Foto/Grafik: gemeinfrei

Trojaner-Überwachung viel umfassender als angekündigt

Im Gesetzesentwurf steht kein Wort über eine Beschränkung auf WhatsApp und andere Chatprogramme, wie seitens des Justizministeriums wiederholt behauptet worden ist. Vielmehr soll jedes einzelne Datenpaket aus dem Netz erfasst werden bis hin zu maschinengenerierten Daten.

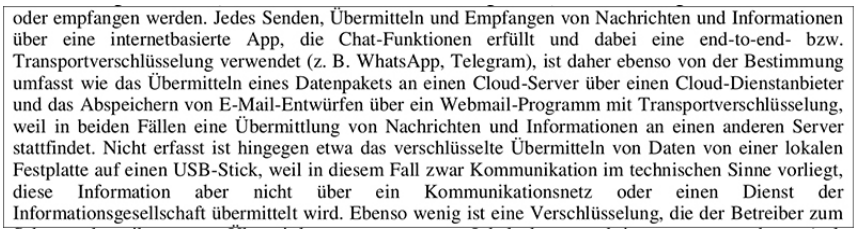
Von **Erich Möchel** <http://fm4.orf.at/tags/erichmoechel>

Die Überwachung verschlüsselter Kommunikation im „Sicherheitspaket" geht weit über alles schon Dagewesene hinaus. Waren es bisher Telefonie, SMS und Standortdaten, so fallen nun grundsätzlich sämtliche Daten darunter, die zwischen dem überwachten Gerät und dem Netz ausgetauscht werden. Von einer Beschränkung auf die Überwachung von WhatsApp und anderen Kommunikationsprogrammen, wie sie Justizminister Wolfgang Brandstetter wiederholt behauptet hatte, ist im Gesetzentwurf überhaupt keine Rede.

Vielmehr wird bereits einleitend betont, dass jedes einzelne Datenpaket aus dem Internet erfasst werden soll und dass alle maschinengenerierten Daten darunter fallen. Damit sind auch die regelmäßigen Abgleiche des lokalen Datenspeichers mit dem externen Back-up eines Nutzers in der „Cloud" dabei. Bei mobiler „Cloud"-Nutzung ist ein externer Speicher schon der Regelfall. Das führt die ohnehin fragwürdige Abgrenzung der „Kommunikationsüberwachung" zur „Onlinedurchsuchung" ad absurdum, denn dieselben Datensätze auf dem Speichermedium des Endgeräts zu durchsuchen ist bei „Kommunikationsüberwachung" verboten.

Zwei Drittel der Erläuterungen zum Gesetzestext sind - wie berichtet - nur dieser Abgrenzung gewidmet, weil „Kommunikationsüberwachung" einfacher genehmigt werden kann. Obendrein sieht der neue Paragraf 135a (3) vor, dass auch in Wohnungen eingebrochen werden darf, um die zur Überwachung nötige Trojaner-Schadsoftware auf einem Gerät zu installieren.

Wie aus den Erläuterungen klar hervorgeht, wurde über die Grundrechte österreichischer Bürger nur unter dem Aspekt diskutiert, **dass staatliche Zugriffe möglichst erleichtert werden sollen** <http://fm4.orf.at/stories/2854246/>.



oder empfangen werden. Jedes Senden, Übermitteln und Empfangen von Nachrichten und Informationen über eine internetbasierte App, die Chat-Funktionen erfüllt und dabei eine end-to-end- bzw. Transportverschlüsselung verwendet (z. B. WhatsApp, Telegram), ist daher ebenso von der Bestimmung umfasst wie das Übermitteln eines Datenpakets an einen Cloud-Server über einen Cloud-Dienstanbieter und das Abspeichern von E-Mail-Entwürfen über ein Webmail-Programm mit Transportverschlüsselung, weil in beiden Fällen eine Übermittlung von Nachrichten und Informationen an einen anderen Server stattfindet. Nicht erfasst ist hingegen etwa das verschlüsselte Übermitteln von Daten von einer lokalen Festplatte auf einen USB-Stick, weil in diesem Fall zwar Kommunikation im technischen Sinne vorliegt, diese Information aber nicht über ein Kommunikationsnetz oder einen Dienst der Informationsgesellschaft übermittelt wird. Ebenso wenig ist eine Verschlüsselung, die der Betreiber zum

Foto/Grafik: gemeinfrei

Cloud ja, USB-Stick nein. Aus den **Erläuterungen zum geänderten Text der Strafprozessordnung** <https://www.ris.bka.gv.at/Dokumente/Begut/BEGUT_COO_2026_100_2_1389702/COO_2026_100_2_1389732.pdf>

Back-ups in der Cloud sind „Internetkommunikation"

„Jedes Senden, Übermitteln und Empfangen von Nachrichten und Informationen über eine internetbasierte App, die Chat-Funktionen erfüllt und dabei eine end-to-end- bzw. Transportverschlüsselung verwendet (z. B. WhatsApp, Telegram), ist daher ebenso von der Bestimmung umfasst wie das Übermitteln eines Datenpakets an einen Cloud-Server", heißt es dazu in den Erläuterungen zum Gesetzestext.

