2011/12 Lifestyle

https://jungle.world/artikel/2011/12/spyware-fuer-despoten

Überwachungssoftware in Zeiten der »Facebook-Revolutionen«

Spyware für Despoten

Von **matthias monroy**

Überwachungssoftware ist in Zeiten der sogenannten Facebook-Revolutionen nicht nur in Afrika und im Mittleren Osten gefragt. Europäische Firmen sind auf dem Markt der Sicherheitstechnologie stark vertreten.

Während in Nordafrika auf gegen autoritäre Regime Revoltierende geschossen wurde, lud ein Messeveranstalter im Februar nach Dubai zur angeblich größten Verkaufsausstellung für Spionagetechnologie. Die beim fast gleichzeitig veranstalteten Europäischen Polizeikongress angepriesenen Produkte zur digitalen Überwachung und Kontrolle erschienen dagegen fast schon moderat.
Die gegenwärtigen Aufstände in den arabischen Ländern demonstrieren die Nutzung zahlreicher IT-Werkzeuge zur digitalen Kontrolle von Protest und Widerstand: Die tunesische Internetbehörde ATI hatte beispielsweise per Phishing-Software die Login-Daten von sozialen Netzwerken ausgelesen, um kritische Postings auf Facebook entweder zu verhindern oder mit eigener Propaganda zu versehen. Die ägyptische Regierung hatte das Internet Ende Januar zeitweise ganz abgeschaltet. Bei der Stürmung der Geheimdienstzentrale in Kairo förderten Demonstranten im März Papiere zutage, die ein Angebot zur Lieferung von Spähsoftware dokumentieren. Zwischen geschredderten Aktenbergen hatte der ägyptische Arzt Mostafa Hussein ein Schreiben der britischen Firma Gamma gefunden, wonach der Verkauf von Trojaner-Programmen geplant war.
Eine kurze Internetrecherche ergibt, dass die von Gamma angebotene »Remote Intrusion Software« von der Münchner Firma Elaman vertrieben wird, die hierfür nach eigenen Angaben eine Lizenz erwarb. Beide Firmen mischen kräftig mit im weltweiten Markt der Homeland Security, dem nach einer Studie des Hamburger Instituts für Weltwirtschaft bis 2015 ein Umsatz von 180 Milliarden Dollar prognostiziert wird. Firmen und Anwender, also Polizei und Geheimdienste, treffen sich regelmäßig zu internationalen Ausstellungen. Produktbeschreibungen und Tagungsorte lassen auf lukrative Absatzmärkte in russisch- und arabischsprachigen Ländern schließen.

Im Februar kamen Anbieter und Anwender des gesamten Portfolios von Spionagetechnik, die zum Eindringen in Kommunikationssysteme verwendet wird, in Dubai zusammen. Die Messe mit dem Titel »Intelligence Support Systems« adressierte Märkte im Mittleren Osten und Afrika. Die Aufstände gegen die autoritären Regime in Nordafrika boten den Ausstellern die Gelegenheit,

