Tomas Rudl

Wenn digitale Gewalt zu physischer Gewalt wird

In einer groß angelegten Untersuchung zeigt die Organisation Forensic Architecture*, wie verbreitet die Spähsoftware* Pegasus *ist. Die NSO Group liefert sie an Regierungen in aller Welt, die damit Menschenrechtsaktivist:innen, Oppositionelle und Journalist:innen überwachen.*

Die Spyware Pegasus kommt selten allein. Ins Visier der Überwachungssoftware gerät oft nicht nur die eigentliche Zielperson, sondern auch das soziale Umfeld des Opfers. Und oft genug schlägt die digitale Gewalt in physische um: Etwa im Fall des saudi-arabischen Journalisten Jamal Khashoggi, der im Exil überwacht, verfolgt und schließlich ermordet[1] wurde.

Der israelische Softwarehersteller NSO Group und sein Spitzel-Tool Pegasus stehen im Zentrum einer umfangreichen Untersuchung der Menschenrechtsorganisation Forensic Architecture.[2] Mit Hilfe von Amnesty International und dem kanadischen Citizen Lab hat die NGO 15 Monate lang öffentlich verfügbare Informationen ausgewertet, rechtliche Dokumente durchgeackert und mit Dissident:innen, Journalist:innen und Aktivist:innen gesprochen.

Daraus ist die bislang umfassendste Dokumentation der NSO Group und ihrer weltweiten Aktivitäten entstanden. Eine Online-Datenbank visualisiert Fälle[3] aus aller Welt, darunter in Spanien, Mexiko, Saudi Arabien, Indien und Ruanda. Die Filmemacherin Laura Poitras hat Interviews mit Betroffenen geführt, der NSA-Whistleblower Edward Snowden leiht dem Projekt seine Erzählstimme.

Weltweites Überwachungsnetzwerk

Die 2010 gegründete NSO Group gilt als einer der weltweit führenden Hersteller von Überwachungssoftware. Ihr Schlüsselprodukt Pegasus verkauft sie an Nationalstaaten, die damit die Rechner und Mobiltelefone von Verdächtigten hacken und überwachen. Doch anstatt damit Kriminelle oder Terroristen zu jagen, wie es in der Produktbeschreibung steht, findet sich die invasive Software regelmäßig auf Geräten von Menschenrechtsaktivist:innen[4], Oppositionellen[5] und Journalist:innen[6] wieder.

„Es ist eine Schadsoftware, die deine Kamera aktiviert, dein Mikrophon, alles, was ein integraler Teil deines Lebes ist“, berichtet die mexikanische Journalistin Carmen Aristegui in einem der Fallbeispiele.[7] Eine unscheinbar wirkende Textnachricht infizierte Anfang 2015 ihr Handy, die Überwachung weitete sich später auf ihre Kolleg:innen und sogar ihren minderjährigen Sohn aus.

Pegasus von Christian Friedrich Tieck auf dem Westgiebel des Schauspielhauses in Berlin-Mitte – Foto: Ajepbah, CC-BY-SA-3.0 DE

Hintergrund dürften kurz zuvor veröffentlichte investigative Recherchen über den damaligen Präsidenten Enrique Peña Nieto gewesen sein, dem Korruption nachgesagt wurde.

Vor Landesgrenzen machen die Tools der NSO Group nicht halt. Der saudische Dissident Omar Abdulaziz, ein Freund des später ermordeten Jamal Khashoggi, wurde im kanadischen Exil gehackt. Zwei seiner Brüder wurden kurz danach in Saudi Arabien verhaftet. Im Ausland lebende Oppositionelle aus Ruanda erhielten mysteriöse Nachrichten und Anrufe über WhatsApp[8], mit denen sie zunächst unbemerkt gehackt und überwacht wurden.

Moratorium für Spähsoftware gefordert

Die für den Einbruch genutzte Sicherheitslücke hat WhatsApp[9] längst geschlossen, die Mutter Facebook geht inzwischen juristisch gegen NSO Group[10] vor. Doch das Problem bleibt: Die Tools der Überwachungsindustrie gelangen allzu leicht in die falschen Hände[11], unter den Opfern können sich selbst Multi-Milliardäre wie der Amazon-Gründer Jeff Bezos[12] wiederfinden.

Expert:innen fordern schon seit langem eine rigorose Kontrolle des Sektors sowie ein Moratorium für den Verkauf von Spähtechnologie[13], bis eine globale Regulierung gefunden worden ist.

Tomas Rudl

Tomas Rudl ist in Wien aufgewachsen, hat dort für diverse Provider gearbeitet und daneben Politikwissenschaft studiert. Seine journalistische Ausbildung erhielt er im Heise-Verlag, wo er für die Mac & i, c't und Heise Online schrieb. Er ist unter ☎ +49 30 577148268 ✉ oder *tomas@netzpolitik.org* (PGP-Key[20]) erreichbar und twittert mal mehr, mal weniger unter *@tomas_np*

Die lässt jedoch auf sich warten. Zuletzt hatte sich etwa die EU auf bloß zahnlose Exportkontrollen für Spähsoftware[14] geeinigt, ein international abgestimmtes Vorgehen scheint derzeit in weiter Ferne. Firmen wie NSO Group können weiterhin in einem Graubereich operieren: Ein aktueller Bericht von Amnesty International[15] legt nahe, dass das Unternehmen ein schwer durchschaubares Firmengeflecht[16] dazu nutze, etwaige Exportbeschränkungen zu umgehen.

