Der Staat als Hacker

Die Bundesverwaltung lädt aus einer «Hackerzentrale» Staatstrojaner auf Handys von Verdächtigen. Die Kollateralschäden für die Cybersicherheit sind enorm. Die Serie zum Schweizer Überwachungsstaat, 3. und letzte Folge.

Von Adrienne Fichter (Text) und Erik Carter (Illustration), 18.01.2024

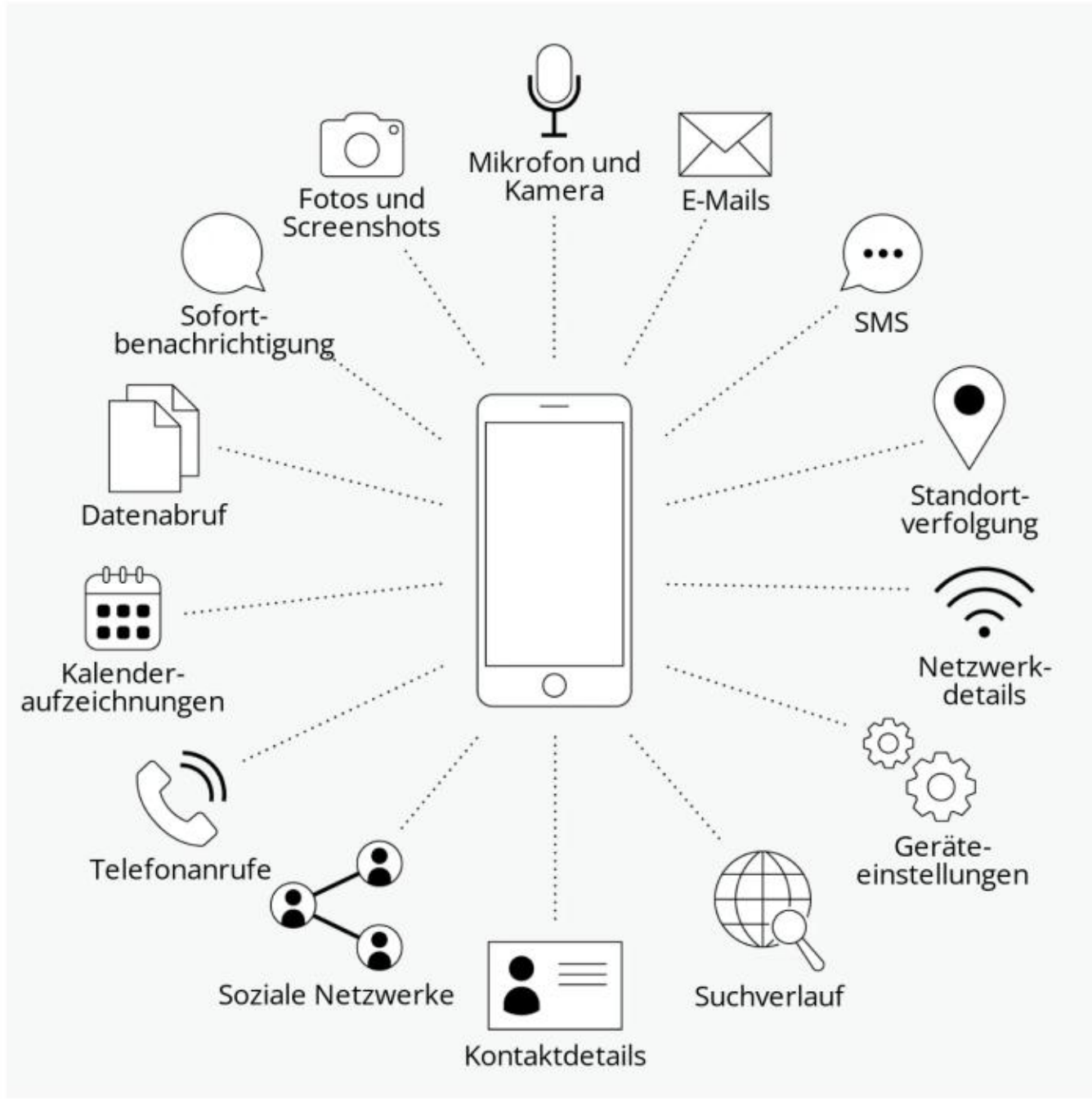
Der Journalist und Aktivist Jamal Khashoggi betrat am 2. Oktober 2018 das saudiarabische Konsulat in Istanbul. Er wollte dort Papiere abholen, die die Scheidung von seiner Exfrau bestätigen würden. Es war der letzte Schritt, der notwendig war, damit der in den USA lebende Khashoggi seine Verlobte in Istanbul hätte heiraten können.