die angepriesenen Produkte quasi live zu präsentieren. Gezeigt wurden etwa Abhörwerkzeuge für alle Arten digitaler Kommunikation, darunter das Eindringen in Computer oder Funknetze, das Knacken von Passwörtern, das Mitschneiden von Mobilfunkgesprächen und SMS, das Aufspüren von Verbindungsdaten oder »Deep Package Inspection« auch verschlüsselter Verbindungen. Der Website der Münchener Firma Elaman zufolge hatte der Kooperationspartner Gamma einen Lieferwagen nach Dubai mitgebracht, der die Überwachungstechnologie auch mobil zum Einsatz bringt.
Eine Woche zuvor hatte in Berlin der Europäische Polizeikongress getagt. Der kommerzielle Charakter der Verkaufsmesse wurde durch eingestreute Vorträge kaschiert, zu denen sich auch Politiker einladen ließen. Ansonsten wurde die Interpretation der Weltlage Rüstungsfirmen überlassen, die als Sponsoren die Veranstaltung finanzierten. Vorstandsvorsitzende lobten die technische Aufrüstung zur Bekämpfung von Chaos und Terror und luden zum gemütlichen Plausch am Verkaufsstand. Dort fanden sich Anwendungen zur digitalen Vereinfachung polizeilicher Ermittlungen, zum Datenabgleich zwischen allerlei Polizeidatenbanken, zum Aufspüren von Flüchtlingsbooten per Satellit oder zur computergestützten Suche nach dem Klang des Wortes »al-Qaida« in abgehörten Telefonaten.
Aussteller in Dubai wie Berlin verkaufen Software, um die Schnüffelei im stetig wachsenden digitalen »polizeilichen Ereignisraum« zu erleichtern. Zudem wachsen die Begehrlichkeiten zur Einbeziehung neuer Datensammlungen. Der »Zukunftsgruppe«, einem Stammtisch europäischer Innenminister, zufolge existiert eine »Unmenge von Daten, die für Verfolgungsbehörden nützlich sein könnten«. Unter dem Vorsitz des damaligen deutschen Innenministers Wolfgang Schäuble wurde ein »Daten-Tsunami« konstatiert. Gemeint war keine Katastrophe, sondern aus der Perspektive der Überwacher das schiere Gegenteil: der Ausbau von Analysekapazitäten durch die verbesserte Auswertung von noch mehr digitalen Spuren. Automatisierte Verfahren bieten neue Wege zur Erschließung bislang unbeachteter Informationen. Dieses sogenannte data mining wird längst im kommerziellen Rahmen angewandt, etwa um Trends zu ermitteln oder Prognosen über Absatzmärkte zu erstellen. Übrigens hilft die Software auch im Falle abgekupferter wissenschaftlicher Arbeiten beim Auffinden ähnlicher Textstellen.

»Die größte Herausforderung besteht nicht mehr in der Sammlung von Information, sondern in ihrer Auswertung«, sagte auch der frühere Vizepräsident von EADS, Markus Hellenthal, vor zwei Jahren auf dem Europäischen Polizeikongress. In der Sprache von Polizei und Geheimdiensten heißen die in den Datenhalden analysierten Verknüpfungen »Risiken«. Je nach angeschlossenen Datenbanken wird ermittelt, wer Buchungen in verdächtigen Reisebüros vornimmt, identische Telefonnummern anruft oder vom gleichen Konto Zuwendungen erhält. Gleichzeitig können Informationen sogenannter open source intelligence miteinbezogen werden, also Einträge in öffentlich zugänglichen sozialen Netzwerken. Kombiniert mit Informationen aus Polizeidatenbanken entsteht eine Art digitales Abbild der Beziehungen zwischen Personen, Sachen und Ereignissen, dem in wissenschaftlichen Studien ein beträchtlicher Informationsgehalt zugesprochen wird. Die Software will zudem Kriminalitätstrends und sogar Straftaten vorhersagen. »Die Evolution in der Verbrechensbekämpfung« bewirbt die Softwarefirma SPSS: »Vom Reagieren über die Vorausschau zur Vorhersage«.
Spätestens wenn die computergestützte Suche im »Daten-Tsunami« nicht nur bei einzelnen Ermittlungen vorgenommen wird, sondern bei Polizei und Geheimdiensten dauerhaft im Hintergrund abläuft, kann von einer permanenten Rasterfahndung gesprochen werden. »Hierfür müssen die rechtlichen Voraussetzungen häufig erst noch geschaffen werden«, lamentierte Hellenthal auf dem Berliner Polizeikongress. Ungeachtet der häufig störenden Bestimmungen zu

Datenschutz und Persönlichkeitsrechten bieten alle großen Rüstungs- und Softwarefirmen entsprechende Lösungen an. Kein Wunder, denn es lockt die Aussicht auf beträchtliche Investitionen in Hardware, Datenbanken, Speichersysteme, Netzwerktechnik, Serversysteme und mobile Technologien.

