Die Irrwege der Überwacher

Wie sich der Schweizer Überwachungsdienst ein teures, weitgehend unbrauchbares System andrehen liess. Wie er eine gesetzliche Hintertür nutzte. Und wie er heute gegen die digitale Verschlüsselung ankämpft. Die Serie zum Schweizer Überwachungsstaat, Folge 2.

Von Adrienne Fichter (Text) und Erik Carter (Animation), 15.01.2024

Es war eine dieser Nachrichten, die Investigativjournalistinnen nur selten erhalten und die so aufregend klingen, dass man dafür einen Moment alles stehen und liegen lässt: Ob ich an Informationen aus dem Maschinenraum der Strafverfolgung interessiert sei, fragt mich ein anonymer Absender im Frühjahr 2022 über einen Messengerdienst.

Ich verabrede mich mehrfach, im In- und Ausland, mit der Quelle, die ich in guter alter angelsächsischer Tradition John Doe nenne. Vor den Treffen vereinbaren wir Codes und Gesten, wie ich es sonst nur aus Geheimdienstfilmen kenne. Damit will John Doe sichergehen, dass mir niemand gefolgt ist. Doch viel wichtiger als diese schauspielerischen Leistungen sind die vielen technischen Vorkehrungen.

Denn hier ist Paranoia leider angebracht: Unsere Smartphones melden unseren Standort alle paar Minuten an die Antennen von Swisscom, Salt oder Sunrise. Die Telecomkonzerne müssen die Informationen dann sechs Monate lang speichern. Bei Bedarf können die Strafverfolgungsbehörden und der Geheimdienst per «rückwirkende Überwachung» darauf zugreifen.

Warum der Whistleblower reden will

Wer also ist dieser John Doe?

Der Whistleblower arbeitete zwei Jahrzehnte lang als technischer Fachmann für die Strafverfolgung – in unterschiedlichen Positionen. Heute ist er bei einem Kanton tätig, so viel dürfen wir schreiben. Bevor er mir seine Dokumente überreicht, will ich von ihm wissen, warum er «auspacken» wolle. Was ihn dazu bringe, einer Journalistin Interna über das Innenleben der Überwachungsbehörden preiszugeben, für die er doch so lange und intensiv selbst gearbeitet hat?

John Doe muss nicht lange überlegen. Die Polizeiarbeit habe sich durch unsere Smartphones verändert, sagt er. Immer mehr technische Sicherheitslücken würden im Auftrag von Staaten offengehalten. Die Öffentlichkeit müsse wissen, dass «die Israelis» den Schweizer Staat und damit dessen Bürgerinnen geschröpft hätten. Und sie müsse wissen, dass sich «rechtschaffene Beamte» mit ethischem Gewissen immer weniger gegen den Überwachungseifer von kantonalen Strafverfolgungsbehörden und Bundespolizei wehren könnten.

John Doe spricht leise, sein Blick ist wach. Mit seiner höflichen Art und seinen konzisen Ausführungen erinnert er an den amerikanischen Whistleblower Edward Snowden, der 2013 die Massenüberwachung durch den US-amerikanischen Auslandsgeheimdienst NSA publik machte. Wie Snowden war John Doe überzeugt davon gewesen, das Richtige zu tun, als er beschlossen hatte, sein Informatik-Know-how in den Dienst des Staates zu stellen. Und wie Snowden konnte John Doe die zunehmende technische Überwachung immer weniger mit seinen Werten vereinbaren.

Die meisten Aussagen von John Doe können anhand von öffentlich verfügbaren Dokumenten überprüft und verifiziert werden: Berichte der Eidgenössischen Finanzkontrolle, direkte Stellungnahmen der Behörden und Hintergrundgespräche mit weiteren Quellen.

Wen also meint John Doe mit «rechtschaffenen Beamten»? Und von welchen «Israelis» spricht er?

Es geht um den Dienst für die Überwachung des Post- und Fernmeldeverkehrs, kurz: Dienst ÜPF. Er ist dem Eidgenössischen Justiz- und Polizeidepartement angegliedert und führt technische Überwachungen durch im Auftrag der Kantone, des Bundesamts fürs Polizei Fedpol, der Bundesanwaltschaft und des Nachrichtendienstes – um Terroristinnen zu schnappen, Menschenhändler zu überführen und Schwerstverbrecher zu fassen.

Im Verlauf der Recherche wird mir klar: Der Dienst ÜPF ist eine komplexe Institution, die grob gesagt an zwei Fronten kämpft.

Einerseits ist sie ein Bollwerk gegen den wachsenden Datenhunger von Bundesämtern und Kantonen: Die Juristinnen und Techniker des Dienstes ÜPF ermöglichen zwar die Überwachung unseres Internets, sie wehren aber auch regelmässig nicht legitimierte Anfragen ab. Und sie versuchen sicherzustellen, dass das Aushorchen von potenziellen Straftäterinnen nicht überbordet.