Doch Khashoggi kam nie wieder aus dem Konsulat raus. Zwei Wochen später, nachdem der türkische Geheimdienst verschiedene Beweise vorgelegt hatte, war klar: Khashoggi, ein dezidierter Kritiker des saudiarabischen Kronprinzen Muhammad bin Salman, war im Konsulat ermordet worden.

Die Cybersecurity-Experten des Citizen Lab der Universität Toronto machten in den Jahren danach in mehreren Recherchen publik: Das engste Umfeld von Khashoggi war vor seiner Tötung durch die Königsfamilie der Saudis überwacht worden – und zwar mit einer Spyware namens Pegasus.

Pegasus ist eine schädliche Software – man sagt auch: Malware – die aus der Distanz auf ein Endgerät gespielt wird. Einmal auf dem Smartphone installiert, lassen sich über das Programm Mikrofone und Kameras aktivieren und eintreffende und ausgehende Nachrichten, auch verschlüsselte, in Echtzeit mitlesen. Die Software kann auch auf Bilder, Videos und sämtliche anderen Inhalte des Geräts zugreifen. Es ist, als ob einem jemand permanent über die Schulter auf den Bildschirm schauen würde – ohne dass man es merkt.

Weil diese Überwachungsprogramme vor allem von staatlichen Stellen eingesetzt werden, nennt man sie im Volksmund auch «Staatstrojaner». Die NSO Group benannte ihr Produkt ebenfalls nach einer Figur aus der griechischen Mythologie: einem geflügelten Pferd.



Bild

Das Handy als offenes Buch: Auf diese Funktionen und Inhalte hat die Spyware Pegasus Zugriff. Bodara

Die Citizen-Lab-Berichte zeigen: Die saudischen Sicherheitsbehörden hatten die Pegasus-Spyware im April 2018 auf das Android-Smartphone von Khashoggis Noch-Ehefrau Hanan Elatr installiert. Auch das Smartphone eines engen Freundes von Khashoggi war mit der Malware infiziert worden. Die beiden Freunde tauschten sich vor Khashoggis Ermordung regelmässig digital darüber aus, wie sich der Widerstand gegen den Kronprinzen organisieren liesse – und die saudische Herrscherfamilie las in Echtzeit mit.

Der Staatstrojaner und die Schweiz

Entwickelt wurde Pegasus von der israelischen NSO Group. Sie hat stets versichert, dass ihr Produkt ausschliesslich an staatliche Nachrichtendienste und Strafverfolgungsbehörden verkauft werde und einzig zur «Verhinderung und Untersuchung von Terror und schwerer Kriminalität» verwendet werden dürfe.

Nur, überprüft wird das von niemandem. Nicht nur das Umfeld von Khashoggi wurde «geschäftswidrig» abgehört. Im Sommer 2021 publizierte ein Konsortium von 17 Medienhäusern, koordiniert vom Netzwerk «Forbidden Stories», die Recherche «Pegasus Project». Die Journalisten werteten die von einer Quelle zugesteckte Liste von 50'000 Telefonnummern von potenziellen Überwachungszielen aus – und entdeckten etliche Handys, die mit dem Pegasus-Virus infiziert worden waren.

Darunter die Smartphones von Journalistinnen, Menschenrechtsanwälten, Politikerinnen, Aktivisten, in Indien, Mexiko oder Marokko, aber

auch in EU-Staaten wie Ungarn, Spanien oder Polen. Die «New York Times» bezeichnete den Staatstrojaner als die «mächtigste Cyberwaffe der Welt».

Ob auch die Schweiz in diesen Spionageskandal involviert war, blieb lange Zeit unklar.

Bereits früh gab es Indizien, dass es auch auf Smartphones von Schweizer Einwohnerinnen zu «Pegasus-Infektionen» gekommen ist. Die Forscher des Citizen Lab konnten in einem Report im September 2018 digitale Spuren von Pegasus im Swisscom-Netz nachweisen. Damit war erwiesen: Gewisse Personen, die sich auf Schweizer Boden befanden und das Schweizer Telecomnetz nutzten, waren Opfer dieses Staatstrojaners geworden. Inzwischen wissen wir noch mehr: Betroffen waren unter anderem die Handys von katalanischen Separatistinnen, die in jenem Zeitraum in der Schweiz im Exil lebten.