Da eben auch Maschinenkommunikation erfasst wird, ist jeder Routineabgleich lokaler Adressbücher und sämtlicher anderer Daten mit einem Back-up-Konto in der Cloud dabei. Wird eine solche Routinesicherung lokaler Daten auf einem Server neu angelegt, wird auch der gesamte Inhalt des lokalen Speichermediums abgegriffen, ohne dass dabei der juristische Sachverhalt einer „Onlinedurchsuchung" gegeben ist. Ein Back-up auf einer lokalen Disk oder einem USB-Stick ist für die Ermittler hingegen tabu, wenn es verschlüsselt wurde.

In EU-Gremien wird hingegen über **alternative Ermittlungsmöglichkeiten ohne Einsatz von Trojaner-Schadsoftware diskutiert** <http://fm4.orf.at/stories/2853764/>.

„Messwerte, Regelungs- und Alarmimpulse"

Weil jedes Datenpaket als „Internetkommunikation" bewertet wird, fallen auch „Messwerte sowie Regelungs-, Steuerungs- und Alarmimpulse" darunter, heißt es in den Erläuterungen. Daher sind „Smart Homes" oder Anwendungen für den Steuerungs- und Produktionsbereich - bekannt als „Industrie 4.0" - legitime Überwachungsziele, ohne dass es dafür eine richterliche Genehmigung für eine Hausdurchsuchung braucht.

Hier schließt sich das österreichische Justizministerium einfach der Rechtsmeinung des deutschen Bundesverfassungsgerichtshofs an. Auch wenn bei Internetüberwachung wesentlich mehr und andere Daten als bei Telefonüberwachung anfielen, so seien das „lediglich Einzelakte einer oft nur kurzen und oberflächlichen Telekommunikation". Das führt zu dem Schluss, dass „die Internetüberwachung sogar weit weniger eingriffsintensiv als eine Hausdurchsuchung ist".

Die im „Sicherheitspaket" geplante neue Vorratsdatenspeicherung <http://fm4v3.orf.at/stories/1776727/> spießt sich insofern, als die Mobilfunker die geforderten IP-Adressen derzeit gar nicht haben.

"... in geschützte Räume einzudringen"

Ein Wohnungseinbruch, um in „durch das Hausrecht geschützte Räume einzudringen, Behältnisse zu durchsuchen und (...) Sicherheitsvorkehrungen zu überwinden", ist laut Gesetzesentwurf jedoch ein legitimes Mittel, um Trojaner-Schadsoftware auf ein Gerät aufzubringen, wenn es dafür keine andere Möglichkeit gibt. Dafür braucht es dann allerdings eine weitere richterliche Genehmigung, heißt es in den Erläuterungen. Nicht näher ausgeführt wird, ob mit dieser Ermächtigung zum Einbruch und zum Durchsuchen von „Behältnissen" auch die Lizenz für eine Durchsuchung einer Festplatte enthalten ist.

(3) Soweit dies zur Durchführung der Ermittlungsmaßnahme unumgänglich ist, ist es zulässig, in eine bestimmte Wohnung oder in andere durch das Hausrecht geschützte Räume einzudringen, Behältnisse zu durchsuchen und spezifische Sicherheitsvorkehrungen zu überwinden, um die Installation des Programms zur Überwachung verschlüsselter Nachrichten in dem Computersystem zu ermöglichen. Die Eigentums- und Persönlichkeitsrechte sämtlicher Betroffener sind soweit wie möglich zu wahren.

Foto/Grafik: gemeinfrei

Der neue Paragraf 135a sieht in Ziffer (3) den Einbruch in Wohnungen, das Überwinden von Sicherheitsmechanismen und das Durchsuchen von Behältnissen vor, um durch die Installation eines Trojaners eine Überwachungsmaßnahme zu ermöglichen, die angeblich „weit weniger eingriffsintensiv" ist als eine

Hausdurchsuchung. **Die gesamten Änderungen der Strafprozessordnung in einer Gegenüberstellung** <https://www.ris.bka.gv.at/Dokumente/Begut/BEGUT_COO_2026_100_2_1389702/COO_2026_100_2_1389733.html>

Dass eine einzige, zeitlich beschränkte Überwachung des Internetverkehrs einer Person die gesamte Kommunikation einer ganzen Gruppe von Personen in Wort, Bild und Video zutage fördern kann, wird nicht erwähnt. Das Abgreifen der Log-in-Daten einer Person öffnet zum Beispiel den Zugang zu einem Forum, das die gesamte Diskussion aller Beteiligten über einen längeren Zeitraum abbildet. Ebenso wenig wird ausgeführt, was mit den abgefangenen Passwörtern und Log-in-Daten passieren soll. Die fallen ja beim Aushebeln der Verschlüsselung ebenso an, weil eben jedes mit einem Server ausgetauschte Datenpaket mitgeschnitten werden soll.

