Reich werden mit der Polizei

Standardsoftware in der Repression und ihre Lieferanten

> Letztes Jahr wurde die IgaSt eingestellt, eine BKA-Datei über „Internationale gewaltbereite Störer“, aus der sich die Behörden regelmäßig bedienten, wenn es darum ging, Linke durch „Gefährderansprachen“ einzuschüchtern, Ausreiseverbote zu verhängen oder anderen Staaten Warnlisten anzudienen. Ein Schritt zu mehr Freiheit und Menschenrechten war das freilich nicht, denn eine etwas breiter gefasste Datei, die PMK-links-Z, übernahm ihre Funktion, mit noch mehr Feldern, die Staatsfeinde und ihre Vereine charakterisieren. Der Wechsel hatte im Wesentlichen einen Grund: Ein Privatunternehmen namens rola.

In den Urzeiten – also während der Terroristenhatz der 70er – bestand Polizeisoftware im Wesentlichen aus einem kleinen Stapel Lochkarten, der bestimmte, nach welchen Kriterien Überweisungsdaten, Stromrechnungen und Mietverhältnisse von sirrenden Bandspulen zusammengebracht werden sollten. Es handelte sich um Spezialentwicklungen, die wie damals üblich in enger Kooperation zwischen Anwender (in dem Fall dem BKA) und Computerhersteller (in dem Fall Siemens) gebastelt wurden.

Als nach und nach alle größeren Polizeien ihre eigenen Computersysteme bekommen sollten, ließ sich zunächst jede Behörde ihre eigene Software entwickeln, in der Regel zwar von Privaten („Systemhaus“ hießen die damals), aber eben doch exklusiv für den vorliegenden Zweck. Ein Höhepunkt dieser Methodik war fraglos INPOL-Neu, eine komplette Neufassung der BKA-Datenbanksoftware, die die Entwicklungstochter der Telekom, T-Systems, in den 90ern besorgen sollte. Auf der Wunschliste des BKA stand allerlei kriminologischer Barock („operative“ und „dispositive“ Fähigkeiten etwa, wobei erstere den normalen Abfragen hätte entsprechen sollen, letztere heute Data Mining – vgl. RHZ 4/06 – genannt würden). Mit sich dehnender Entwicklungszeit redigierte das BKA seine Wunschlisten regelmäßig, und der Ruf von T-Systems, große und kleine Projekte mit Lust punktgenau gegen die Wand zu fahren, ist auch nicht ganz unverdient.

So starb INPOL-Neu im Jahr 2000 einen flammenden Tod von Otto Schilys Hand. Nach einem vergeigten Inspektionsbesuch des Innenministers nämlich hatte dieser die Unternehmensberatung KPMG nach Wiesbaden geschickt, und diese fällte das Urteil, INPOL-Neu sei nur zu retten, wenn die Spitzenkräfte von der KPMG alles rauskanten dürfen, was die T-Systems-Leute vorher gemacht haben. Das passierte auch, und INPOL-Neu wurde ein einfacheres System, das viele Gemeinsamkeiten mit dem sich damals auf Länderebene etablierenden POLAS hatte. POLAS wiederum war eine Reaktion verschiedener Länder auf explodierende Kosten und mangelnde Stabilität ihrer Spezialentwicklungen und wird inzwischen von einer breiten Koalition von Ländern weiterentwickelt.

Profiling mit Turbo Pascal

Die POLAS-Fragmente waren indes nicht die erste „Standardsoftware“ beim BKA. Der Trend zu Programmen von der Stange wurde eingeläutet ausgerechnet von einem Produkt einer staatlichen Behörde, nämlich der Royal Canadian Mounted Police (RCMP). Diese hat nicht mehr viel mit Pferden zu tun, sondern ist eine Art kanadisches Gegenstück zu Bundespolizei und BKA in einem Haus. Die RCMP hatte in den 90er Jahren einige Ermittlungserfolge durch den Einsatz eines Computerprogramms namens ViCLAS, Violent Crime Linkage Analysis System. Dabei handelte es sich um ein Hilfsmittel fürs „Profiling“, das per (papierenem) Fragebogen gut 150 Merkmale von Schwerkriminalität und Vermisstenfällen erfasste und dann Verbindungen finden sollte. Das im anfangs winzigen Programmiersystem Turbo Pascal geschriebene Programm lief auf den für damalige Behörden höchst suspekten PCs. Dennoch hatte es für die Ordnungshüter offenbar großen Reiz, vermutlich, weil es um

Längen cooler war als das, was zwischen unfähigen Entwicklerbuden und gesetzlichen Rahmenbedingungen auf ihrer „großen“ EDV lief.

