 - 41 28
kneifel.ge@pvw.tu-darmstadt.de

www.tu-darmstadt.de/presse
presse@tu-darmstadt.de

Darmstadt, 10.09.2012. Die Vorratsdatenspeicherung ist in Deutschland heftig umstritten. Die Befürworter argumentieren, dass mit der sechsmonatigen Speicherung von Telefondaten Planungen terroristischer Anschläge wie den auf das World Trade Center in New York womöglich verhindert werden könnten. Wissenschaftler der TU Darmstadt haben nun jedoch gezeigt, dass sie womöglich kein geeignetes präventives Mittel ist.

„Das hierzulande vorgebrachte Hauptargument, dass Terroristen schon vor einer Straftat identifiziert werden könnten – also rein präventiv -, ist nach unserer Studie fraglich“, bringt es der Bioinformatiker Prof. Kay Hamacher vom Fachgebiet Computational Biology and Simulation, auf den Punkt. „Entgegen bisheriger Vermutungen haben unsere Simulationen gezeigt, dass die Wahrscheinlichkeit, Terroristen ausfindig zu machen, praktisch nicht steigt“, konkretisiert Hamacher, der die Studie gemeinsam mit Prof. Stefan Katzenbeisser, Security Engineering Group der TU Darmstadt, leitete.
Die Darmstädter haben sogenannte Agenten-basierte Simulationen durchgeführt, eine Methode aus der Biologie, um Netzwerke von Interaktionen, wie zum Beispiel bei Individuen („Räuber“ und „Beutetiere“) hin zu untersuchen. Dabei werden konkrete Situationen simuliert und Interaktionen zwischen den Beteiligten modelliert. Diese Methode haben die beiden Forscher nun erstmals auf die Evaluierung von sicherheitsrelevanten Richtlinien (sogenannten 'policies') angewendet, indem sie die „Agenten“ als „Terrorist“ und „Bürger“ annahmen.

Kürzer würde mehr Sinn machen
Hierfür nutzten die Wissenschaftler reale Terrornetzwerke, die vom FBI nach den Anschlägen von 9/11 ermittelt und deren Interaktionen untereinander nachträglich bekannt wurden. Diese kleinen Gruppen von acht bis 17 Terroristen wurden in unterschiedlichen Simulationen verschieden großen Gruppen von 50.000 bis zu einer Millionen „Bürgern“ quasi eingepflanzt. Die Annahme war dabei, dass sie sich im Kommunikationsverhalten der unbescholtenen Mitmenschen zumindest zeitweise unterscheiden. So zum Beispiel, wenn eine bestimmte Person ein längeres und kurz darauf mehrere kurze Telefonate führt: eine Vorgehensweise, wie sie bei der Planung eines Anschlags realistisch ist, wenn zunächst Befehle abgesprochen und danach weitergegeben werden. „Wir haben Kommunikationsmuster definiert, oder besser gesagt Kommunikations-Hierarchien, die Abweichungen vom durchschnittlichen

Kommunikationsverhalten darstellen und (terroristische) Planungen widerspiegeln könnten.“ Mögliche Variablen sind dabei Zeitpunkte, Länge, Abstände und Abfolgen von Telefonaten. Das Problem ist jedoch, dass auch unverdächtige und gesellschaftlich gewollte Organisations- und Kommunikationsstrukturen auf diese Weise funktionieren. „Befehlsketten sind bei 'Projekten' ähnlich, ob man nun ein Flugzeug entführen oder ein Haus bauen will“, so Hamacher. Um eine Unterscheidung treffen zu können, sind daher sehr viele Eigenschaften der Kommunikation zu beachten. Diese „Verfeinerung des Filters“ hat wiederum zur Folge, dass es noch schwieriger wird, auffällige Kommunikations-Hierarchien ausfindig zu machen – als würde man den Heuhaufen, in dem eine Nadel gesucht wird, noch weiter vergrößern.

Wird nun doch ein Fall ungewöhnlichen Kommunikationsverhaltens ausfindig gemacht, „kann dieser Effekt allerdings bei längerfristiger Speicherung wieder verwischen“, erläutert der Bioinformatiker, „denn die Wahrscheinlichkeit, dass eine Gruppe von Bürgern ohne terroristischen Hintergrund ebenfalls kurzfristig häufiger miteinander telefoniert – beispielsweise um eine Hochzeit zu organisieren – steigt natürlich mit jedem Tag“. Das führt zu mehr falsch positiven Ereignissen. Anders gesagt: „Eine Speicherfrist von etwa 14 Tagen bis drei Monaten hat sich in unseren Simulationen als sensitiver herausgestellt als beispielsweise eine sechsmonatige Speicherung.“

Nutzenanalyse im Vorfeld gefordert

Hinzu kommt, dass hochgefährliche, kleine Gruppen, wie sie die Darmstädter untersucht haben, sehr einfache Möglichkeiten haben, die Ermittler auf falsche Spuren zu locken. „Sie müssen lediglich eine Art Zwillings-Gruppe schaffen. Dazu reicht es, statistische Eigenschaften der Kommunikation der Originalgruppe einzuhalten – und schon haben sie sich eine Art Schatten geschaffen, der ins Visier der Ermittler rückt.“ Ob das Resultat der Vorratsdatenspeicherung den Aufwand und die Kosten rechtfertigt, ist ohnehin unsicher. Denn eine neuere Untersuchung des Bundeskriminalamts zeigt, dass auch die Aufklärungsquote bereits verübter Delikte um maximal 0,06 Prozent steigt – darunter überwiegend Betrugsdelikte. Das Freiburger Max-Planck-Institut für Strafrecht kommt auf gerade einmal 0,002 Prozent.

Daher plädieren die Wissenschaftler der TU Darmstadt dafür, eine Kosten-Nutzen-Analyse zu sicherheitsrelevanten Fragen vor der Einführung neuer Maßnahmen und Richtlinien durchzuführen. „Unser Ansatz eignet sich für die Untersuchung von Netzwerken generell – seien es nun Netzwerke von Ökosystemen, Terroristen, Unternehmen oder auch Staaten, zum Beispiel im Zusammenhang mit transnationalen Finanztransaktionen. „So ließe sich im Vorfeld von teilweise doch einschneidenden Maßnahmen testen, ob der

erhoffte Benefit realistisch ist.“ Künftige Anwendungen sind da zahlreiche denkbar.

Pressekontakt

Prof. Kay Hamacher
Tel. 06151 / 16-5318
Mail: hamacher@bio.tu-darmstadt.de
Prof. Stefan Katzenbeisser (ab 17. September)
Tel. 06151 / 16-5016
Mail: katzenbeisser@seceng.informatik.tu-darmstadt.de

MI-Nr. 72/2012, gek