Die polizeiliche Implementierung von Überwachungssoftware ist die zivile Übersetzung einer militärischen Doktrin. Diese »vernetzte Operationsführung« will die Überlegenheit über den Gegner erringen, indem eine größtmögliche Menge an Informationen verarbeitet wird. Beim Militär, der Polizei, der Feuerwehr oder beim Katastrophenschutz laufen eingehende Daten in Kontrollräumen (monitoring centres) zusammen und werden dort auf wandgroßen Monitoren visualisiert. Eine Software berechnet Entscheidungshilfen, deren Alternativen zuvor in Übungen oder Simulationen gesammelt wurden.
Die Relevanz dieser Kontrollzentren zur vorausschauenden Handhabung abweichenden Verhaltens wird beispielsweise beim Polizeiaufbau in der West Bank deutlich. In einem von der EU großzügig geförderten Programm werden in mehreren Städten operation rooms eingerichtet, die von einem EU-Ausbilder als das »Herz der Polizei« bezeichnet werden.
Auch die Polizei in Dubai nutzt längst ein deutsches »Police Command and Control Centre«, das 2006 von Siemens installiert wurde und von der Firma als eines der »weltweit fortgeschrittensten« bezeichnet wird. Mehr als 1 000 Video- und Thermokameras können in dem Raum von der Größe eines Theaters gesteuert und ausgewertet werden. Journalisten zeigen sich beeindruckt von der Auflösung und der Zoomfunktion der Kameras. Polizeifahrzeuge, auch Fahrräder, sind mit GPS-Trackern ausgerüstet und werden auf einem zwölf Meter großen Bildschirm zusammen mit GPS-Positionsdaten abgebildet. Integriert werden auch Bilder aus der Satellitenüberwachung. Die Plattform bewerkstelligte vor einem Jahr die detaillierte Rückverfolgung der mutmaßlichen Mörder des Hamas-Kommandeurs Mahmoud al-Mabhouh.
Zusammen mit dem finnischen Kommunikationskonzern Nokia hatte Siemens ein Kontrollzentrum aus dem Programm »Homeland Security Suite« in den Iran geliefert, das zum Instrument der Unterdrückung von Protest wurde. Der österreichische Journalist Erich Moechel beschrieb, wie im polizeilichen Kontrollraum in Teheran auch Daten von Mobilfunkbetreibern verarbeitet wurden. Damit konnten die Behörden jederzeit überwachen, ob sich auffällig viele Mobiltelefone in einer Funkzelle aufhielten und damit spontane Versammlungen anzeigten.
Die deutsche Polizei wird unter anderem mit monitoring centres der Schweizer Firma Ruag beliefert. Beim Nato-Gipfel 2009 kam deren Plattform »Panther Command« zum Einsatz, die seit Jahren die Einsatzleitung beim Weltwirtschaftsforum in Davos unterstützt.
Je nach An- oder Abwesenheit von Grundrechten können die computergestützten Informationszentralen indes jederzeit mit weiteren Funktionen ausgestattet werden. Skrupellos bewirbt beispielsweise die Firma Rola Security Solutions aus Oberhausen auf dem Europäischen Polizeikongress ihr »umfangreiches Software-Framework für die Informationsgewinnung und -verarbeitung«, das gleichermaßen von »Polizei, Militär, Nachrichtendiensten, Sicherheitsabteilungen von Unternehmen und mit Sicherheitsaufgaben betrauten Organisationen« eingesetzt werden kann. Weitere Überwachungs-Apps können »kundenspezifisch« mit einer »Vielzahl von Fachanwendungen, Modulen, Funktionen und Schnittstellen« hinzugefügt werden. So können auf der Basis von Gesichtern und Stimmen verdächtiger Personen Abhörprotokolle und Fotos durchsucht werden. In diese Richtung forscht etwa das EU-Vorhaben Indect, das verschiedene Spuren digitaler Überwachung im öffentlichen Raum – auch mit fliegenden Kameras – in einer einzigen Plattform vereinigen will. Neben der Universität Wuppertal sind die deutschen Firmen PSI Transcom und Innotec Data an Indect

beteiligt.

In Kreisen kritischer Netzaktivisten kursiert nach den Funden beim ägyptischen Geheimdienst jetzt die Idee einer Kampagne zur weltweiten Ächtung von Trojaner-Programmen. So unwahrscheinlich die Erfüllung der Forderung ist, weist sie doch in die richtige Richtung: Vielfach bleibt die Brisanz der neuen polizeilichen Spionagetechniken unverstanden. Als ähnlich erfolglose, aber einsichtige Forderung könnte darauf gedrängt werden, den Quellcode polizeilich genutzter Data mining-Software offenzulegen: Individuen sollten immerhin in Kenntnis darüber gesetzt werden, mittels welcher technischer Verfahren und Algorithmen sie von der Rüstungs- und Softwareindustrie zu Risiken erklärt werden.