Wer gab den Auftrag für diese Überwachungen? Dies herauszufinden, ist bei Spyware praktisch unmöglich. Die NSO Group verwendet komplizierte und verkettete Serverinfrastrukturen, um die Spuren zu ihren Kunden zu verschleiern. Eine Recherche der Republik im Sommer 2021 zeigte beispielsweise, dass die NSO Group für ihre Operationen die Server der Schweizer Firma Akenes SA verwendete. Deren Infrastruktur wurde 2020 ohne ihr Wissen für das Hochladen und Verbreiten von Staatstrojanern genutzt. Im Fall der Katalaninnen gibt es laut Citizen Lab einige Evidenz dafür, dass sich die spanische Regierung hinter den Angriffen verbarg.

Doch waren oder sind auch Schweizer Behörden Kunden der NSO Group?

Die NZZ kam durch eigene Recherchen nach dem Pegasus-Skandal zum Schluss: ja. Auch das Westschweizer Fernsehen berichtete, dass die Schweizer Ermittlungsbehörden einen Trojaner einsetzten, der zumindest «Pegasus-ähnlich» sei.

Was bis anhin jedoch nicht bekannt war: Die Schweizer Strafverfolgungsbehörden beschafften sich Pegasus bereits zu einem frühen Zeitpunkt, nämlich im Jahr 2017.

Schweigen im Situation Room

Ein knappes Jahr vor dem Mord am saudischen Journalisten Jamal Khashoggi – also im Herbst 2017 – treffen sich mehrere Herren am Holzikofenweg 8 in Bern zu einem Meeting beim Bundesamt für Polizei Fedpol.

Anwesend sind Verkäufer und Informatiker der NSO Group, Kantonspolizistinnen, Staatsanwälte, ein Berater des Consultingunternehmens AWK Group und IT-Forensiker des Fedpol. Die ersten Medienberichte über die Israelis und ihre Wunderwaffe Pegasus sind da schon vor einiger Zeit erschienen, hauptsächlich mit negativen Schlagzeilen: etwa darüber, wie 2016 das Smartphone eines Menschenrechtsanwalts aus den Vereinigten Arabischen Emiraten angegriffen worden ist.

Das scheint das Interesse der Schweizer Ermittler jedoch nicht zu dämpfen, sondern eher noch zu steigern. Lange haben sie auf die Livedemonstration im Jahr 2017 gewartet, die Plätze sind sehr begehrt.

Die beiden israelischen Verkäufer haben das Equipment neben sich in einem kleinen Koffer aufgestellt, samt Antenne. Schritt für Schritt demonstrieren sie ihr Produkt und zeigen, was Pegasus alles kann.

In einer Livedemonstration steuern sie das Testsmartphone eines anwesenden Forensikers. Der schaut auf den Bildschirm seines Geräts und bemerkt – nichts Ungewöhnliches. Der Bildschirm sieht so aus wie immer. Doch was immer er gerade anklickt und anschaut, wird allen eins zu eins auf einer Leinwand ausgespielt. Die Vertreter der NSO Group schalten die Kamera und das Mikrofon ein, rufen die Kalendereinträge auf, zeigen die letzten Nachrichten von Whatsapp an. Der Raum wird gespenstisch still.

Pegasus macht das Rennen

Diese Szenen sind Schilderungen mehrerer Teilnehmer gegenüber John Doe, dem Whistleblower, der in Folge 2 dieser Serie eine zentrale Rolle spielte. Er selbst war an diesem Tag nicht am Holzikofenweg. «Man sagte mir, dass es nach der Demonstration eine längere Pause gab. Alle mussten nach draussen gehen und Luft schnappen», erzählt er. Zwei andere Personen aus dem Umfeld der Bundespolizei bestätigen diese Schilderungen. Auch sie hatten nach dem Treffen mit Teilnehmerinnen gesprochen, die vor Ort gewesen waren. Die Präsentation sei *«mind-blowing»* gewesen. Die anwesenden Polizisten seien begeistert gewesen.

Die Schweizer Behörden bezeichnen Staatstrojaner als Govware (Government Software) oder auch «besondere Informatikprogramme». Im Rahmen des Beschaffungsprozesses des Bundes mussten damals alle kommerziellen Govware-Anbieterinnen einen Fragebogen zur Selbstdeklaration ausfüllen, der der Republik vorliegt. Er ist datiert auf den 10. Februar 2017. Die Hersteller mussten angeben, inwiefern mit ihrer Software verschlüsselte Kommunikationsinhalte abgefangen und an das Fedpol ausgeleitet werden können. Und ob sie bereit wären, eine Dokumentation der gesamten Architektur offenzulegen.