Auf der anderen Seite liegt es aber natürlich auch in der Natur eines Überwachungsdienstes, Möglichkeiten zur Überwachung bewahren zu wollen. Und das heisst auch: technologische Fortschritte zu bekämpfen. Fortschritte, die vor zehn Jahren in Gang gesetzt wurden – mit den Enthüllungen Edward Snowdens im Jahr 2013. Sie hatten eine weitreichende Verschlüsselung unseres Internetverkehrs zur Folge. Was den Schutz unserer Privatsphäre erhöht. Und die Überwachung erschwert.

In diesem Jahr 2013 beginnt auch John Does Geschichte.

Die problematische Anschaffung

2013 bereitet der Bundesrat die Revision des «Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs» vor, kurz Büpf. Das Justizdepartement will die Überwachung mit einem digitalen Upgrade leistungsfähiger machen. Alle Kantone sollen die gleichen technischen Mittel erhalten, um Schwerverbrechen aufzuklären. 112 Millionen Franken sind für das gesamte Überwachungsprogramm vorgesehen.

Im Dezember 2013 unterzeichnen die Beamten vom Dienst ÜPF einen Vertrag mit einem israelisch-amerikanischen Unternehmen namens Verint. Projektname: «Firefly». Es geht um die Beschaffung einer neuen Komponente für die Echtzeitüberwachung namens Interception System Schweiz, kurz: ISS. Sie ist das Herzstück des «Verarbeitungssystems zur Fernmeldeüberwachung FMÜ», in dem alle Daten aus Telefonie, SMS, Standort-

ortung und Internetverkehr zusammenfliessen und für Kantonspolizisten und Staatsanwältinnen lesbar gemacht werden.

Das Projekt «Firefly» wirft rasch Fragen auf. Der damalige Waadtländer SP-Nationalrat Jean-Christophe Schwaab etwa findet, wer bei einer Firma wie Verint Geräte bestelle, könne «den Schlüssel dazu gerade so gut gleich der NSA übergeben». Denn Verint arbeitet eng mit dem US-Geheimdienst zusammen. Heute hat das Unternehmen seinen Hauptsitz in Melville, New York, ursprünglich war es ein Tochterunternehmen des israelischen Softwarekonzerns Comverse Technology, der nach wie vor Anteile an Verint hält. Bis heute pflegt Verint enge Verbindungen zum israelischen Geheimdienst. Ob das Überwachungssystem tatsächlich Hintertüren für Geheimdienste offen hält, ist bis heute nicht klar.

Allgemein lässt sich sagen: Die Zusammenarbeit mit Israel wird von den Bundesbehörden bis heute wenig hinterfragt. Beschaffungen von israelischen Produkten im Bereich Rüstung, Strafverfolgung und Terrorismus haben vielmehr fast schon Tradition: So entwickelt das israelische Rüstungsunternehmen Elbit Systems heute an seinem Schweizer Standort in Uetendorf das neue Funkgerätesystem für die Schweizer Armee, wie die WOZ kürzlich recherchierte. Zudem kauft die Schweiz bei etlichen israelischen Sicherheitsunternehmen sogenannte Spyware ein – also invasive Spionagesoftware, die auf Smartphones von Straftäterinnen oder Terroristen geladen werden kann.

Die Retter in der Not

Zurück ins Jahr 2014. Auch Balthasar Glättli, der Zürcher Nationalrat der Grünen, äussert sich damals kritisch zum Verint-Deal: In der parlamentarischen Fragestunde will er wissen, warum der Auftrag für das Überwachungssystem nicht an ein Schweizer Unternehmen gegangen sei. Justizministerin und SP-Bundesrätin Simonetta Sommaruga antwortet darauf: Kantone, Bund und Strafverfolgungsbehörden hätten sich «einstimmig für dieses System» ausgesprochen.

Sie nennt auch einen weiteren zentralen Punkt: Das System von Verint sei das einzige, das «Gewähr bietet, die Fernmeldeüberwachung ohne Unterbruch sicherzustellen».

Faktisch hatte das Justizdepartement nämlich schlicht keine Alternative. Es stand kurz vor einem Riesendebakel, die Israelis waren die Retter in der Not. 2008 hatte der Bundesrat beschlossen, das damalige Überwachungssystem LIS zu erneuern, weil es veraltet und nicht mehr zeitgemäss war. Das Justizdepartement hatte sich bei der Suche nach Ersatz in einem Einladungsverfahren für das Angebot einer Berner Beratungsfirma namens Exanovis entscheiden. Doch deren System ISS wurde nie abnahmefähig geliefert. Es leide an «klaren technischen Mängeln», stand im Februar 2013 im Auditbericht. Die Komplexität sei unterschätzt worden, da es für den Lieferanten «das erste Projekt in dieser Grössenordnung» gewesen sei. Exanovis stellte 2014 den Betrieb ein.

