Missbrauch programmiert

Datenbanken für Ermittler sind oft nicht dicht

Die Drohmails der „NSU 2.0“ an bekannte Persönlichkeiten machen deutlich, wie leicht Innentäter heimlich Zugriff auf IT-Systeme der Polizei und damit verknüpfte Register haben. Außer Hessen sind auch andere Bundesländer betroffen.

Von Stefan Krempl

Die Affäre um rechtsextreme, mit „NSU 2.0“ oder „SS-Obersturmbannführer“ unterzeichnete Drohschreiben an Personen des öffentlichen Lebens zieht Kreise. Mitte Juli wurde bekannt, dass der anonyme Verfasser oder die dahinterstehende Gruppe nicht nur der Berliner Kabarettistin Idil Baydar, der Frankfurter Rechtsanwältin Seda Basay-Yildiz sowie den linken Politikerinnen Martina Renner, Janine Wissler und Anne Helm einen nahen Tod prophezeit hatten. Auch taz-Kolumnistin Hengameh Yaghoobifarah, „Welt“-Autor Deniz Yücel sowie TV-Moderatorin Maybrit Illner waren auf der Liste.

Laut dem Hessischen Rundfunk hat der Verfasser in jüngsten Fällen angedeutet, „selbst Polizist zu sein“ und schon mehrere rechtsextreme Mails verschickt zu haben. Mehrere einschlägige Schreiben enthielten persönliche Informationen wie nicht öffentliche Adressen oder Verwandtschaftsbeziehungen, die aus hessischen Polizeidatenbanken abgefragt wurden. Im zwei Jahre alten, noch per Fax bewerkstelligten Fall Basay-Yildiz führte die Spur zu einem Polizeirechner im 1. Frankfurter Revier, bei späteren Vorgängen zum 3. und 4. Revier in Wiesbaden. Das dortige Innenministerium schließt ein rechtes Netzwerk in Reihen von Ermittlern nicht mehr aus.

Baydar, die über YouTube als Jilet Ayse in der Figur einer prolligen Kreuzberger Türkin und als Neuköllner Hausfrau Gerda Grischke bekannt wurde, kritisierte die Polizeiarbeit in der ARD. „Mein Leben ist nicht so, wie es vorher mal war“, beklagte die 45-Jährige. Erfahren habe sie von der Datenabfrage erst aus der Presse: „Von der Polizei habe ich bis heute nichts gehört.“ Das sorge nicht für Vertrauen.

Zuvor hatte die Kabarettistin erklärt, dass sie wegen Todesdrohungen schon 2019 acht Anzeigen erstattet habe. Alle Ermittlungen dazu seien eingestellt worden. Die Nachrichten hätten sie über das Onlineportal 5vor12 auf ihrem Handy erreicht, über das anonym SMS versendet werden können. „Die Plattform war bereit, die Daten herauszurücken, aber die Polizei hat das offenbar nicht einmal angefragt“, bedauerte Baydar. Die Ordnungshüter hätten sich sogar gewundert, „wie meine Nummer überhaupt öffentlich werden konnte“.

Hessen ist kein Einzelfall. Im Mai leitete die Polizei Brandenburg wegen Verdachts auf unberechtigte Datenabfragen

Bild: Boris Roessler/dpa

Die Rechtsanwältin Seda Basay-Yildiz gehörte zu den ersten Empfängerinnen von Drohnachrichten.

Disziplinarverfahren gegen zwei Polizisten ein, die dem Verein Uniter angehörten. Der wird vom Verfassungsschutz beobachtet und steht im Verdacht, Teil des rechtsextremen „Hannibal“-Netzwerks zu sein. Beiden Beamten wurden sämtliche Zugangsberechtigungen für polizeiliche Auskunftssysteme entzogen. Das LKA prüft eine mögliche strafrechtliche Relevanz.

Die brandenburgische Datenschutzbeauftragte Dagmar Hartge hatte zuvor in ihrem Tätigkeitsbericht 2019 konstatiert, dass die Polizei das erforderliche „systematische Rahmensicherheitskonzept“ etwa für das polizeiliche Vorgangsbearbeitungssystem Comvor, das Informations- und Auskunftsverfahren Polas sowie das Einsatzleitsystem Elbos „trotz wiederholter Aufforderung“ über Jahre hinweg nicht komplett vorgelegt habe.

