Stellungnahme des C3W zum Überwachungspaket 2018/1

> Wir laufen seit Jahren wie Schlafwandler in einen Überwachungsstaat.
> **– Reinhard Kreissl, Kriminalsoziologe**

Österreich hat – selbst innerhalb Europas – eine der am weitesten entwickelten Demokratien. Nach den Gräueln des Faschismus mit Krieg, Massenmord und Überwachung, hat sich Österreich zu einer der fortgeschrittensten Demokratien entwickelt. Die ökonomische Entwicklung, das Nachhinken der Arbeitseinkommen gegenüber Kapital- und Unternehmensgewinnen bewirken eine Teilung, ein Auseinanderbrechen der Gesellschaft. Die Ausweitung dieses Bruchs wird von manchen politischen Parteien und auflagenstarken Massenmedien gefördert. Für uns ist es unumgänglich, diese bedrohlichen Tendenzen in Gesellschaft und Verwaltung aufzuzeigen und zu verhindern.

Die Bundesegierung legt wieder einmal ein Überwachungspaket vor, das massive Eingriffe in die Grundrechte sowie verschärfte Überwachung ermöglichen soll.

Hier zeigt sich besonders deutlich, dass durch ständige Ausweitung der Überwachungsmaßnahmen die Grund- und Freiheitsrechte Stück für Stück beschnitten werden – der demokratische Rechtsstaat wird langsam zum Überwachungs- und Polizeistaat.

Das Überwachungspaket der Bundesregierung umfasst u.a.:

1. Bundestrojaner (staatliche Überwachungssoftware)

SMS überwachen ist heute bereits erlaubt, WhatsApp und andere Messenger aber bislang nicht. Das will die türkis-blaue Regierung mit ihrem Überwachungspaket ändern. Künftig sollen die Internet-Kommunikation via Messenger-Apps (Whatsapp, Skype) durch staatliche Spionagesoftware überwacht werden. Der sogenannte Bundestrojaner soll zur Anwendung kommen. Der Bundestrojaner soll auch “remote” installiert werden können. Damit soll es dem Staat ermöglicht werden, mit Schadsoftware auf „Computersysteme“ und Mobiltelefone von „Verdächtigen“ und „Gefährdern“ einzubrechen.

Zweck sei es, Kommunikationsüberwachung so wie Telefonüberwachung zu ermöglichen. Telefonüberwachung ermöglicht das Mithören und Aufzeichnen von Kommunikation von außerhalb der intimsten Privatsphäre Betroffener.

Die neuen Überwachungsmöglichkeiten erfordern jedoch das Eindringen in die intimsten Bereiche der Privatsphäre; um technisch überhaupt zu funktionieren, muss der Zugriff auf Systemebene erfolgen. Damit ist jede Manipulation am betroffenen Gerät möglich: Zugriff auf alle vorhandenen Funktionen und Datenbestände des Geräts: Lesen, Kopieren, Verändern, Löschen, Hinzufügen und Ausleiten von Daten auf dem Gerät, unbemerkt vom und ungesteuert durch den Benutzer, bzw. Besitzer.

Letztlich wird damit zwangsweise die Beweiskraft von Datenbeständen ausgehebelt, da nach einem solchen Eingriff nie sichergestellt werden kann, welche Daten tatsächlich vom Besitzer des Gerätes stammen und welche ggf hinzugefügt oder verändert wurden. Da ein Zugriff auf Systemebene mittels

Chaos Computer Club Wien (C3W)
buero@c3w.at

schwerwiegender Sicherheitslücken erfolgen muss, kann eine Manipulation von Daten jederzeit nicht nur durch zugreifende Behörden, sondern auch durch Kriminelle stattfinden, die sich ebenfalls durch die Sicherheitslücken zu Geräten Zugriff verschaffen können. Hier werden schwerwiegende Probleme in der Rechtsgültigkeit von Beweismitteln eröffnet.