18 Millionen Franken waren für teure Beraterinnen in den Sand gesetzt geworden. Und als im Sommer 2013 die parlamentarische Beratung der Gesetzesrevision beginnt, steht das Departement ohne ISS da.

In diesem Moment meldet sich Robert Lander.

Lander arbeitet zu der Zeit für Syborg, die Tochterfirma des israelisch-amerikanischen Unternehmens Verint. Genau diese Syborg im deutschen Saar-

land hat das Überwachungssystem LIS betrieben, das es nun abzulösen gilt. Robert Lander, gemäss einem weiteren Insider ein hervorragender Verkäufer, ist bestens vernetzt bei den Kantonspolizeien in Zürich, Waadt und Bern. Und jetzt inszeniert er sich als Retter. Als John Doe davon erzählt, sitzt er mit kerzengerader Haltung auf dem Sofa. Er sagt: Wenn die Systemlieferantin – also Syborg – bei den Kunden ihres Dienstes – also den Kantonspolizeien – direkt lobbyiere, «dann wird es schwierig für den Dienst, sich dem zu widersetzen». John Doe wirkt angespannt. Über Verint und Syborg spricht er nicht gerne, bei jedem unserer Treffen fürchtete er, dass diese davon Wind bekommen könnten. «Mit ihnen ist nicht zu spassen», sagt er.

Im Namen von Verint, dem Mutterkonzern mit Sitz im israelischen Herzlia, offeriert Robert Lander am 9. August 2013 die technische Lösung für das Interception System Switzerland 2, kurz ISS 2 (die Nummer «2» kommt daher, dass der erste Versuch der Firma Exanovis gescheitert war). Das System dient – simpel gesagt – der Echtzeitüberwachung von Telefonie und Internet und der Lokalisierung von Zielpersonen.

Beim Produkt handelte es sich um eine Standardsoftware, die die Israelis weltweit verkauft haben. Es sei aber auch eine Blackbox, kritisiert die Eidgenössische Finanzkontrolle 2014. Deshalb habe der IT-Dienstleister des Justizdepartements «nur beschränkten Einfluss auf die verbauten Technologien».

Die Finanzkontrolle hält auch fest: ISS 2 sei «mit den Sicherheitsweisungen des Bundes nur begrenzt kompatibel», weshalb «viele Ausnahmegenehmigungen notwendig» seien, die auch erteilt worden seien. Durch «die verspätete Erstellung und Genehmigung des Sicherheitskonzeptes» bestehe das Risiko, dass «Nachbesserungen an technischen und/oder betrieblichen Konzepten notwendig werden».

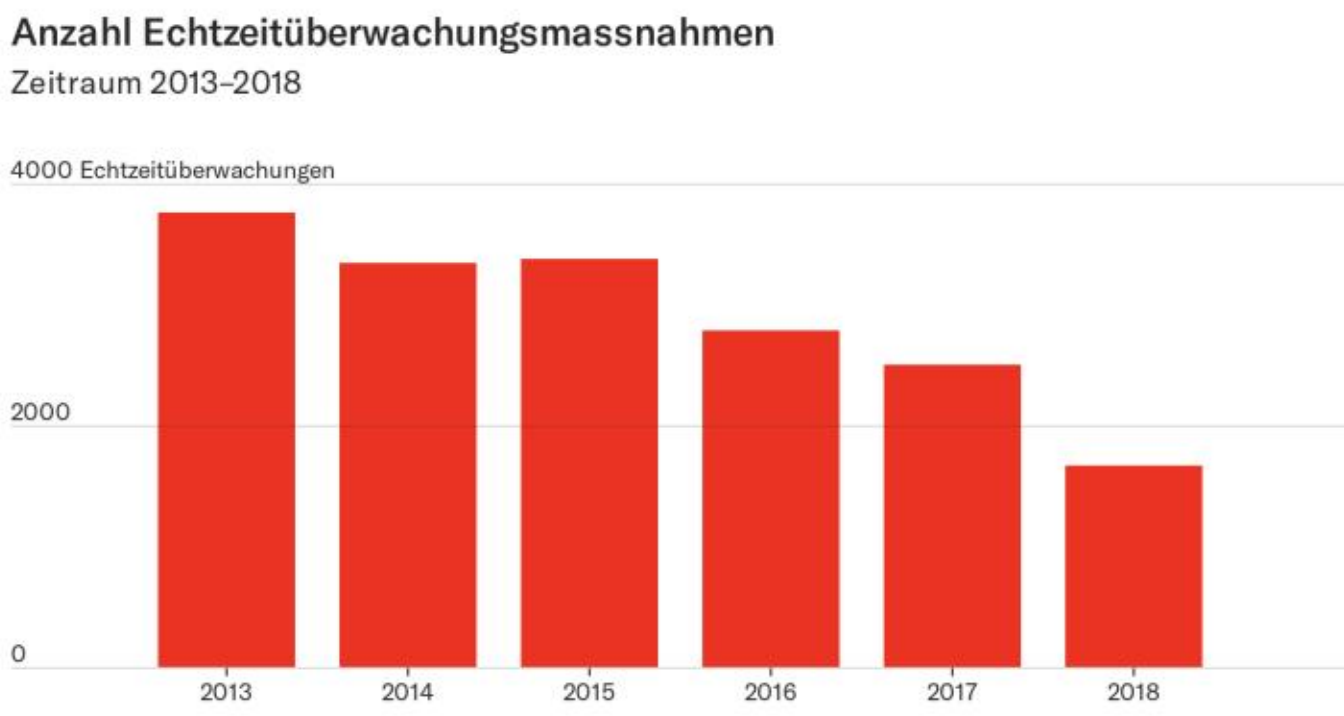
John Doe sagt: «Lander konnte alles diktieren, die Funktionen und auch den Preis.» Denn das Justizdepartement habe notgedrungen zuschlagen müssen, ohne eine Ausschreibung machen zu können. Ansonsten hätte ein «Totalausfall der Telekommunikationsüberwachung» gedroht, sagt der ehemalige Überwachungsspezialist.

