Autoritäre Regime setzen auf Überwachungssoftware „Made in Europe“

Für unliebsame Journalisten, Blogger, Bürgerjournalisten und Demokratieaktivisten wird die digitale Überwachung immer mehr zur allgegenwärtigen Bedrohung – vor allem in Ländern, in denen es zur Tagesordnung gehört, dass die Pressefreiheit eingeschränkt wird. Die Technik dafür kommt dabei zumeist aus dem Westen.

Der folgende Text stammt aus „Das Netz 2012“, dem Jahresrückblick Netzpolitik von iRights. Das ganze Heft können Sie als E-Book oder Print kaufen. Mehr Infos und ein Preview hier und auf der Website des neuen Verlags iRights.media.

Die Betreiber der marokkanischen Webseite Mamfakinch.com waren noch gutgelaunt, nachdem ihnen im August der „Breaking Borders Award“ von Global Voices und Google verliehen wurde. Ausgezeichnet wurden ihre Anstrengungen zum „Schutz und der Förderung der Informationsfreiheit im Internet“. Das Projekt, hervorgegangen aus dem Arabischen Frühling, ist eine von Bürgerjournalisten betriebene Plattform, die über aktuelle politische und gesellschaftliche Entwicklungen in Marokko berichtet.

Doch nur elf Tage nach der Preisverleihung war die gute Stimmung verflogen, denn die Computer der Journalisten waren über eine fingierte E-Mail mit Überwachungssoftware der Regierung infiziert worden. Dieser Trojaner konnte fortan Bildschirminhalte fotografieren, Skype-Telefonate aufzeichnen, E-Mail-Verkehr mitlesen und die Mikrofone der Computer nutzen, um die Umgebung abzuhören.

Immer wieder geraten Journalisten, Blogger, Bürgerjournalisten und Demokratieaktivisten in Ländern, die die Meinungs- und Pressefreiheit einschränken, in den Fokus digitaler Überwachung. Die verwendete Software stammte Recherchen zufolge im konkreten Fall von der italienischen Firma „Hacking Team“ aus Mailand. Marokko steht auf der Rangliste der Pressefreiheit von Reporter ohne Grenzen auf Platz 138 von 179. Auch andere autoritäre Regime setzen auf Überwachungssoftware „Made in Europe“.

Während des Arabischen Frühlings wurde der Einsatz westlicher Späh- und Zensurprogramme unter anderem in Libyen, Tunesien, Syrien und Ägypten nachgewiesen. Geliefert haben die deutsche Firma Trovicor, die nach negativen Schlagzeilen aus dem Gemeinschaftsunternehmen Nokia Siemens Networks herausgelöst wurde, sowie die zur internationalen Gamma Group (mit Sitz im Vereinigten Königreich) gehörende Gamma International GmbH aus München mit ihrer Finfisher-Software. Der Einsatz von Finfisher wurde unter anderem in Bahrain dokumentiert: Dort geriet die Journalistin, Aktivistin und Universitätsdozentin Ala’a Shehabi in den Fokus der Überwachung.

Die Verantwortung der Journalisten

Werden Journalisten auf diese Weise überwacht, ist das eine nicht hinnehmbare Einschränkung der Pressefreiheit. Ein wirksamer Schutz der eigenen Quellen und eine freie Recherche sind dann nicht mehr möglich. Die durch Überwachung gewonnen Informationen können zu Inhaftierung, Folter oder Mord führen. Hier sind auch Journalisten und Journalistenorganisationen weltweit gefragt, eine größere Sensibilisierung in Bezug auf Datenschutz und Datensicherheit bei Journalisten zu erreichen. Einem britischen Journalisten wurde in Syrien das Notebook entwendet. Da die Festplatte nicht verschlüsselt war, erfuhr das Regime alle Informationen über seine Gesprächspartner. Glücklicherweise konnten sich alle enttarnten Personen rechtzeitig in Sicherheit bringen.

Die Hersteller von Überwachungssoftware werben häufig mit sehr eindeutigen Videos und Werbesprüchen wie „Einfach besser überwachen“. Diese Eigenwerbung lässt kaum Zweifel über den Sinn und Zweck dieser Software zu. Um Missbrauch zu vermeiden, so die Hersteller, verkaufen sie ihre Produkte nur an staatliche Akteure. Mit welchen Regierungen sie zusammenarbeiten und ob es in den Ländern Menschenrechtsverletzungen oder

rechtsstaatliche Kontrollen gibt, scheint dabei nur eine untergeordnete Rolle zu spielen.