Schwarzmarkt der Sicherheitslücken

> Um entsprechende Sicherheitslücken zu kennen, muss der Staat sich direkt oder indirekt am Schwarzmarkt für Sicherheitslücken beteiligen und für Steuergelder Sicherheitslücken, sog. Zerodays, einkaufen. Einschlägigen Firmen bieten Sicherheitslücken an, die sie selbst teilweise am Schwarzmarkt einkaufen. So zahlt der US-Amerikanische Anbieter Zerodium bis zu 1,5 Millionen US-Dollar für ein Lücke im iPhone-Betriebssystem iOS.
>
> Für eine Lücke in WhatsApp sind 500.000 US-Dollar drinnen. Deren Geschäftsmodell verbietet es allerdings, betroffene Firmen oder die Öffentlichkeit über Lecks zu informieren. Wird solche Software gekauft, dann konterkariert man staatliche Bemühungen um mehr Cybersicherheit. Ein Bereich, in dem Betriebe und der Staat Millionen Euro investiert werden.[1]

Die genannten Summen gehen natürlich auf das Konto der österreichischen SteuerzahlerInnen. Es kann nicht sein, dass die Regierung die Steuergelder seiner BürgerInnen dafür ausgibt, die Sicherheit für alle Menschen - weit über die eigenen Staatsgrenzen hinaus - unterwandert. Sicherheitslücken gehören den Herstellern gemeldet und gefixt, um die Sicherheit für alle Menschen weltweit zu erhöhen. Die Beteiligung der österreichischen Regierung am Schwarzmarkt für Sicherheitslücken verurteilen wir ausdrücklich.

2. Einschränkung des Briefgeheimnisses

Die vorgeschlagenen Novelle der Strafprozessordnung 1975 zur Beschlagnahme von Briefen, Auskunft über Daten einer Nachrichtenübermittlung, Auskunft über Vorratsdaten sowie Überwachung von Nachrichten sieht folgende Streichung vor: § 135. (1) Beschlagnahme von Briefen ist zulässig, wenn sie zur Aufklärung einer vorsätzlich begangenen Straftat, die mit mehr als einjähriger Freiheitsstrafe bedroht ist, erforderlich ist und sich der Beschuldigte wegen einer solchen Tat in Haft befindet oder seine Vorführung oder Festnahme deswegen angeordnet wurde. Das bedeutet eine massive Beschränkung des Briefgeheimnisses, eines Grundrechtes, das in der Verfassung demokratischer Staaten garantiert ist. Dies gefährdet eine bedeutende Errungenschaft, die nach der Überwindung des metternichschen Überwachungsstaats erkämpft wurde. [2]

3. Lauschangriff im Auto

Im Arbeitsprogramm der Bundesregierung 2017/2018 wurde angekündigt, dass der große Lauschangriff nun schon bei Delikten, die mit einer Freiheitsstrafe von mehr als drei Jahren bedroht sind, zulässig sein soll. Diese höchst eingriffsintensive Maßnahme soll also zukünftig auch bei niederschwelligen Delikten angeordnet werden können. Mit dieser vorgeschlagenen Maßnahme wird die Hürde für den „großen Lauschangriff (§ 136 Abs. 1 Z 3 StPO)“ drastisch reduziert.

[1] https://text.derstandard.at/2000075331814/Bundestrojaner-Der-Staat-muss-wieHacker-oder-Krir
[2] https://epicenter.works/thema/ueberwachungspaket#Briefgeheimnis

4. Grundrechtseingriffe auch bei Bagatelldelikten möglich

Der aktuelle Gesetzesvorschlag sieht eine noch deutlich niedrigere Hürde für den Einsatz dieser Maßnahme vor, nämlich schon bei Straftaten, die mit einer Freiheitsstrafe von mehr als einem Jahr bedroht sind. Das bedeutet, dass bereits bei Straftaten mit einem geringen Strafmaß die Grundrechte der Betroffenen beschnitten werden können.