Wie wichtig das Geschäft offenbar war, zeigt folgende Zahl: Im Jahr 2014, als ISS 2 dann eingeführt wurde, flog insgesamt 12-mal eine Delegation des Justizdepartements nach Tel Aviv, wie ein Departementssprecher auf Anfrage sagt. Zum Vergleich: In den Jahren danach waren es jeweils 5- bis 6-mal.

Doch etwas ist seltsam.

Ein Blick in die Statistik zeigt: Zum Zeitpunkt des Vertragsabschlusses mit Verint im Jahr 2013 ist die Schweiz in einem «Überwachungshoch»: Bund und Kantone veranlassen in diesem Jahr insgesamt 3700 Echtzeitüberwachungen: ein Rekordwert. Und das mit dem veralteten System, das dringend abgelöst werden sollte.

Danach aber geht es bergab. Mit ISS 2 hören Bund und Kantone von Jahr zu Jahr weniger Telefonate ab, verfolgen weniger Google-Suchanfragen und lesen weniger E-Mails mit. 2018 waren nur es noch 1676 Massnahmen.



Quelle: https://www.li.admin.ch/de/stats

Der Rückgang hat einen Grund. Das System der israelisch-amerikanischen Firma versagt bei einer seiner Kernaufgaben: der Internetüberwachung.

Von der Verschlüsselung überholt

An eines unserer Treffen bringt John Doe das Handbuch zur Verint-Software mit. Darin ist abgebildet, wie der gesamte Internetverkehr einer überwachten Person mitgelesen werden kann. Verint verspricht den Polizistinnen Zugang zu jeder Website und jeder Suchanfrage einer mutmasslichen Straftäterin.

Doch die Sache hat einen grossen Haken: Sämtliche Abbildungen zeigen Beispiele mit HTTP-Standard an. Die Software ist also auf dem technologischen Stand von 2013. Die Snowden-Enthüllungen im selben Jahr haben allerdings zur Folge, dass die wichtigsten Techunternehmen wie Apple, Mozilla und Google danach eine Transportverschlüsselung (HTTPS) in ihre Browser und App-Stores integrierten. Damit werden alle Datenpakete verschlüsselt – und offensichtlich gelingt es in der Folge nicht, die Verint-Software so anzupassen, dass sie genügend nützliche Informationen aus den verschlüsselten Daten gewinnen kann.

So erfahren Sie, welche Daten über Sie bei Ihrem Telefonanbieter gespeichert sind

Wollen Sie wissen, welche Daten über Sie im Fall einer «rückwirkenden Überwachung» an die Strafverfolgung weitergegeben werden? Alle Schweizer Telecomkonzerne liefern diese Informationen mit wenigen Klicks. Swisscom beispielsweise schickt ihren Kundinnen innert 5 Minuten nach Bestellung umfangreiche CSV-Dateien.

In der Datei «Network Access» zum Beispiel sind die Adressen aller Antennen gelistet, mit denen unser Handy kommuniziert – und damit auch unser jeweiliger Standort. Diese Informationen sind bei Ihrem Telecomanbieter sechs Monate lang gespeichert. Das heisst auch: Über ausnahmslos jede Person in der Schweiz, die einen Handyvertrag bei einer Schweizer Firma hat, kann eine «rückwirkende Überwachung» angeordnet werden.

