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 Au
mons" im Haus der Kulturen der
neue Formen kollaborativer Wa
ver Ästhetik, heißt es in der Be
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/
rcs-hackingteam-drogenkartell-
berwachungssoftware-saudischer-
atsapp-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

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

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.

Diesmal wird wohl auch keine neue PR-Initiative mit Home-Stories und mit vorher noch nie gewährten Einblicken in die angeblich so wichtige Arbeit gegen das Verbrechen[1] 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 anvisierter Überwachungsopfer. Die an Amnesty International geleakten Listen von Kunden der NSO Group beinhalten über fünfzigtausend 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.

Das Projekt trägt den Namen der Software Pegasus, die von der NSO Group angeboten wird und iPhones und Android-Telefone ausspionieren kann. Typischerweise werden nach der Infektion heimlich Daten aus Messengern, E-Mail-Programmen oder Foto-Apps ausgeleitet. Aber nicht selten werden auch aktive Hacks durchgeführt, bei denen Mikrofone und Kameras aktiviert oder Ortsdaten in Echtzeit übertragen werden. Praktisch wird das infizierte Telefon zu einer Wanze, die mit dem Gerät durchgeführte, aber auch in der Nähe stattfindende Kommunikation ausspionieren kann.

Rücksichtslose Branche

Damit kommt nicht nur die Privatsphäre der Opfer und deren Kommunikationspartner in den Fokus, sondern auch ihr höchstpersönlicher Bereich, die Intimsphäre. Denn was man neben dem Smartphone so sagt und macht, ist bei vielen Menschen nochmal eine andere Dimension als das, was man ins Gerät hineinspricht oder -tippt. Dafür finden sich in der aktuellen Berichterstattung des Pegasus-Projekts auch prompt wieder konkrete Beispiele: Denn nicht jeder legt sein Telefon in einen anderen Raum, wenn er Sex hat.

Wollen wir wirklich weiterhin dulden, dass man bei jedem Gespräch immer darüber nachdenken müsste, ob das Telefon gerade in Reichweite ist? Wollen wir dulden, dass wir manchmal mit schalem Blick auf das Gerät schauen und denken, ob es wohl doch eine Wanze sein könnte? Und wollen wir diese ganze rücksichtslose Branche weiter mit Steuergeldern alimentieren?

Denn das haben die Parteien CDU, CSU und SPD im Bundestag kürzlich beschlossen[4], als sie das staatliche Hacken und Staatstrojaner auch noch für alle deutschen Geheimdienste erlaubt haben. Künftig werden also auch deutsche Gelder in diesem widerwärtigen Geschäftsfeld landen, denn ohne technische Hilfe aus dieser Branche sehen deutsche Staatshacker alt aus.

Mobiltelefone im Zentrum der Überwachung

Es ist beileibe nicht das erste Mal, dass der israelische Anbieter NSO Group und auch konkret seine Spitzel-Software Pegasus in der öffentlichen Kritik stehen. Erst vor wenigen Tagen machte eine umfangreiche Untersuchung der Menschenrechtsorganisation Forensic Architecture[5] nochmal klar, wie stark Journalisten, Oppositionelle und Aktivisten betroffen sind. Und es ist auch kein Skandal anderer Länder, wenn das deutsche Bundeskriminalamt[6] mitmischt und der bayerische Innenminister sich die Software vorführen lässt.

Dass Mobiltelefone heute im Zentrum der Überwachung stehen, kommt nicht von ungefähr: Für staatliche Behörden ist es mittlerweile ein Leichtes, an SIM-Karten-Daten mit gesicherter Identifizierung zu kommen, übrigens sowohl in demokratischen als auch diktatorischen Staaten. Denn die Zwangsregistrierung mit Identitätsnachweis ist im letzten Jahrzehnt fast überall eingeführt worden. Die Begründung war auch hier die Kriminalitätsbekämpfung. Einmal mehr zeigt sich die Schattenseite dieser einseitigen Politik: Es ist eben auch ein ungeheurer Machtzuwachs für jene, die auf die Telefon-Identifizierungsdaten sämtlicher Menschen zugreifen können.

Was man nach den neuesten Veröffentlichungen, aber im Grunde schon über die seit Jahren anhaltende kritische Berichterstattung festhalten muss, ist die Tatsache, dass um Journalisten, Anwälte oder Aktivisten eben längst kein Bogen mehr gemacht wird, wenn es um das Hacking ihrer Geräte geht – im Gegenteil, sie sind in zunehmendem Maße Ziel. Wenn weiterhin auch in Deutschland jeder Mensch verpflichtet wird, die SIM-Karte des eigenen Telefons mitsamt Identifizierung seiner Person registrieren zu lassen, bedeutet das schlicht, dass sie weiterhin auch Zielscheibe sein können.

Dass es Schadsoftware von Firmen wie der NSO Group auch künftig geben wird, können wir nicht kurzfristig ändern. Auch dass es an lange geforderten effektiven Kontrollen solcher Unternehmen fehlt, kann man vorerst nur weiterhin beklagen. Wir müssen hierzulande als Sofortmaßnahme aber die Identifizierung des eigenen Telefons und der SIM-Karte abschaffen. Denn das schafft die Grundlage dafür, dass der Raum eingeengt ist, in dem noch sicher und unbeobachtet kommuniziert werden kann.

Wer für die Exploits bezahlt

Die NSO Group ist mit einer anwachsenden Liste von Missbrauchsfällen schon über Jahre hinweg unangenehm aufgefallen. Kritik ließ sie stets abtropfen. Damit, dass Spionage-

Unternehmen und auch andere Marktteilnehmer nun ihr Geschäftsgebaren ändern, ist leider nicht zu rechnen. Sie werden weitermachen, finanziert von den Steuerzahlern der Käuferländer und protegiert von deren Regierungen. Die NSO Group dürfte auch weiterhin sogenannte Zero-Day-Exploits nutzen[7], also noch unbekannte Sicherheitslücken, die für hohe Preise gehandelt werden.