Wer die meisten Punkte beim Fragebogen und bei der Livedemonstration erzielte, gewann den Zuschlag. Er fiel damals auf die NSO Group, wie John Doe und zwei andere Quellen aus der Bundespolizei bestätigt haben. Auch die Kantone prophezeiten dieser Software eine grosse Zukunft. In einer Umfrage der Eidgenössischen Finanzkontrolle im Jahr 2018 antworteten unter den Kantonen, dem Fedpol und der Bundesanwaltschaft 17 von 18 mit «Ja» auf die Frage, ob sie davon ausgingen, dass «aufgrund der zunehmenden Verschlüsselung in Zukunft vermehrt Govware eingesetzt werden wird».

Heute stellt sich die Frage: Hat sich diese Prognose bewahrheitet?

Es spricht einiges dafür. Schweizer Bundesbehörden und Kantone nutzen nachweislich bis heute unterschiedliche Govware-Produkte, die allesamt in Israel entwickelt worden sind.

- Gemäss den der Republik vorliegenden Informationen und mehreren Quellen im Umfeld der Bundespolizei haben die Kantone, das Fedpol und der Nachrichtendienst des Bundes (NDB) Pegasus mindestens bis 2022 genutzt. Ob der Trojaner heute noch im Einsatz ist, wissen wir nicht. Die Behörden – dazu später mehr – halten sich dazu so bedeckt wie nur irgendwie möglich.
- Dieselben Quellen bestätigen auch: Die Bundesbehörden haben die Software Predator der israelisch-irischen Firma Intellexa zumindest getestet. Einer breiteren Öffentlichkeit bekannt geworden ist diese Software durch eine umfangreiche Recherche der «Wochenzeitung» (WOZ), die gemeinsam mit dem «Spiegel», «Mediapart» und weiteren Medienhäusern durchgeführt wurde. Das Fedpol bestätigte gegenüber den Journalistinnen der WOZ lediglich, dass es Gespräche mit dem Herstel-

ler gegeben habe, der auch eine Tochterfirma in der Schweiz hat. Der Vorteil der Predator-Spyware: Sie «überlebt» einen Neustart des Smartphones.

– Heute breit im Einsatz sowohl bei der Bundespolizei als auch in Kantonen wie dem Kanton Bern ist die Software der Firma Cellebrite, die auch aus Israel stammt. Mit ihr können konfiszierte Handys von verhafteten oder verdächtigten Personen entsperrt und Verschlüsselungen geknackt werden. Nicht immer geht es dabei um Terror oder schwere Verbrechen: Die Bundespolizei entsperrte 2021 die Handys von drei Klimaaktivisten aus Lausanne. Cellebrite wird weltweit eingesetzt und wurde unter anderem auch zur «Durchsuchung» der Handys der Mitarbeiterinnen des russischen Oppositionellen Alexei Nawalny durch die russische Regierung verwendet.

Wie die Staatshacker arbeiten

Immer wieder betonen die Ermittler: Der Einsatz von Govware sei die «Ultima Ratio», das letzte Mittel. Sie werde nur bei Verdacht auf besonders schwere Straftaten eingesetzt – bei Pädokriminalität, bei Gefahr für Leib und Leben oder bei Terrorismus. Zudem ist der Einsatz von Staatstrojanern bewilligungspflichtig: Er muss im Falle einer Strafverfolgung von einem Zwangsmassnahmengericht, bei einer Überwachung durch den NDB vom Bundesverwaltungsgericht sowie von der Vorsteherin des Verteidigungsdepartements, derzeit also Viola Amherd, und zwei weiteren Bundesrätinnen abgesegnet werden.

Spyware wie Pegasus kommt oftmals erst dann zum Einsatz, wenn die Analyse der Metadaten mithilfe anderer Überwachungsmassnahmen (- über die wir in Folge 2 berichteten) nicht mehr ausreicht. Statistiken des Überwachungsdiensts zum Einsatz von Staatstrojanern gibt es seit dem Jahr 2019. Pro Jahr gab es seither maximal ein Dutzend Einsätze.