Vorreiter bei der Einführung von ViCLAS in der BRD war 1996 Bayern, 2000 zog das BKA nach. Dabei ist nach wie vor kein Fall breiter bekannt, in dem das kanadische System tiefe Erkenntnisse geliefert hätte. Bei den NSU-Morden etwa erkannte ViCLAS nur die gemeinsamen Tatwaffe – wofür es beileibe keine raffinierte Software braucht –, mitnichten aber beispielsweise, dass da Nazis am Morden waren.

Security Solutions

Während mit mit ViCLAS allmählich PCs bei der Polizei einzogen, begann Anfang der 2000er auch der kometenhafte Aufstieg einer Firma namens rola Security Solutions aus Oberhausen. Dort wurde eine Software entwickelt, die auch über die üblichen Abfrageschnittstellen („Auskunftssysteme“) hinausging und sich entsprechend wieder mit dem umsatzträchtigen Label Data Mining schmückte. Der generische Handelsname war rsCase, was schon die Positionierung als „Fallbearbeitung“ nahelegt, als ein System also, das die im Laufe einer Ermittlung anfallenden Daten zusammenfasst und womöglich zur gemeinsamen Auswertung mit weiteren Fällen zur Verfügung stellt. Wiederum war Bayern vorne, rechtsstaatliche Problematiken großzügig hintanzustellen. Im Freistaat kam rolas Software unter dem Namen easy ab 2003 an den Start.

Großkunde bei rola ist aber auch Europol, das seine „Analysis Work Files“ (AWF) schon seit den frühen 2000ern auf rsCase laufen lässt; dabei handelt es sich um gemeinsame Dateien mehrerer Europol-Mitgliedsstaaten und ggf. dritter Staaten, die sich mit jeweils einzelnen Deliktbereichen beschäftigen (z.B. Monitor für Rocker, Cyborg für „organisierte Kriminalität“ im Netz oder Dolphin für „nicht-islamistischen Terrorismus“, wozu beispielsweise auch Tierschutz- oder Umweltorganisationen zählen). An den AWFs arbeiten „Analyst_innen“ von Europol, die die von den teilnehmenden Ländern eingelieferten Daten nach dem Muster von Fernsehkrimis auf tiefe Erkenntnisse durchforsten. Angesichts der geheimpolizeilichen Orientierung von Europol ist nicht ganz klar, wer schon alles unter den AWFs hat leiden müssen. Immerhin war Europol etwa in die nach langer U-Haft mit einem Freispruch abgeschlossene Verfolgung österreichischer Tierrechtsaktivist_innen verwickelt (Dolphin?) oder auch in die als großer Schlag gegen Anonymous verkaufte „Operation Thunder“ (Cyborg?).

Endgültig als Hoflieferant etablierte sich rola, als das BKA die Software ins Herz der Deutschen Polizei holte und einige seiner Datenbestände in das neue System (beim BKA gebrandet als „b.case“) brachte. Zwar bleiben die inzwischen als „INPOL-Z“ zusammengefassten Kernstücke der BKA-EDV (der Kriminalaktennachweis sowie die Dateien für Erkennungsdienst und Personenfahndung) weiterhin auf dem POLAS-Derivat INPOL-Neu, doch immer mehr von den kleineren Dateien für allerlei Spezialzwecke und auch die Fallbearbeitung migrieren nach und nach auf die Standardsoftware.