Öffnungszeitbeschränkung für die Büchse der Pandora

Während sie sämtliche im Justizministerium geplanten Maßnahmen nach Kräften juristisch untermauert hatten, scheint den von Justizminister Brandstetter berufenen Experten - allesamt Juristen - dennoch geschwant zu haben, dass damit womöglich eine technische Büchse der Pandora geöffnet wird. „Die notwendige Manipulation am Endgerät und die Missbrauchsgefahr macht den Eingriff in internetbasierte Kommunikation in gewisser Weise heikler als herkömmliche Nachrichtenüberwachung“, heißt es in einer der Stellungnahmen. Daher kamen „Verwertungsverbote“ in den Gesetzestext, und der Strafrahmen für Delikte wurde mit fünf Jahren entsprechend hoch angesetzt.

Die Welle der Überwachungshysterie begann mit einer zu Jahresbeginn gestarteten Europol-Kampagne, die **im „Sicherheitspaket“ bereits ihren Niederschlag fand** <http://fm4v3.orf.at/stories/1776635/> .

§ 135a. (1) Überwachung verschlüsselter Nachrichten ist zulässig:

1. *in den Fällen des § 135 Abs. 2 Z 1,*
2. *in den Fällen des § 135 Abs. 2 Z 2, sofern der Inhaber oder Verfügungsberechtigte des Computersystems, in dem ein Programm zur Überwachung verschlüsselter Nachrichten installiert werden soll, der Überwachung zustimmt,*
3. *wenn dies zur Aufklärung einer Straftat, die der Zuständigkeit des Landesgerichts als Schöffen- oder Geschworenengericht (§ 31 Abs. 2 und 3) unterliegt, erforderlich ist oder die Aufklärung oder Verhinderung einer im Rahmen einer kriminellen oder terroristischen Vereinigung oder einer kriminellen Organisation (§§ 278 bis 278b StGB) begangenen oder geplanten Straftat ansonsten wesentlich erschwert wäre und*

Foto/Grafik: gemeinfrei

Die Beschränkung auf Delikte mit mindestens fünf Jahren Strafausmaß ist in der Bedingung versteckt, dass der Fall in die Zuständigkeit eines Schöffen- oder Geschworenengerichts fallen muss

Deutsche „Roadmap“ für Österreich

Die enorme Ausweitung des Einsatzes von polizeilicher Trojaner-Schadsoftware in Deutschland und ihre **Folgewirkung im „Sicherheitspaket“ in Österreich** <http://fm4.orf.at/stories/2846038/> .

Das entspricht der Regelung zum deutschen „Bundestrojaner“, die seit der Einführung dieses „Ermittlungsinstruments“ in Deutschland 2009 bis vor wenigen Wochen galt. Ende Mai wurde der bis dahin auf schwere Verbrechen mit einem Strafmaß von mindestens fünf Jahren beschränkte Einsatz von Trojanern in Deutschland auf insgesamt 38 Delikte bis hin zur Kleinkriminalität ausgedehnt. Statt ausgewählter Dienststellen erhalten nun sämtliche Bundes- wie Landespolizeibehörden und -kriminalämter, Verfassungsschützer und sogar Zollbehörden die Lizenz zum Einsatz von Trojaner-Schadsoftware.

Das zeigt, wohin auch hierzulande die Reise gehen soll. Der laufende Wahlkampf könnte diesen Prozess noch beschleunigen. Noch-Justizminister Brandstetter hatte wiederholt eine Art Überwachungsaufholjagd angekündigt, weil „andere Staaten hier schon viel weiter sind“.

Publiziert am 16.07.2017

- 

19. Juli 2017

Die Sorge um Soundcloud macht User kreativ

- 

19. Juli 2017

mit akzent

Eine Freundin will einen „Kurs für listige Frauen“ machen!

- 

19. Juli 2017

Esther Csapo und Hanna Issa sagen „Hello Damascus!“

- ORF ORF
- Impressum/OffenlegungImpressum
-

Werbung X