Sollten Sie aus irgendeinem Grund in das Visier der Strafverfolgungsbehörden geraten, dann hätten Sie maximal 60 Minuten Zeit, Ihre digitalen Spuren zu verwischen. So lange dauert es während Bürozeiten, bis eine Echtzeitüberwachung eingerichtet ist.

John Doe beschreibt die Entwicklung so: «Die Überwachungsbehörden kauften also für mehrere Millionen ein System ein – und plötzlich stellte die gesamte Internetwelt grossflächig auf HTTPS um. Eine Riesendemütigung!» Als das neue Bundesgesetz Büpf im März 2018 in Kraft tritt, ist das fünf Jahre zuvor gekaufte Verint-System bereits wieder veraltet. «Die Polizei in den Kantonen war blind, und alle lachten den Dienst ÜPF aus», sagt John Doe. Denn nun sahen die Strafverfolgerinnen nur noch, welche Webseite ein Verbrecher ansteuert und welche App er nutzt, aber nicht, was er genau damit macht (Beispiel: Die Polizisten können live mitverfolgen, dass der Verbrecher Republik.ch aufruft, wissen aber nicht, welchen Artikel er anklickt).

Auch im Bericht der Finanzkontrolle vom 23. November 2018 sind diese Missstände dokumentiert: «Die zunehmende Verschlüsselung der Kommunikation, beispielsweise durch Skype, Whatsapp oder Telegram, mindert den Nutzen der FMÜ [Fernmeldeüberwachung]», steht darin. Es bestehe ein Risiko, dass deshalb «vermehrt auf FMÜ-Massnahmen verzichtet» werde.

Die Abkehr von der Flop-Software

«Die Lieferantin konnte das System nicht an die neuen technologischen Realitäten anpassen», räumt auch Jean-Louis Biberstein im Gespräch ein. Er ist Leiter der Abteilung Recht und Controlling und Mediensprecher des Dienstes ÜPF. Anders als die anderen, deutlich verschwiegeneren Sicherheitsbehörden wie das Fedpol oder der Bundesnachrichtendienst NDB ist der Überwachungsdienst um einen direkten Draht zu Medienschaffenden bemüht. So lädt er Journalistinnen auch mal direkt an den Sitz im modernen Verwaltungsgebäude im bernischen Zollikofen ein, wo auch das Bundesamt für Informatik und Telekommunikation residiert. Im lichtdurchfluteten Gebäude präsentiert sich der Überwachungsdienst fast schon als hippes Start-up: mit bequemen Sofaecken, Telefonboxen, Stehpulten und Mitarbeitern, die in weissen Sneakers herumlaufen.

Hier residiert der Überwachungsdienst jedoch erst seit 2021. Davor befand er sich in Bern an der Fellerstrasse, wo er vor sieben Jahren das Verint-Management hinzitierte. Denn der Verschlüsselungsflop hatte die Verantwortlichen im Justizdepartement erzürnt. Die Verint-Manager machten etliche Versprechungen, wie sie ISS 2 verbessern würden. Und liessen sich in der Folge jegliche Zusatzarbeit an der Software verrechnen.

Insgesamt erhielt Verint 24 Millionen Franken vom Schweizer Staat, wie der Überwachungsdienst mitteilt. Für ISS 2 budgetiert gewesen waren 14 Millionen Franken. Viel Spielraum habe der Überwachungsdienst damals nicht gehabt, sagt John Doe. Denn er war abhängig von den Israelis. Sonst hätte es keine Echtzeitüberwachungen mehr gegeben.

Irgendwann wird der Frust bei den Bundesbeamten über die Verint-Software so gross, dass auch Landers Netzwerk nichts mehr ausrichten kann. Das Justizdepartement entscheidet sich im Herbst 2018, ISS 2 nicht mehr weiter auszubauen, sondern es mit neuen Komponenten zu ergänzen, die eine «flexiblere Reaktion auf neue Technologien wie die vermehrte Verschlüsselung» ermöglichen. Und das Verint-System so schnell wie möglich loszuwerden.

Das Justizdepartement will aus dem Desaster seine Lehren ziehen: Das Nachfolgeprodukt soll eine komplette Eigenentwicklung sein. Das heisst:

Eine externe Firma soll das Produkt unter Regie des Departements entwickeln und komplett auf das Schweizer Überwachungsrecht zuschneiden.

Der Nachfolger von ISS 2 heisst Flicc und wurde von der Zürcher Firma Adnovum entwickelt, ist also «Swiss made». Flicc wird 2024 vollständig in Betrieb sein, das System der Israelis spätestens 2025 eingestellt.

Der staatspolitische Kniff

Tragikomisch ist auch, dass das System ISS 2 durchaus einige sehr nützliche Funktionen hatte – nur durften diese zum Teil nicht legal genutzt werden.