5. Vorratsdatenspeicherung 2.0

Die Regierung fordert in ihrem Überwachungspaket auch die Wiedereinführung der Vorratsdatenspeicherung. Dieses Gesetz wurde schon mehrfach von Höchstgerichten in ganz Europa aufgehoben. Erst im Dezember 2016 hat der Europäische Gerichtshof entschieden, dass die nationalen Regelungen zur Vorratsdatenspeicherung in Großbritannien und Schweden nicht mit den Grundrechten vereinbar sind. In Österreich wurde diese Art der verdachtsunabhängigen, anlasslosen Massenüberwachung 2014 vom Verfassungsgerichtshof wegen Grundrechtswidrigkeit annulliert. [3]

6. IMSI-Catcher

Auch der Einsatz von IMSI-Catchern für die Überwachung von Mobiltelefonie soll kommen. Diese Geräte verhalten sich gegenüber dem Mobiltelefon wie eine Funkzelle (Basisstation). So ist es möglich, Telefone ohne Mitwirkung des jeweiligen Netzbetreibers zu lokalisieren. Viel wahrscheinlicher ist es jedoch, dass mit diesen Geräten auch Gesprächsinhalte abgehört werden sollen, denn obwohl dies die eigentliche Funktion von IMSI-Catchern ist, fehlt dafür weiterhin die Rechtsgrundlage (*§ 135 Abs 2a StPO-E*). [4]

7. Vernetzung von Videoüberwachung (inkl. Gesichtserkennung!)

Das Innenministerium soll Zugriff auf die Video- und Tonüberwachung aller öffentlichen und privaten Einrichtungen, denen ein öffentlicher Versorgungsauftrag zukommt, bekommen. Damit gibt es eine zentrale, staatliche Kontrolle aller öffentlichen Plätze und des dortigen Lebens. Für den Zugriff auf diese Daten braucht es keinen konkreten Verdacht, ähnlich wie im Polizeilichen Staatsschutzgesetz reicht als Begründung die Vorbeugung von wahrscheinlichen Angriffen (*§ 53 Abs 5 SPG-E*). Die Sicherheitsbehörden können mittels eines einfachen Bescheids eine zweiwöchentliche Vorratsdatenspeicherung der gesamten Videoüberwachung eines Anbieters verlangen (*§ 93a SPG-E*).

In einem nächsten Schritt könnte dieses Bildmaterial ausgewertet werden, um automatisch auffälliges Verhalten zu registrieren und mittels Gesichtserkennung einzelne Personen zu verfolgen. In Österreich gibt es bereits derartige Forschungsprojekte (siehe z.B. iObserve). Dass die Technik dazu nicht fern ist, zeigt sich an jedem Mobiltelefon, das bereits eine Gesichtserkennung in der Kamerasoftware integriert hat. Auch beim Hochladen von Fotos auf Social Media werden Gesichter automatisch erkannt und Personen automatisch getaggt. Die Verwendung dieser Technologie durch Behörden wäre ein konsequenter nächster Schritt, der die Möglichkeiten der ÖsterreicherInnen, sich frei und unüberwacht im eigenen Land zu bewegen, zerstört.

Ob Videoüberwachung überhaupt ein geeignetes Mittel ist, um Terroranschläge zu verhindern, muss

[3] VfGH: Gesetze zur Vorratsdatenspeicherung in Österreich verfassungswidrig `https://www.vfgh.gv.at/downloads/presseinformation_verkuendung_vorratsdaten.pdf`
[4] `https://epicenter.works/thema/ueberwachungspaket#VDS`

Chaos Computer Club Wien (C3W)
buero@c3w.at

bezweifelt werden. Schließlich wurde auch die gesamte Uferpromenade von Nizza mit Videokameras überwacht und der Anschlag dort konnte damit dennoch nicht verhindert werden. Im Gegenteil: Videokameras können Terroristen sogar als Ansporn und zur Auskundschaftung dienen. Schließlich zielen sie mit ihren Gräueltaten auf die größtmögliche Verstörung der Bevölkerung, um Angst zu verbreiten.

Im Jänner wurde bekannt, dass die LPD Wien 15 von 17 Überwachungskameras abbauen ließ, weil die Kosten zu hoch waren und der Nutzen für die Verbrechensbekämpfung nicht erkennbar war. Diesem Trend sollte weiter nachgegangen werden.