„Die Untersuchung zeigt das Ausmaß, in dem die digitale Sphäre, in der wir leben, die neue Grenze für Menschenrechtsverletzungen geworden ist", sagt Shourideh Molavi, leitende Forscherin für Forensic Architecture. Es handle sich um einen Bereich von staatlicher Überwachung und Einschüchterung, der physische Gewalt in der realen Welt ermögliche, so Molavi.

Auftakt für interdisziplinäre Praxis

In diese Welt schwappt auch die multimediale Untersuchung: Bis zum 8. August läuft die Ausstellung „Investigative Commons" im Haus der Kulturen der Welt[17] in Berlin. Sie präsentiert neue Formen kollaborativer Wahrheitsfindung und investigativer Ästhetik, heißt es in der Beschreibung: Ähnlich der NSO-Untersuchung sollen dabei Open-Source-Ermittlungen mit strategischer, juristischer Menschenrechtsarbeit verknüpft werden, hinzu kommen Methoden von Investigativ-Reporter:innen, Aktivist:innen und Wissenschaftler:innen.

Es soll der Auftakt sein für eine interdisziplinäre Praxis[18], die Forensic Architecture mit dem European Center for Constitutional and Human Rights (ECCHR) angestoßen hat. Gemeinsam mit anderen Gruppen, darunter die investigative Rechercheplattform Bellingcat und die Berliner Initiative Mnemonic, will das breit aufgestellte Netzwerk Verletzungen von Menschenrechten aufdecken.[19]

Quelle: https://netzpolitik.org/2021/spyware-pegasus-wenn-digitale-gewalt-zu-physischer-gewalt-wird/

Anmerkungen

1 *https://netzpolitik.org/2018/troll-armeen-und-spione-der-online-feldzug-der-saudi-arabischen-regierung/*
2 *https://forensic-architecture.org/investigation/digital-violence-how-the-nso-group-enables-state-terror/*
3 *https://www.digitalviolence.org/#/explore*
4 *https://netzpolitik.org/2018/spionagesoftware-pegasus-gegen-amnesty-international-eingesetzt/*
5 *https://netzpolitik.org/2020/wie-autoritaere-staaten-dissidenten-im-ausland-verfolgen/*
6 *https://netzpolitik.org/2020/citizen-lab-dutzende-iphones-von-journalistinnen-gehackt/*
7 *https://www.digitalviolence.org/#/pegasus-stories*
8 *https://www.bbc.com/news/technology-50249859*
9 *https://techcrunch.com/2019/05/13/whatsapp-exploit-let-attackers-install-government-grade-spyware-on-phones/*
10 *https://www.theguardian.com/technology/2020/jul/17/us-judge-whatsapp-lawsuit-against-israeli-spyware-firm-nso-can-proceed*
11 *https://www.zeit.de/digital/datenschutz/2020-12/ueberwachungssoftware-mexiko-rcs-hackingteam-drogenkartell-puebla/komplettansicht*
12 *https://netzpolitik.org/2020/ueberwachungssoftware-saudischer-kronprinz-soll-jeff-bezos-mit-whatsapp-nachricht-gehackt-haben/*
13 *https://netzpolitik.org/2019/un-bericht-fordert-transparentere-zusammenarbeit-zwischen-ueberwachungsunternehmen-und-staaten/*
14 *https://netzpolitik.org/2020/dual-use-verordnung-eu-verwaessert-neue-regeln-fuer-ueberwachungsexporte/*
15 *https://www.amnesty.org/download/Documents/DOC1041822021ENGLISH.PDF*
16 *https://www.digitalviolence.org/#/corporate*
17 *https://www.hkw.de/de/programm/projekte/2021/investigative_commons/start.php*
18 *https://www.sueddeutsche.de/kultur/berlin-haus-der-kulturen-der-welt-ausstellung-investigative-commons-menschenrechte-1.5341956*
19 *https://www.theguardian.com/law/2021/jun/27/berlins-no-1-digital-detective-agency-is-on-the-trail-of-human-rights-abusers*
20 *https://keys.openpgp.org/vks/v1/by-fingerprint/CA052285DC96CFC89E980514745121858AE13AED*

Constanze Kurz

Die Branche der Staatshacker ächten

Wieder wurde der Spionage- und Hackingdienstleister NSO Group beim systematischen Missbrauch seiner Software Pegasus erwischt. Solche Unternehmen gehören geächtet und als das benannt, was sie sind: eine Gefahr für Leib und Leben von Menschen. Ein Kommentar.

erschienen in der FIfF-Kommunikation, herausgegeben von FIfF e.V. - ISSN 0938-3476 www.fiff.de

Diesmal wird wohl auch keine ne… …r. Die an Amnesty International ries und mit vorher noch nie ge… …der NSO Group beinhalten über geblich so wichtige Arbeit gegen das Verbrechen helfen. Dem Spionage- und Hackingdienstleister NSO Group, der die Software namens Pegasus an dutzende Länder verkauft hat, wurde erneut systematischer Missbrauch seiner Technologie nachgewiesen.

Ganze Scharen von Menschenrechtlern, Reportern, Anwälten und politischen Entscheidungsträgern wurden und werden mit der Software ausspioniert oder finden sich auf langen Listen

…tausend Telefonnummern.

Nachzulesen ist das beim am Sonntag an die Öffentlichkeit gegangenen Pegasus-Projekt[2], in dem eine Gruppe von Journalisten gemeinsam ihre Recherchen zur NSO Group und deren Kunden koordiniert hat. Die am Markt der Staatstrojaner- und Spionagesoftware wohlbekannte Firma bezeichnet sich selbst als Führer im Feld des Cyber Warfare[3] und verkauft ihre Überwachungstechnologie weltweit exklusiv an staatliche Behörden.