«Am meisten taugte das System ISS 2 für die Visualisierung von Bewegungsdaten und die Analyse von Audioaufnahmen», sagt John Doe. Bei der Visualisierung geht es um Folgendes: Jede Tatverdächtige kann innert Minuten geortet werden, weil jedes Smartphone ständig seine Position an eine Funkzelle meldet. Und aus jedem Zellenwechsel lässt sich nun mit ISS 2 ein Bewegungsprofil erstellen.

Dass das Feature «Kartenfunktion» bereits 2013 mitverkauft wurde, belegen die Dokumente, die John Doe an eines unserer Treffen mitbringt. Im Handbuch wird erklärt, wie sich mit wenigen Klicks ein Bewegungsprofil erstellen lässt. Wenn zum Beispiel eine pädophile Person überwacht wird, wird ein sogenannter «Geo-Zaun» eingerichtet – um Schulhäuser oder Kindergärten. Sobald der Verdächtigte in der Nähe auftaucht, schlägt ISS 2 Alarm.

Doch genau für diese Profile, Visualisierungen und Analysen fehlt eine «explizite Gesetzesgrundlage», wie auch der Bundesrat später festhält.

Der Überwachungsdienst weiss, dass er jedes technische Detail zur Überwachung im Gesetz abbilden muss. Denn sonst folgt reflexartig Widerstand aus der überwachungskritischen Zivilgesellschaft.

Um also Rechtssicherheit zu schaffen, muss die Kartenfunktion irgendwie legalisiert werden. Doch wie? Das Bundesgesetz ist 2018 soeben revidiert worden, ebenso die Verordnung. Was nun folgt, ist, je nach Interpretation, ein juristischer Geniestreich – oder ein staatspolitisch höchst fragwürdiges Vorgehen.

Erik Schönenberger sitzt im Juni 2023 im dritten Stock der Zürcher Zentralwäscherei im Büro der Digitalen Gesellschaft, er ist der Geschäftsleiter. Im selben Stockwerk residieren auch ein «Hackerspace»-Kollektiv, das einen offenen Raum für digitale Kunst, Wissenschaft und Technologie bieten möchte, der Chaos Computer Club Zürich oder die Linux User Group. An diesem Freitagnachmittag stehen Club-Mate-Flaschen sowie leere Kaffeetassen herum, überall blinkt es, jemand testet gerade Lautsprecher für ein kleines Soundexperiment.

Als ich Schönenberger auf dem grossen Bürotisch die Auszüge aus dem Verint-Handbuch vorlege, fallen ihm die «Tomaten von den Augen», wie er selber sagt. Nun ergebe alles Sinn. Es seien praktisch dieselben Kartenabbildungen, die er einmal «über drei Ecken» zugesteckt bekommen habe.

Worum geht es?

Im Jahr 2019 hatte der Bundesrat die Vernehmlassung über ein «Bundesgesetz über administrative Erleichterungen und die Entlastung des Bundeshaushalts» eröffnet, die Digitale Gesellschaft war damals nicht eingeladen. Dabei handelt es sich um ein sogenanntes Mantelgesetz, das Änderungen in verschiedenen Regelwerken zur Folge hat. So auch im Büpf, in

dem die Kostenfrage für die Überwachungsmassnahmen neu geregelt wurde.

Doch nebenbei liess das Justizdepartement auch noch zwei inhaltliche Änderungen bei Artikel 7 reinschmuggeln – was lediglich in der Botschaft erwähnt wurde. Dort heisst es:

> Neu wird in Artikel 7 Buchstabe d präzisiert, dass die Bearbeitungsfunktionen des Verarbeitungssystems des Dienstes ÜPF auch Analysefunktionen einschliessen.

Nun lautet dieser Artikel 7, Buchstabe d folgendermassen:

> Das Verarbeitungssystem dient dazu: Bearbeitungsfunktionen, einschliesslich Analysefunktionen, wie Visualisierung, Alarmierung oder Sprechererkennung, für die im System gespeicherten Daten anzubieten.

Als der Überwachungsdienst im März 2022 mitteilte, dass nun die «gesetzliche Grundlage für die Analysefunktionen» geschaffen worden seien, gab es in der Medienmitteilung keinerlei Hinweis darauf, dass dies über das Vehikel «Bundesgesetz über administrative Erleichterungen und die Entlastung des Bundeshaushalts» geschehen war.

Per Zufall erfuhr Schönenberger davon, dass hier durch die gesetzliche Hintertür eine wichtige Überwachungsfunktion legalisiert werden sollte. In einem Communiqué wies die Digitale Gesellschaft umgehend darauf hin, das Gesetz sei «keine Finanzvorlage, sondern eine Mogelpackung», da es hier um «einen Ausbau der Ermittlungsmöglichkeiten der Strafverfolgungsbehörden und des Geheimdienstes» gehe.