Diese Zahl wirkt erst einmal beruhigend niedrig – doch sie ist mit Vorsicht zu lesen. Erstens handelt es sich dabei nur um die Einsätze, die das Fedpol im Auftrag der Kantone und der Bundesanwaltschaft durchgeführt hat. Jene des Nachrichtendiensts werden nicht erfasst. Er muss keine öffentliche Auskunft geben – und gibt auch keine. Zwar wird die Gesamtzahl der bewilligungspflichtigen Überwachungsmassnahmen in den Lageberichten aufgeführt, diese werden jedoch nicht nach Kategorien wie Govware aufgeschlüsselt.

Zweitens gelingt das Aufspielen von Govware längst nicht jedes Mal, wenn es versucht wird. Es ist ein technisch sehr komplexer Angriff. De facto ist die Zahl der Anläufe wohl um ein Vielfaches höher als die der erfolgreichen Überwachungen.

Schliesslich sind die Fedpol-Überwachungen mithilfe von Staatstrojanern auch deshalb nicht häufiger, weil deren Einsatz wahnsinnig teuer ist. Gemäss dem Stand vom August 2022 verrechnet das Fedpol den Kantonen eine Pauschalgebühr von 3100 Franken pro Woche und Zielgerät.

Die Kantone selbst haben in der Regel nicht die nötige IT-Kompetenz für diese komplexen Operationen. Daher ist eine spezifische Arbeitsteilung entstanden: Das Bundesamt für Rüstung Armasuisse beschafft die Trojaner, das Fedpol kümmert sich um den Rest: Die dafür geschulten Staatshacker schleusen im Auftrag der Kantone Malware auf die Smartphones einer verdächtigten Person. Das Fedpol hat diesen Bereich in den letzten Jahren zentralisiert und professionalisiert.

Entstanden ist dabei eine staatliche «Hackerzentrale», wie mehrere Insiderinnen bestätigen: das «Kompetenzzentrum FMÜ P4 Govware» – FMÜ steht für Fernmeldeüberwachung, «P4» heisst das Govware-Programm der Bundesbehörden. Früher war dieses Zentrum am Holzikofenweg beheimatet. Heute hat es seinen Sitz gemäss Insidern beim Fedpol-Gebäude im Berner Wankdorf-Quartier (siehe Infobox).

Wie das «Hackerzentrum» des Fedpol die Handys von verdächtigten Personen «infiziert»

Darüber, was im «Kompetenzzentrum FMÜ P4 Govware» des Fedpol genau geschieht, ist wenig bekannt. Wie die Fedpol-Hacker beim Upload eines Trojaners vorgehen, lässt sich nach mehreren Gesprächen jedoch konstruieren: Firmen wie die NSO Group bieten ihren Kundinnen fixfertige Plattformen mit einfacher Benutzeroberfläche an. Die Kantonspolizistin kann sich die benötigten Tools für einen geplanten Angriff in einem «Menü» zusammenstellen: Sie wählt die Plattform der zu überwachenden Person, also ob deren Mobiltelefon ein Android- oder iOS-Betriebssystem hat. Zudem wählt sie die gewünschte Methode zur Anbringung der Schadcodes: Wenn der Staatshacker im Kompetenzzentrum «P4 Govware» zuerst eine Phishing-E-Mail verschickt, die zum Anklicken eines Links verleiten muss, ist der Cyberangriff günstiger. Denn das Opfer muss zuerst in die Falle tappen und auf den Link klicken. Eine geschulte Zielperson fällt nicht darauf rein.

Die kostspieligere Variante sind die Zero-Click-Programme. Also Sicherheitslücken in den Betriebssystemen, die etwa Google oder Apple noch nicht entdeckt haben. Ein Eindringen über diese Lücken erfordert nicht einmal ein unbewusstes Mitwirken der Zielperson. Sie hat keine Chance, sich zu wehren.

Die Staatshackerinnen versuchen nun, auf dem von der Polizistin «gebuchten Weg» auf das Gerät zu gelangen. Ist die Infektion des Smartphones geglückt, meldet sich der ins Handy eingeschleuste «Agent» und ist bereit, Befehle entgegenzunehmen.

Einblick unerwünscht

Es ist schwierig, mehr über die Anwendung von Pegasus und Co. zu erfahren. Auf konkrete Anfragen dazu verweigern die Behörden kategorisch die Auskunft. Bleibt die Möglichkeit, zu versuchen, an Dokumente zu gelangen. Aber auch das ist nicht einfach. Schon allein deshalb nicht, weil viele Absprachen zwischen Behörden und Spyware-Herstellerinnen mündlich gemacht werden.

