DATENSCHUTZ

Mixer in New York

Surfen im Netz, ohne Spuren zu hinterlassen: Die TU Dresden hat dafür mit Steuergeldern eine Software entwickelt. BKA-Ermittler versuchen nun, sie auszuschalten.

In eiligen Fällen kennen selbst Beamte kein Wochenende. Es war an einem Samstagmittag, als Ermittler des Wiesbadener Bundeskriminalamts (BKA) und des sächsischen Landeskriminalamts vor dem Haus von Hermann Härtig standen. Gleich an der Tür präsentierten die Fahnder dem verblüfften Direktor des Instituts für Systemarchitektur an der TU Dresden ihren Durchsuchungsbeschluss: Sie begehrten umgehend Einlass in Härtigs Institut.

Die Männer hatten es auf einen speziellen Datensatz abgesehen. Würde er den herausgeben, das war dem Computerexperten klar, wäre das Ziel jahrelanger Forschungsarbeit dahin: dass es nämlich dank einer an der TU Dresden entwickelten Software namens Java Anon Proxy (Jap) möglich ist, im Internet zu surfen, ohne Spuren zu hinterlassen.

Doch Widerstand schien selbst aus Sicht von Juristen zwecklos, die Ermittler waren schließlich einem Ring von Pädophilen auf der Spur, die ihre Bilder im Netz tauschen. Der überrumpelte Professor händigte die Daten aus. So erlitt Jap, der weltweit innovativste und angeblich sicherste Internet-Anonymisierdienst, sein erstes Leck – das Bürgerrecht auf Datenschutz war einmal mehr mit der Staatspflicht Verbrechensbekämpfung kollidiert.

Seit jenem Samstag Ende August ist in der Internet-Gemeinde nichts mehr, wie es einmal war: Die Surfer sind erschüttert. In einschlägigen Foren werden wütend Polizeistaatsmethoden beklagt, Vergleiche mit dem Dritten Reich und der Stasi gezogen.

Dabei hatte das Projekt vor vier Jahren für die Dresdner Forscher noch so hoffnungsvoll begonnen: Das Wirtschaftsministerium in Berlin spendierte 600 000 Euro an Steuergeld, der Deutschen Forschungsgemeinschaft war es 260 000 Euro wert, dass Surfer sich künftig über eine kostenlose Software völlig anonym im Netz bewegen können. Niemand sollte mehr anhand von Daten Profile von Menschen erstellen können, die davon nichts ahnten.

Seit zweieinhalb Jahren ist das Tarnsystem online, schon 20 000 Surfer täglich vertrauen auf den Schutz vor Überwachung. Im Gegensatz zu anderen Anbietern wie Anonymizer, Rewebber oder Steganos bleibt der Nutzer von Jap selbst gegenüber dem Tarndienst unerkannt.

SVEN DÖRING / VISUM

Institutschef Härtig: *Datenwust im Rührwerk*

Das Konzept ist so revolutionär wie simpel: Normalerweise hinterlässt die IP-Adresse, die jedem Surfer bei der Einwahl zugeteilt wird, Spuren im Netz, die später verfolgt werden können. So ist leicht zu ermitteln, welche Internet-Seiten der Benutzer aufgerufen und welche Informationen er abgerufen hat.

Jap hingegen anonymisiert diese Daten zuverlässig. Sie werden über so genannte Mixe geleitet, die den Datenwust aller Nutzer gleichsam wie in einem Rührwerk verwirbeln (siehe Grafik). Am Ende weiß kein außen Stehender mehr, wer auf welche Homepage zugegriffen hat. Auch nicht die Jap-Leute.

Die Datenschützer jubelten über die geniale Lösung, die Surfer feierten – allein das BKA meuterte: Die Ermittler sahen sich in ihrer Arbeit behindert.

Seit 2002 jagen die Fahnder unter dem Decknamen „Twins“ einen internationalen Ring von Kinderporno-Betrachtern, die ihr Material in geschlossenen Internet-Foren tauschen. BKA, FBI, Europol und die Londoner National Hi-Tech Crime Unit machten zahlreiche Tauschpartner ausfindig, von denen sich einige im vergangenen Jahr auf einer Farm in Missouri zu einem so genannten Teddybär-Picknick trafen. 40 Pädophile haben die Fahnder allein in Deutschland inzwischen identifiziert.

Doch Programme wie Jap machen den Kriminalisten die Enttarnung schwer, also sannen die Wiesbadener auf Arbeitserleichterung: Sie erwirkten Anfang Juli einen Beschluss des Amtsgerichts Frankfurt am Main, der die Jap-Betreiber verpflichtet, die Software so umzuschreiben, dass Zugriffe auf eine bestimmte IP-Adresse gespeichert werden können.

Der BKA-Erfolg war nicht von Dauer. Schon acht Tage später setzte die nächsthöhere Instanz, das Landgericht Frankfurt, den Vollzug der Aufzeichnung wieder aus. Den Dresdnern übermittelte das freilich keiner: Durch ein „Büroversehen“ kam die Nachricht erst nach 46 Tagen an der Elbe an – so lange hatten die Jap-Leute die IP-Adresse brav überwacht.

Das BKA reagierte nun umgehend: Sofort wurde wiederum beim Amtsgericht Frankfurt ein Durchsuchungsbeschluss für die Geschäfts- und Nebenräume sämtlicher Jap-Beteiligten erwirkt. Der aufgezeichnete Datensatz sollte umgehend beschlagnahmt werden.

Was Institutschef Härtig den Fahndern aushändigte, dürfte dem BKA wenig Freude bereiten: In der ganzen Zeit hatte ein einziger Jap-Nutzer die fragliche Adresse angewählt. Und ob die Strafverfolger dessen Daten je verwerten dürfen, ist fraglich: Das Landgericht Frankfurt hob vergangene Woche den Aufzeichnungsbeschluss des Amtsgerichts gänzlich auf. Er sei rechtswidrig.

Ob die Beschlagnahme rechtmäßig war, ist auch zweifelhaft. Die Entscheidung über eine Beschwerde der Jap-Aktivisten steht bisher aus.

Auch ohne juristischen Beistand sind die Jap-Macher längst weiter. Einer ihrer Mixer steht nun in New York. Der Beschluss eines deutschen Gerichts löst dort nur Schulterzucken aus.

STEFFEN WINTER

Getarnt in der Masse

Prinzip der anonymen Internet-Nutzung mit Jap

DER SPIEGEL

1 Ein Internet-Nutzer möchte anonym die Internet-Seite X öffnen. Seine Jap-Software verbindet ihn mit einer Zwischenstation, einem so genannten Mix.

2 Der Mix versteckt den Kontakt zur Seite X unter den Verbindungen von vielen weiteren Jap-Nutzern. Wer von ihnen die Seite X nutzt, kann kaum mehr zugeordnet werden.

3 Mehrere Mixe an verschiedenen Orten kodieren die Daten weitere Male um, damit die Rückverfolgung gänzlich auszuschließen ist.