500 Felder gegen Links

Ein für die RH ziemlich interessantes Beispiel für diese Entwicklung ist die Datei PMK-links-Z. Rechtlich handelt es sich dabei um eine „Zentraldatei“, d.h., das BKA füttert eigene „Erkenntnisse“ ein, die dann von anderen Polizeien abgefragt werden. Die PMK-links-Z soll speziell das „Erkennen von relevanten Personen, Organisationen und Strukturen“ im linksradikalen Bereich ermöglichen, wobei das BKA eine Person als „relevant“ ansieht, wenn sie „die Rolle einer Führungsperson, eines Unterstützers/Logistikers oder eines Akteurs einnimmt“ oder eine Kontakt- oder Begleitperson ist. Damit sich gesträubte Haare von Datenschützer_innen legen, murmelt die Regierung in einer Auskunft an den Bundestag noch was von der Prognose auf Straftaten im Sinne von §100a StPO – das sind die, für die Telefonüberwachung angeordnet werden kann –, will sich aber auch nicht darauf beschränken lassen; dementsprechend fehlt in der Errichtungsanordnung auch jede Spur einer solchen Einschränkung.

Die Errichtungsanordnung zeigt aber schön, wohin es führt, wenn Standardsoftware in diesem Bereich eingesetzt wird: Die Auflistung der in der Datei vorhandenen Daten erstreckt sich über fünfzehn (15) Seiten – kein Wunder, es handelt sich wohl einfach um um eine Darstellung des „Schemas“ (also des Satzes von Tabellen und ihren Spalten) von rsCase, in dem dann mal alles, was während einer Fallbearbeitung irgendwo so auftauchen könnte, mitgenommen wurde: Dazu gehören Buchungsnummern von Überweisungen ebenso wie der Farbeffekt von Fahrzeugen, Tätowierungsmotive und mitgeführte Tiere ebenso wie Katasteramts-Nummern von Gebäuden, der Erfasser eines Hinwei-

ses ebenso wie mp3-Dateien aus der Telefonüberwachung.

Insgesamt gibt es gegen 500 Datenkategorien (was zu vergleichen ist mit den 150, die bei ViCLAS fürs Profilen reichen sollen, und vielleicht 250 im noch spezialentwickelten PMK-links-Z-Vorgänger IgaSt). Zur Würze sind zahlreiche, schon rechtlich nur mäßig eingegrenze Freitextfelder enthalten, und was früher mal von den offiziellen Datenschutzbeauftragten für einen skandalösen Missbrauch von Polizeidatenbanken gehalten wurde, das Einspeisen kompletter Ermittlungsakten, wird nun von der Errichtungsanordnung gedeckt – wo kämen wir auch hin, wenn Features, für die rola Geld bekommen hat, nur wegen alberner Legalitätserwägungen nicht genutzt werden könnten.

Menschenrechte verkaufen

Was hier passiert, ist als „Kommodifizierung“ bekannt: aus Spezialanfertigungen wird nach und nach eine ganz normale Handelsware. Wie nebenbei Ansprüche des bürgerlichen Datenschutzes hinten runter fallen, zeigt der Vergleich der PMK-links-Z mit ihren Vorgängern.

Die Kommodifizierung von Repressionssoftware hat aber auch weitere hässliche Gesichter. Rola etwa dient sein rsCase inzwischen unter dem Handelsnamen rsFrame auch Geheimdiensten, Militär und Privatfirmen für deren „Sicherheitsaufgaben“ an. Eine Konsequenz aus der Vereinheitlichung von Plattformen ist jedenfalls erleichterter Datenaustausch, und das ist keine gute Nachricht, denn weit weniger als Widerstand aus bürgerlichen oder linken Kreisen haben Schwierigkeiten bei den Software-Schnittstellen den Sicherheitssumpf immer wieder gezwungen, Großangriffe auf die verbliebenen Freiheiten aufzuschieben.

Ein weiteres Beispiel für die bürgerrechtlichen Kosten des Warenhandels liefert das Prüm-System – dabei tauschen europäische Polizeien untereinander biometrische Daten der verschiedenen Untertanen aus. Für Fingerabdrücke funktioniert das auch sechs Jahre nach Vertragsabschluss nicht richtig, denn die verschiedenen staatlichen Systeme zur Beschreibung all der Schleifen und Verzweigungen auf den Fingerkuppen sind zutiefst inkompatibel, und bei weitem nicht alle Polizeien können mit einfachen Scans der Abdrücke etwas anfangen.

Bei DNA-Spuren sieht die Sache ganz anders aus: Es gibt nicht viele Hersteller von DNA-Profilmaschinen, und wer vom gleichen Hersteller kauft, kann praktisch auch schon Daten austauschen. Dementsprechend funktioniert der Austausch von DNA-Profilen innerhalb von Prüm vergleichsweise glatt.