Journalisten und Anwältinnen haben in den letzten drei Jahren gestützt auf das Öffentlichkeitsgesetz mehrere Gesuche eingereicht, um etwas Licht auf die Beschaffung und die Nutzung von Spyware durch den Bund werfen zu können. Das Fedpol und der Nachrichtendienst liessen bisher all diese Gesuche abblitzen.

Sie berufen sich dafür auf Ausnahmeregelungen im Beschaffungs- und Öffentlichkeitsrecht und behaupten, die Preisgabe gefährde die innere und äussere Sicherheit der Schweiz. Der Walliser Anwalt und ehemalige Datenschützer Sébastien Fanti will nun erwirken, dass die Verträge des Fedpol mit der NSO Group – falls es denn tatsächlich solche gibt – offengelegt wer-

den müssen. Vor dem Bundesverwaltungsgericht erlitt er am 9. Januar 2024 allerdings eine Niederlage.

Die Begründung der Richter: Wenn die Öffentlichkeit von einem Govware-Produkt Bescheid wisse, torpediere dies dessen Wirksamkeit – weil die mutmasslichen Täter dann wüssten, wie sie sich davor schützen könnten. Angesichts der Tatsache, dass man sich vor dem Upload von Spyware-Programmen kaum schützen kann, eine doch eher abenteuerliche Begründung. Fanti wird den Fall deshalb ans Bundesgericht weiterziehen.

Auch die Republik hat versucht, an weitere Informationen rund um die staatliche Hackerzentrale «P4 Govware» zu gelangen. Doch das Bundesamt mauerte auf der ganzen Linie. Die Fedpol-Juristinnen bestätigten zwar die Existenz aller eingeforderten Dokumente (Skizze der IT-Architektur, Konzepte und Evaluationen), lehnten das Gesuch jedoch vollständig ab. Nach einer Schlichtungssitzung und nach einer Empfehlung des eidgenössischen Datenschutzbeauftragten hat die Republik nun eine entsprechende Verfügung beim Fedpol verlangt. Die Bundespolizei muss nun nochmals über die Bücher. Beharrt sie weiterhin auf ihrem Nein, so wäre der nächste Schritt für die Republik ebenfalls das Bundesverwaltungsgericht.

Gemäss der norwegisch-amerikanischen Sicherheitsexpertin Runa Sandvik, die lange für die «New York Times» tätig war und heute mit ihrem Start-up Granitt Journalisten in puncto digitaler Sicherheit berät, ist die Schweiz da keine Ausnahme. Sie beobachtet schon länger, wie auch die EU-Staaten alle Initiativen für mehr Transparenz abblocken: «Die europäischen Regierungen wollen nichts preisgeben. Sie möchten, dass wir ihnen einfach vertrauen, dass sie diese Waffe ‹richtig› einsetzen.»

Sandvik dokumentiert unter anderem Cyberangriffe auf die Zivilgesellschaft, die laut der Firmenpolitik der Spyware-Hersteller gar nicht passieren dürften. Sie trackt und publiziert weltweit bekannt gewordene Fälle von Politikerinnen, Stars, Aktivisten und Journalistinnen, deren Handys mit Pegasus oder Predator infiziert worden sind. Namen von Schweizerinnen befinden sich bisher keine auf der Liste.

Werden Journalisten bald legal abgehört?

Dass die Anfragen von Journalistinnen abgeblockt werden, ist das eine. Doch bald könnten sie auch selbst «Mittel zum Zweck» werden – und ganz legal ausgehorcht werden. Solche Möglichkeiten werden derzeit in Brüssel verhandelt.

Eigentlich sollte das Europäische Medienfreiheitsgesetz die Situation von Medienschaffenden verbessern, etwa beim Versuch politischer Einflussnahme durch die Verlagshäuser. Doch nun könnte sich die Lage von Journalisten in einem entscheidenden Punkt sogar verschlechtern. Sieben EU-Staaten, darunter Frankreich, Italien, Finnland und Griechenland, haben im Dezember einen Vorstoss eingereicht, der es möglich machen soll, «im Namen der nationalen Sicherheit» Staatstrojaner auf das Handy von Journalistinnen zu schleusen.

Seither ringen die Mitgliedsländer heftig um Formulierungen, die ihnen weitgehende Kompetenzen für die Geheimdienste und die Strafverfolgung einräumen. Ein finaler Text steht noch aus.

Mit der Legalisierung von Spyware auf den Handys von Journalisten wäre der Quellenschutz – ein in der Europäischen Menschenrechtskonvention verankertes Recht – faktisch tot.