Doch der Protest verhallte. Die Änderungen traten alle in Kraft.

«Keine elegante Lösung»

Die Geoinformationen können also erst seit 2022 legal ausgewertet werden. Doch die Funktion ist in der Praxis entscheidend. «Ohne Visualisierungsfunktion hat ein Polizist einfach eine Tabelle mit 300-Antennenkoordinaten erhalten», sagt Schönenberger. «Damit kann jemand ohne technische Kenntnisse nichts anfangen.» Natürlich brauche es da ein Tool, das Bewegungsdaten visualisiere. Seine These wird in der Botschaft zum «Bundesgesetz über administrative Erleichterungen und die Entlastung des Bundeshaushalts» bestätigt: Die Visualisierungsfunktion stelle für die kantonalen Strafverfolgungsbehörden «eine wesentliche Entlastung dar, da sie die Daten nicht exportieren und einen Dritten mit der Datenanalyse beauftragen (...) müssen».

Das Verint-Handbuch beweist: Die Kartenfunktion wurde von Anfang an mitgeliefert. Und der Überwachungsspezialist John Doe und andere Insider bestätigen: Sie wurde von einigen Kantonen und Behörden auch genutzt. Davon geht auch Schönenberger aus: «Schlussendlich wird einfach angewendet, was technisch schon da ist.»

Weshalb hat die Überwachungsbehörde diese Funktion in eine sachfremde Vorlage versteckt? Mediensprecher Biberstein räumt ein, dass das «keine elegante Lösung» gewesen sei. Aber man habe wegen ein paar wenigen Funktionen nicht eine gesamte neue Revision durchführen wollen. Er weist zudem darauf hin, dass das Büpf alle Grundsätze des Datenschutzes einhalte.

Verordnung sorgte für Aufschrei

Wie die Überwachungsbehörde an der zunehmenden Verschlüsselung des Internets verzweifelt, zeigt sich auch bei der Vorratsdatenspeicherung. Dabei geht es um die bereits erwähnte Datensammlung, zu der die Schweizer Telecomkonzerne verpflichtet sind und durch die die Behörden in Erfahrung bringen können, wo sich eine Person in den letzten sechs Monaten aufhielt und mit wem sie telefonierte.

Viele EU-Staaten haben ähnliche Gesetze. Die Digitale Gesellschaft versucht am Europäischen Gerichtshof für Menschenrechte in Strassburg die Schweizer Vorratsdatenspeicherung ebenfalls wieder rückgängig zu machen. Das Urteil wird womöglich dieses Jahr gefällt und wegweisend sein.

Bereits 2018 wollten die Überwacher vom Dienst ÜPF auch die Schweizer Kommunikationsdienste zur Vorratsdatenspeicherung verpflichten, die explizit mit Datenschutz werben – den Schweizer Messengerdienst Threema und den E-Mail-Dienst Proton. Für Threema, damals noch ein kleines Schweizer Start-up, wäre eine solche Verpflichtung ein massiver Eingriff ins Geschäftsmodell gewesen, was Politikerinnen schon während der Beratung 2014 im Parlament stark kritisierten. Das global tätige Unternehmen wehrte sich dagegen mit allen juristischen Mitteln – und mit Erfolg: Threema muss dank einem Bundesgerichtsurteil vom 17. Mai 2021 die Daten nicht auf Vorrat speichern, dasselbe gilt auch für Proton gemäss Bundesverwaltungsgericht.

Als der Überwachungsdienst merkte, dass er mit den Verfügungen gegen Schweizer Unternehmen, die stark auf Datenschutz setzen, nicht wirklich weiterkommt, startete er 2022 einen neuen Versuch, diese in die Knie zu zwingen: über den Verordnungsweg. Bei der Revision der Verordnung zum Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs im Sommer 2022 machte er die Vorgabe, dass alle Schweizer Kommunikationsdienste die eigenen Verschlüsselungen aufheben müssen. Ein Aufschrei ging durch die Medien.

Die Piratenpartei und die Digitale Gesellschaft mutmassten, dass der Schweizer Überwachungsdienst die Chatkontrolle der EU kopieren wolle. Das heisst: Eine Technologie auf unseren Smartphones scannt Nachrichten in Apps wie Whatsapp massenhaft etwa auf Kindsmissbrauchsmaterial und leitet Funde an die Strafverfolgung weiter. Damit wäre eine der wichtigsten technologischen Errungenschaften unterwandert: die Ende-zu-Ende-Verschlüsselung.

Der Dienst ÜPF beschwichtigte gegenüber Medienschaffenden: Niemand wolle die Ende-zu-Ende-Verschlüsselung aufheben. Dennoch hat er den umstrittenen Artikel aus der Verordnung entfernt.

Ein erstes Paket der Revision trat am 1. Januar 2024 in Kraft, ein weiterer Teil steht noch aus.