Wer das hier nun lesen will als eine Gegenüberstellung ineffizienter staatlicher versus effizienter privater Organisation: Das ist natürlich Unsinn. Nicht erst der von der Firma Digitask hergestellte Staatstrojaner hat gezeigt, wie haarsträubend die private Repressionsindustrie arbeitet: de facto nicht vorhandene Verschlüsselung der erbeuteten Daten, lieblos zusammengeklickte Software-Hintertüren, nicht mal ein erkennbarer Versuch, auf irgendeine Sorte Menschenrechte Rücksicht zu nehmen, die dreiste Verweigerung jeder Inspektion unter Hinweis auf Betriebsgeheimnisse, die Unmöglichkeit, der ohnehin schon fast defätistischen Forderung nachzukommen, Gesprächsanteile aus dem „Kernbereich der persönlichen Lebensgestaltung“ wenigstens *nach* dem Abgreifen und Anhören zu löschen.

Gegenüber den üblichen Katastrophen aus dem reinen Behördenalltag sind die Fehlkonstruktionen aus privater Hand aber eine ganze Ecke schlimmer, schon, weil der Hersteller solcher Machwerke ein weit größeres Interesse hat als eine Behörde, ihren Murks möglichst breit eingesetzt zu sehen. So wird der Markt schnell angebotsorientiert, will sagen: Eine Firma hat für Saudi-Arabien eine tolle Unterdrückungstechnologie entwickelt und will sie auch in der BRD zu Geld machen. Tatsächlich lief es jedenfalls bisher eher umgekehrt: Eine für die BRD entwickelte tolle Unterdrückungstechnologie beglückt Potentaten im Rest der Welt. Was liegt auch näher, als den Behörden, mit denen „man“ ja ohnehin schon gut zurechtkommt, nahezulegen, sie bräuchten gerade das, was die Firma hat, zur Abwehr einer dramatischen Gefahr?

Zu den Quasisymbiosen zwischen Herstellern und Konsumenten von Unterdrückungstechnologie tritt normalerweise noch ein dicker Filzbelag, den Firmen in der Umgebung großzügig ausgestatteter Behörden wuchern lassen.

Mehr Menschenrechte verkaufen

Digitask beispielsweise hat vor einigen Jahren für das BKA auch einen Lauschangriff auf einen Satz in Nürnberg stehender Server einer linksradikalen Organisation durchgeführt, bei dem der komplette Netzwerkverkehr ausgeleitet wurde. Für Stunts dieser Art fühlt sich offenbar niemand zuständig, weder finanziell, denn die Mietkosten von rund einem Neupreis im

Monat für eher triviale Hardware lagen offensichtlich viel zu hoch, noch inhaltlich – es gibt keine Rechtsgrundlage für das Abschnorcheln aller Daten auf Serverseite für Polizeien, und das sollte wohl auch für „Rechtshilfe“ gelten (das betreffende Verfahren ist von der Schweizer Polizei geführt worden).

Das ist nicht *viel* schlimmer als das, was wir jetzt haben, aber eben doch ein wenig; als Bürger_innen eines Exportlands für Unterdrückungstechnologie macht unsere Trägheit zudem noch vielen anderen Menschen das Leben schwer. Dabei wäre es eigentlich nicht so schwer, das Treiben von Digitask (Haiger, nicht weit von Siegen) und rola (Oberhausen und Berlin; am zweiten Standort haben auch schon mal kreative Maler_innen vorbeigeschaut) oder auch von Unterdrückungshökern wie der Münchner Firma elaman öffentlich zu machen. Schon die eine oder andere Demonstration oder Mahnwache mag das Geschäft mit der Repression unattraktiver erscheinen lassen.

Wer nach besonders widerwärtigen Läden in seiner/ihrer Umgegung sucht: datenschmutz.de hat eine Seite zu Herstellern, mit einem weiteren Fokus bietet http://buggedplanet.info immer mehr Gelegenheit zur Empörung.

Datenschutzgruppe der Roten Hilfe Heidelberg

Kontakt und Artikel-Archiv: https://datenschmutz.de

PGP Fingerprint: a3d8 4454 2e04 6860 0a38 a35e d1ea ecce f2bd 132a