Auch hierzulande könnte der Nachrichtendienst den Einsatz von Spyware ausweiten, auf Anwältinnen, Ärzte und Journalistinnen. Im ersten Halbjahr 2024 wird eine zweite Vernehmlassung zur Revision des Nachrichtendienstgesetzes gestartet. Beim ersten Anlauf im Jahr 2022 wollte der Nachrichtendienst erreichen, dass die Spionagetätigkeit in gewissen Fällen auch auf diese bislang geschützten Berufsgruppen hätte angewandt werden dürfen. Faktisch wären dadurch das Berufsgeheimnis und der Quellenschutz aufgehoben worden. Der Einsatz von Staatstrojanern etwa auf den Handys von Journalisten wäre legal geworden.

Die Kritik an der Vorlage war dann jedoch derart gross, dass sie nun noch einmal überarbeitet wird. Dazu, ob an dieser Ausweitung der Überwachungsmöglichkeiten in der Version 2.0 festgehalten werden soll, will sich der Nachrichtendienst nicht äussern.

Ausbau statt Regulierung

Während das Uno-Menschenrechtsbüro vor Spyware warnt und die USA die NSO Group sogar auf eine schwarze Liste gesetzt haben, zeigen Politikerinnen in der EU und in der Schweiz kein grosses Interesse daran, diese Schadprogramme zu regulieren – obwohl Mitarbeiter der EU-Kommissionen oder der französische Präsident Emmanuel Macron selber von Pegasus betroffen waren. Zu wichtig ist der Einsatz von Staatstrojanern für Geheimdienste und die Strafverfolgung mittlerweile offenbar geworden.

Eine Untersuchung des EU-Parlaments zeigt: Insgesamt 22 Behörden in 12 verschiedenen EU-Staaten waren Kunden der NSO Group. Die niederländische EU-Abgeordnete Sophie in ’t Veld, Mitglied der liberalen Fraktion Renew Europe, brachte es gegenüber dem Medienportal «Euractiv» folgendermassen auf den Punkt: «Spyware ist zu einer Hydra geworden, und Europa ist ihr sicherer Hafen.» Waren es ursprünglich die deutsche Firma FinFisher und das italienische Hacking Team, die die ersten Trojaner für Europa auf den Markt brachten, bringen sich laut einer «Politico»-Recherche heute immer mehr europäische Spyware-Hersteller in Stellung.

In der Schweiz stellten bisher nur wenige Parlamentarier kritische Fragen. Eine Ausnahme machte der mittlerweile abgewählte GLP-Nationalrat Jörg Mäder, der 2021 wissen wollte, ob die Schweizer Behörden Pegasus oder ähnliche Spyware einsetzten und ob es Richtlinien für deren Einsatz gebe. Verteidigungsministerin Viola Amherd blieb in ihrer Antwort vage. Und stellte klar: «Zum operativen Einsatz äussert sich der Bundesrat aus Sicherheitsgründen nicht.»

Bemerkenswert ist auch, was derzeit in Zürich auf kantonaler Ebene passiert. Die Sicherheitsdirektion möchte in der Teilrevision des Zürcher Polizeigesetzes, zu der es im Sommer 2023 eine Vernehmlassung gab, festschreiben, dass sie sich künftig mithilfe von «besonderen Informatikprogrammen» in geschlossene Nutzerforen einschleusen darf. Und dies sogar bei Straftatbeständen wie «Aufruf zu schweren Sachbeschädigungen».

Die Frage, ob damit der Einsatz von Staatstrojanern ermöglicht werden soll, will die Zürcher Sicherheitsdirektion seit sechs Monaten partout nicht beantworten. Die Medienstelle möchte sich erst nach Auswertung der Vernehmlassung zu dieser Frage äussern. Die Digitale Gesellschaft und die Piratenpartei sehen in diesem Paragrafen einen Freipass für noch mehr Einsätze von Spionageprogrammen.

Staatliches Hacken als «Kompromiss»

Insgesamt ist davon auszugehen, dass das Katz-und-Maus-Spiel vorerst weitergehen wird: Auf der einen Seite stehen die Big-Tech-Konzerne, die stets versuchen, Sicherheitslücken in ihren Programmen möglichst rasch zu schliessen. Und auf der anderen Seite die Spywareindustrie, die unermüdlich nach neuen Sicherheitslücken sucht und Programme entwickelt, um diese auszunutzen – finanziert und gefördert von westlichen Regierungen.