Überwachungssoftware nistet sich unbemerkt auf dem Rechner des Opfers ein. Meist wird sie durch infizierte Dateianhänge oder gefälschte Software-Updates eingespielt. Einmal installiert, können die Programme alle Aktivitäten der Zielpersonen nachvollziehen und so sogar den Inhalt eigentlich verschlüsselter E-Mail- oder Chat-Nachrichten einsehen. Vom Auswertungszentrum der zuständigen Polizei- oder Geheimdienstbehörde können alle Funktionen des Trojaners ferngesteuert werden. Einige Programme erlauben es, nachträglich Dateien, zum Beispiel gefälschte Beweise, auf dem infizierten Rechner zu platzieren.

Reporter ohne Grenzen hat die Bundesregierung im August in einem Positionspapier aufgefordert, konkrete Maßnahmen zu ergreifen, um den Export solcher Software aus Deutschland und der Europäischen Union an autoritäre Staaten zu unterbinden. Dazu könnte Überwachungssoftware in die Regelwerke für den Export von Gütern mit zivilem und militärischem Verwendungszweck, sogenannte Dual-Use-Güter, aufgenommen werden. Außerdem haben wir die Regierung gebeten offenzulegen, inwiefern Hermesbürgschaften eingesetzt wurden, um den Export deutscher Überwachungstechnik abzusichern. Eine offizielle Antwort steht noch aus.

Das Thema ist seit vielen Jahren auf der politischen Tagesordnung – bewegt hat sich bislang leider nur wenig. Bei verschiedenen Anlässen haben sowohl die Bundeskanzlerin als auch der Außenminister die freiheits- und demokratiefördernde Wirkung des Internets hervorgehoben und gelobt. Doch als es im Europaparlament 2011 darum ging, ein System zur Exportkontrolle einzuführen, intervenierte der damalige Wirtschaftsminister Brüderle und die Europaabgeordneten der FDP stimmten einer entsprechenden Resolution nicht zu – und verhinderten sie damit.

Wirtschaftsförderung für Überwachung

Das Bundeswirtschaftsministerium betrachtet Überwachungstechnik als Zukunftsmarkt, und fördert diesen Sektor mit dem Programm „Zukunftsmarkt Zivile Sicherheit“ ausdrücklich. In Kooperation mit dem Nah- und Mittelostverein der deutschen Wirtschaft (NUMOV) und den Ländern des Golfkooperationsrates förderte das Wirtschaftsministerium die „1st German GCC Security Conference“ in Düsseldorf, bei der führende deutsche Hersteller von Überwachungs- und Grenzsicherungstechnik ihre Produkte vorstellen konnten.

Die Veranstaltung wurde mit bis zu 40.000 Euro aus dem Haushaltstitel „Erschließung von Auslandsmärkten, Unterposition Markterschließungsmaßnahmen für KMU des produzierenden Gewerbes und Dienstleister“ des Wirtschaftsministeriums finanziert. Journalisten waren nicht eingeladen, einem Mitarbeiter von Reporter ohne Grenzen wurde die Anmeldung verweigert. „Wenn Sie von Siemens wären, könnten wir da eventuell etwas tun“, so ein Mitarbeiter des ausrichtenden NUMOV telefonisch.

In einer Antwort auf eine kleine Anfrage der Fraktion der Grünen hat das Bundesministerium für Wirtschaft und Technologie nicht ausgeschlossen, dass Hermesbürgschaften für den Export deutscher Überwachungstechnik vergeben wurden.

Das Auswärtige Amt scheint einer Regelung entsprechender Exporte deutlich positiver gegenüberzustehen. Außenminister Guido Westerwelle sprach sich bereits mehrfach für Exportkontrollen aus, meist jedoch nur auf einzelne Länder wie Syrien und Iran beschränkt. Bei einer im September vom Auswärtigen Amt ausgerichteten Konferenz zum Thema „Internet und Menschenrechte“ wurde das Thema von den eingeladenen Experten ausgiebig diskutiert und tauchte auch in der Abschlusserklärung auf.

Das kann allerdings nur ein Anfang sein. Das Ziel ist es, endlich ein effektives Exportkontrollregime auf europäischer Ebene einzuführen. Doch der Weg dahin scheint noch lang.

Die Autoren sind Mitglieder bei der internationalen Nichtregierungsorganisation Reporter ohne Grenzen, die sich für Pressefreiheit und gegen Zensur einsetzt.

Das Heft „Das Netz 2012“ können Sie für 14,90 EUR bei iRights.media bestellen. Sie können auch eine E-Mail mit der gewünschten Anzahl und der Versandadresse an info@irights-media.de schicken. „Das Netz 2012 – Jahresrückblick Netzpolitik“ gibt es auch als E-Book, zum Beispiel bei Amazon, beim Apple iBookstore oder

bei Beam (dort auch DRM-frei).