Warum die Behörden 5G nicht mögen

Eine weitere Begründung der Behörde für das Update der Revision: die «Schliessung von Überwachungslücken wegen technologischer Weiterentwicklung». Was mit dieser kryptischen Formulierung gemeint war: der neue Mobilfunkstandard 5G. Dieser ist, was wenig bekannt ist, ein Fortschritt für die Privatsphäre – und drohte die Überwachung tatsächlich massiv zu erschweren.

Zum einen ermöglicht der neue Standard zwar eine noch präzisere Lokalisierung als bei 4G, was eine bessere «Qualität der Überwachungsdaten» ermöglicht, wie der Überwachungsdienst auf Anfrage schreibt (was auch die Suche nach vermissten Personen vereinfachen würde). Doch die neuen 5G-Standards schaffen auch neue technische Hürden für Ortung – was den Bundesbehörden gar nicht gefällt. Das internationale Normierungsgremium 3GPP für Mobilfunk hat nämlich beschlossen, dass die Identifikatoren unserer Smartphones verschlüsselt mit den Antennen kommunizieren sollen. Nicht nur das: Die verschlüsselten IDs unserer Geräte sollen auch permanent ändern. Das erschwert das «Abfangen» von Mobilgerätekennungen durch die Polizei. Damit die Büpf-Gesetzestexte also nicht zur Makulatur werden, mussten alle genannten technischen Parameter angepasst werden.

Bei 5G verlieren auch sogenannte Imsi-Catcher an Wert, die von Kantonspolizistinnen genutzt werden. Mit diesen Geräten wird eine Funkzelle «simuliert», sodass die Telefonnummern von Verdächtigen bestimmt werden können. Oftmals sitzen Polizistinnen dafür in einem Van oder in einem Helikopter und umkreisen einen Ort, bei dem sie Verbrecherinnen vermuten. Dann verbindet sich das Telefon der Täter mit den Imsi-Catchern, und die Polizisten erfahren über das Verarbeitungssystem die zugehörige Telefonnummer – und können ihre Überwachungsaktion starten.

Weil der neue 5G-Standard solche Massnahmen erschwert, schickt der Überwachungsdienst seine besten Ingenieure regelmässig zu den Meetings der internationalen Normierungsgremien. Um Kompromisse zu finden, die die gesetzeskonforme Überwachung durch den Staat weiterhin möglich machen. Wann Swisscom, Salt und Co. 5G als technischen Standard für das gesamte Internet ausrollen, ist derweil noch ungewiss.

Das Mittel der Wahl: Trojaner

Wagen wir ein vorläufiges Fazit: Überwachungsbehörden mögen Verschlüsselungen nicht. Egal, ob diese den Internetverkehr, eine Messenger-App oder die Kommunikation unserer Handys mit Antennen schützen. Der Kampf des Schweizer Staats gegen die technologischen Errungenschaften ist zäh – und er wird nicht so bald aufhören.

Die Behörden rüsten weiter auf. Fedpol und Nachrichtendienst beschaffen sich insbesondere Analysetools, mit denen sie auch aus Metadaten oder Geräteinformationen immer mehr Erkenntnisse gewinnen können. «Oft lässt sich daraus schon eine Menge ableiten», sagt John Doe.

Doch wenn Strafverfolger oder Mitarbeiter von Geheimdiensten allein mit den Metadaten nicht mehr weiterkommen, müssen sie irgendwie an den Kommunikationsinhalt in Mails oder Chats gelangen. Daran, was Kriminelle, Spioninnen, Staatsfeinde oder Terroristen nun effektiv digital verhandeln oder planen. Um präventiv eingreifen zu können.

Und dieser Zugriff erfolgt am effektivsten mithilfe von Staatstrojanern. Sie ermöglichen den Zugriff auf die Inhalte und brechen sämtliche Verschlüsselungen unserer Endgeräte.

Es ist der krasseste Eingriff in die Privatsphäre. Und er verursacht massive Kollateralschäden. Der Staat nutzt dabei dieselben Sicherheitslücken wie Cyberkriminelle und Hackerinnen. Die Kantone, Staatsanwaltschaften und das Fedpol haben in den letzten Jahren die Nutzung dieser Super-Spionagewerkzeuge intensiviert.

Darum wird es im dritten und letzten Teil dieser Serie gehen.

Der kontinuierliche Ausbau des technischen Überwachungsapparats müsse gestoppt werden, sagt John Doe in unserem letzten Gespräch. Eine Erkenntnis, die dazu führte, dass er nun in anderen Politikfeldern als der Strafverfolgung arbeitet. «Der Schweizer Staat will immer mehr Überwachung. Doch mehr Überwachung bewirkt oft nicht mehr Sicherheit.» Die Bürgerinnen würden einfach nur beginnen, sich selbst zu zensieren.