Beim Thema Staatstrojaner manifestiert sich ein grundlegender Interessenkonflikt: zwischen Cybersicherheit und Strafverfolgung. Der Staat hat ein legitimes Interesse an einem sicheren Internet, das seine Bürgerinnen möglichst vor Angriffen schützt. Gleichzeitig nutzt er technische Defizite und Sicherheitslücken, um Täter aufzuspüren (ein Interessenkonflikt, der sich im Übrigen auch bei der Entstehung des neuen Bundesamts für Cybersecurity zeigte).

Der Einsatz von Spyware ist für die Ermittlerinnen so gesehen ein «Kompromiss»: Die Verschlüsselungen in unseren Handys bleiben insgesamt unangetastet, in Einzelfällen werden sie jedoch mit «Spezialwerkzeugen» wie Spyware geknackt.

Eine Win-win-Situation für die Gesellschaft und den Staat? Nicht ganz.

Dass die Behörden die Erlaubnis haben sollen, Überwachungen durchzuführen und digitale Spuren auszuwerten, ist in der Schweiz politisch praktisch unbestritten. Ebenso besteht ein breiter Konsens, dass Sicherheitsbehörden und Geheimdienste dafür entsprechende technische Mittel benötigen.

Doch die «Lizenz zum Hacken», die dem Staat damit ausgestellt wird, hat eine Kehrseite. Es stellt sich die Frage: Möchten wir wirklich, dass der Staat technische Sicherheitslücken bewusst offen lässt und sich Schadcode beschafft, um diese Sicherheitslücken für die Überwachung auszunutzen? Oder möchten wir, dass er in erster Linie versucht, seinen Beitrag zu leisten, damit diese Lücken geschlossen werden?

Das oft geäusserte Standardargument «Wer nichts zu verbergen hat, hat nichts zu befürchten» wird spätestens beim Thema Trojaner zur gefährlichen Floskel. Denn wenn der Staat immer mehr Staatstrojaner einsetzt, um Verschlüsselungen aufzubrechen, betrifft das eben nicht nur jene, die überwacht werden.

Wenn Staaten wie die Schweiz in der digitalen «Unterwelt» bei dubiosen Dealern Programme einkaufen, fördern sie einen Schwarzmarkt, auf dem sich auch Cyberkriminelle eindecken. Und wenn sie Sicherheitslücken zur Überwachung ausnutzen, statt sie zu schliessen, gefährden sie die Cybersicherheit überhaupt – und damit die ganze Gesellschaft. Niemand möchte seine persönlichen Daten im Darknet von Kriminellen verkauft sehen.

Zivilgesellschaftliche Organisationen wie Amnesty Tech oder die Schweizer Organisation Digitale Gesellschaft fordern deshalb vehement ein Moratorium für oder gar ein Verbot von Spyware.

Die Spuren der Überwachung

Ob nun bei der anstehenden Revision des Nachrichtendienstgesetzes oder beim Kampf gegen die Verschlüsselung durch den neuen Mobilfunkstandard, über den wir in Folge 2 berichtet haben: Die Schweizer Bundesbehörden werden weiter nach Möglichkeiten suchen, die Überwachung Schritt für Schritt auszuweiten. Mit dem neuen, bürgerlicheren Bundesparlament dürfte der Bundesrat auf Mehrheiten für Law-and-Order-Gesetze zählen können. Und die Arbeit von Investigativjournalistinnen dürfte noch schwieriger werden.

Doch die immer invasiveren staatlichen Eingriffe in unsere digitale Privatsphäre hinterlassen Spuren. Eine neue Studie des Instituts für Kommunikationswissenschaft und Medienforschung der Universität Zürich zeigt: Die Zahl der Schweizer Internetnutzer, die eine Verletzung der Privatsphäre durch die Regierung befürchten, ist seit 2021 um 10 Prozentpunkte gestiegen – auf 37 Prozent.

Unsere Recherchen haben gezeigt: Diese Furcht ist durchaus begründet.

Die Serie «Surveillance fédérale» ist mit dieser 3. Folge abgeschlossen. Doch die Geschichte rund um die staatliche Überwachung wird weitergehen.

Wir bleiben dran.

Die Veranstaltung zur Serie

Am Dienstag, 23. Januar, diskutieren wir in Zürich darüber, wie wir zunehmend überwacht werden. Mit dabei sind Viktor Györffy, Anwalt in verschiedenen Verfahren für die Digitale Gesellschaft, Janik Besendorf, Digital Security Lab von «Reporter ohne Grenzen», und Adrienne Fichter, Tech-Reporterin und Autorin der Serie «Surveillance fédérale». Alle Informationen zu dieser Veranstaltung finden Sie hier.