All das finanzieren die Kunden solcher Anbieter mit. Allein die US-amerikanischen Behörden geben Millionen Dollar[8] aus, um iPhones und Android-Telefone zu hacken, auch mit Hilfe der NSO Group[9]. Auch Deutschland hat dafür erst kürzlich die Weichen gestellt, indem die Erlaubnis zum staatlichen Hacken gesetzlich noch weiter ausgedehnt wurde.

Der aktuelle Skandal beweist, wie falsch diese Weichenstellung war und wie blind die politischen Entscheider für die Realitäten einer Branche von Staatshackern sind, die sich ihr gutgehendes Geschäft nicht durch Menschenrechte oder durch den Schutz von Geheimnisträgern vermasseln lassen.

Wir alle sind es, die nicht nur direkt, sondern vor allem indirekt dafür bezahlen, dass solche Firmen wie die NSO Group überhaupt legal existieren dürfen. Wir bezahlen mit unsicheren und ausspionierbaren Smartphones, deren Sicherheitslücken aufgekauft statt geschlossen werden. Wir bezahlen aber auch, weil wir hinnehmen, dass Menschen aus dem aktivistischen und journalistischen Bereich mitsamt ihren Familien und ihrem Umfeld nur in Angst noch ihrem Beruf oder ihrer Berufung nachgehen können.

Ich sehe das schon lange nicht mehr ein. Wir brauchen schnellstens eine Ächtung solcher Unternehmen in Deutschland, am liebsten gleich in ganz Europa. Wir müssen sie als das benennen, was sie sind: eine Gefahr für Leib und Leben von Menschen, mit denen man nichts zu schaffen haben darf. Keine deutsche oder europäische Behörde darf je (wieder) Kunde der NSO Group sein.

Quelle: https://netzpolitik.org/2021/schadsoftware-pegasus-die-branche-der-staatshacker-aechten/

Anmerkungen

1 *https://www.technologyreview.com/2020/08/19/1007337/shalev-hulio-nso-group-spyware-interview/*
2 *https://www.zeit.de/politik/ausland/2021-07/spionage-software-pegasus-cyberwaffe-ueberwachung-menschenrechte-enthuellung*
3 *https://www.documentcloud.org/documents/815991-1276-nso-group-brochure-pegasus.html*
4 *https://netzpolitik.org/2021/verfassungsschutz-und-bundespolizei-bundestag-beschliesst-staatstrojaner-fuer-geheimdienste-und-vorstraftaten/*
5 *https://netzpolitik.org/2021/spyware-pegasus-wenn-digitale-gewalt-zu-physischer-gewalt-wird/*
6 *https://www.zeit.de/politik/ausland/2021-07/ueberwachungsaffaere-spionage-software-pegasus-einsatz-deutschland-bundeskriminalamt-handydaten-rechtsstaat*
7 *https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso/*
8 *https://www.forbes.com/sites/thomasbrewster/2017/04/13/post-trump-order-us-immigration-goes-on-mobile-hacking-spending-spree/*
9 *https://www.vice.com/en/article/gygxk9/the-dea-met-with-controversial-iphone-hackers-nso-group*

Infos zur Autorin siehe Seite 57

Tom Jennissen

Uploadfilter werden Gesetz

Mit dem Urheberrechts-Diensteanbietergesetz werden erstmals Uploadfilter gesetzlich vorgeschrieben. Nach diesem Dammbruch ist zu befürchten, dass Uploadfilter künftig nicht nur zur automatisierten Durchsetzung des Urheberrechts zum Einsatz kommen, sondern zum universalen Regulierungswerkzeug werden.

Wenn der Bundestag am heutigen Donnerstag[1] abschließend über die Umsetzung der EU-Urheberrechtsrichtlinie[2] in deutsches Recht abstimmt, werden die im umstrittenen Artikel 17[3] vorgesehenen Uploadfilter endgültig in deutsches Recht gegossen. Größere Diensteanbieter wie etwa YouTube müssen dann nach den Vorgaben des Urheberrechts-Diensteanbietergesetzes (UrhDaG) spätestens ab August sämtliche Inhalte, die hochgeladen werden, automatisiert überprüfen und gegebenenfalls blockieren.

Ein seit Jahrzehnten etablierter Konsens der Internetregulierung ist damit aufgekündigt: Während Plattformen bisher in Notice-and-Takedown-Verfahren auf Hinweise hin vermeintlich rechtswidrige Inhalte prüfen und eventuell löschen mussten, sollen sie nun sämtliche Uploads ihrer Nutzerinnen und Nutzer aktiv überwachen.

Dabei galt es lange in der deutschen Politik als Konsens, dass Inhalte und Nutzende nicht umfassend überwacht werden sollen. Alle im Bundestag vertretenen Parteien haben sich gegen Uploadfilter ausgesprochen und auch die Regierungskoalition hat in ihrem Koalitionsvertrag[4] vom März 2018 unmissverständlich klargemacht: „Eine Verpflichtung von Plattformen zum Einsatz von Upload-Filtern, um von Nutzern hochgeladene Inhalte nach urheberrechtsverletzenden Inhalten zu ‚filtern', lehnen wir als unverhältnismäßig ab."

Dass dieses Versprechen nicht viel Wert war, wurde ziemlich genau ein Jahr später klar, als die Regierung im Rat der Europäischen Union der Urheberrechts-Reform und damit der Einführung von Uploadfiltern zustimmte.