Spionage im Bekanntenkreis

2018 monierte Hartges Berliner Kollegin Maja Smoltczyk, dass der Zugang zum dortigen Landespolizeisystem Poliks immer wieder missbraucht werde, um „Freunde, Familie, Nachbarn oder Dritte und deren Lebensumstände auszuspionieren“. Später rügte sie, dass bei der Millionen Menschen erfassenden Datenbank lange keine regelmäßige Zugriffskontrolle stattgefunden habe, sondern „nur eine stichprobenartige und aus unserer Sicht nicht ausreichende Überprüfung“.

Der baden-württembergische Datenschutzbeauftragte Stefan Brink verhängte 2019 ein Bußgeld von 1400 Euro gegen einen Polizisten, der dienstlich erlangte personenbezogene Daten eigenmächtig für private und damit nicht gesetzeskonforme Zwecke weiterverarbeitete. Auch der Datenschutzbeauftragte von Mecklenburg-Vorpommern, Heinz Müller, verwies auf einschlägige „unerfreuliche Fälle“. So hätten Strafverfolger etwa ihre Dienststellung ausgenutzt, „um an die Kontaktdaten minderjähriger Mädchen zu gelangen“ und diesen „sexuelle Avancen“ zu machen.

Missbrauch ist programmiert. Im Alltag auf der Wache ist es gang und gäbe, dass ein Beamter sein Kennwort in einen Rechner eingibt und in den damit verknüpften Systemen arbeitet. Anwender können so – je nach Berechtigung – etwa auch das nationale Polizeisystem Inpol, Melderegister, das Schengener Informationssystem, das Ausländerzentralregister oder in Hessen ein Big-Data-Warehouse der umstrittenen US-Firma Palantir abfragen.

Sesam, öffne dich

Für Berliner Polizisten dient ein Login in ihren „multifunktionalen Arbeitsplatz“ (MAP) laut dem Senat als „Sesam, öffne dich“ für bis zu 130 lokale, bundesweite, europäische und weltweite Datenbanken.

Wer auf der Dienstelle auf die Toilette oder unerwartet zu einem Einsatz muss, loggt sich oft nicht aus. Kollegen können so eine Sitzung kapern, ohne ihr eigenes Passwort zu verwenden. Bei protokollierten verdächtigen Abfragen wird der Kontoinhaber allenfalls als Zeuge gehört. Teils werden auch Dienststellenkennungen vergeben, die für alle auf einem Revier als Universalschlüssel fungieren. Bei Einträgen zu Ordnungskontrollen oder Aufzeichnungen wegen mündlicher Verwarnungen wird zudem meist ungenau oder gar nicht protokolliert.

Kritische Fahnder sind damit unzufrieden. Zurzeit verfügten rund 17.000 Mitarbeiter der Berliner Ordnungshüter über eine Berechtigung für Datenabfragen in Poliks, konstatierte Jörn Badendick von der Vertretung „Unabhängige in der Polizei“ jüngst bei einer Anhörung im Abgeordnetenhaus. Verstöße gegen die Regeln seien vielfach bezeugt, auch Kollegen hätten im Rahmen von Mobbing solche Vorfälle angezeigt. Die Staatsanwaltschaft habe sich aber geweigert, überhaupt zu ermitteln.

Bild: Stefan Krempl

Die Kabarettistin Idil Baydar wurde ebenfalls bedroht. Auffällig: Die Drohschreiben richteten sich fast ausschließlich an Frauen.

Auf massiven öffentlichen Druck hin hat der hessische Innenminister Peter Beuth (CDU) zusammen mit dem neuen Landespolizeichef Roland Ullmann Mitte Juli ein Maßnahmenpaket vorgestellt, um die Systeme abzudichten: Zugangsberechtigungen werden demnach alle drei Wochen zurückgesetzt, Datenschutz soll in jeder Dienststelle Chefsache werden. Jeder Abfrageverstoß „wird disziplinarisch und strafrechtlich verfolgt“. Die automatische Stichprobenkontrolle zu Datenabfragen werde engmaschiger, die Passwortsicherheit erhöht.

Schon bei Abruf der Eingabemaske soll das Benutzerpasswort fällig sein. Drittabfragen werden umfangreich dokumentiert, Vorgesetzte sollen täglich stichprobenartige Kontrollen durchführen. Mittelfristig ist eine Zwei-Faktor-Authentifizierung biometrisch per Fingerabdruck oder „Token“ auf dem Smartphone vorgesehen. Zudem soll eine Liste mit Personen des öffentlichen Lebens hinterlegt werden. Wer deren Daten bekommen will, braucht das Plazet eines höheren Dienstgrads. *(jo@ct.de)* c't