8. Lückenlose Überwachung des Autoverkehrs (Kennzeichenerfassung)

Künftig soll auch auf allen österreichischen Straßen von jedem Auto der Lenker des Fahrzeugs, das Kennzeichen, Marke, Typ und Farbe erfasst werden. Die von den Sicherheitsbehörden selbst ermittelten oder auf deren Ersuchen von der ASFINAG übermittelten Daten, können in Verdachtsfällen bis zu fünf Jahre gespeichert werden (§ 53a Abs 6 SPG-E). Sind die Daten allerdings nicht zur weiteren Verfolgung gerichtlich strafbarer Handlungen erforderlich, sind sie nach längstens 48 Stunden zu löschen. Dennoch ist auch hier anzumerken, dass die Kameras auch in der Lage sind, neben den Kennzeichen und Fahrzeugen auch die Gesichter der Personen darin zu erfassen und konkreten Personen zuzuordnen.

Damit entsteht eine neue Form der anlasslosen Massenüberwachung und jeder Autofahrer wird unter Generalverdacht gestellt.

Aus grundrechtlicher Perspektive ist dieser Schritt in Richtung einer kompletten Überwachung aller Kennzeichen sehr problematisch. Der VfGH hat 2007 in seiner Entscheidung zur Section Control festgestellt, dass eine Überwachung von AutofahrerInnen nur auf bestimmten, besonders gefährlichen und per Verordnung festgelegten Strecken zulässig ist. Zudem dürfen laut VfGH nur Kennzeichendaten gespeichert und an die Behörden übermittelt werden, wenn die erfassten Fahrzeuge zu schnell unterwegs oder bereits zur Fahndung ausgeschrieben sind.

Diese Form der Vorratsdatenspeicherung nicht mit diesem Erkenntnis vereinbar und steht auch im Widerspruch zur Rechtsprechung des EuGH im Fall Watson/Tele 2 Sverige, nach der eine Vorratsdatenspeicherung unter anderem nur zur Bekämpfung schwerer Kriminalität zulässig sein kann.

9. Registrierungspflicht für Wertkarten

Jeder Kauf einer SIM-Karte müsste mit der Registrierung der Identität einhergehen. Damit wird eine weitere Möglichkeit abgeschafft, unbeobachtet zu kommunizieren. Kriminelle können diese Maßnahme leicht mit ausländischen SIM-Karten oder gratis verfügbaren, anonymen Messaging-Diensten umgehen. Für die Mehrzahl der NutzerInnen in Österreich fällt jedoch eine weitere Möglichkeit weg, anonym zu kommunizieren. Damit werden 4,5 Millionen NutzerInnen unter Generalverdacht gestellt. Der äußerst zweifelhafte Nutzen für die Bekämpfung von Kriminalität, steht einem Eingriff in das Recht aller ÖsterreicherInnen, frei und unbeobachtet zu kommunizieren gegenüber. Diese Maßnahme ist daher nicht verhältnismäßig.

Mexiko hat das Verbot anonymer SIM-Karten wieder abgeschafft, da die Verbrechensrate sogar stieg und es nur zu einem Schwarzmarkt für SIM-Karten führte. Tschechien, Neuseeland, Kanada, Rumäni-

en, Großbritannien und die EU-Kommission haben die Maßnahme analysiert und sich aufgrund der fehlenden Belege dagegen entschieden.[5]

Zusammenfassend ist festzuhalten:

1. Die Sicherheit der IT-Infrastruktur in Österreich wird wissentlich und schwer gefährdet. Dies geht durch das Wesen des Internets als globales Medium weit über die Landesgrenzen hinaus und betrifft alle Menschen, die sich an der IT Infrastruktur weltwelt beteiligen. Diese wissentliche Gefährdung ist unverantwortlich und daher zu verurteilen.
2. Eine Überwachungsgesamtrechnung wurde nicht durchgeführt.
3. Eine Wirkungsfolgenabschätzung bzgl. Auswirkungen auf Grundrechte und Gesellschaft fehlt im Begutachtungsentwurf.
4. Durch die Anlassdatenspeicherung soll eine Vorratsdatenspeicherung durch die Hintertür eingeführt werden.
5. Die Schwellen für viele Grundrechtseingriffe werden sukzessive herabgesetzt.
6. Insgesamt sollen eine Fülle an (weiteren) Bestimmungen mit polizeistaatlichen Tendenzen Einzug in den österreichischen Rechtsbestand halten. Es ergibt sich zunehmend das Bild, dass Österreich in einen Polizei- und Überwachungsstaat umgebaut wird.
7. Es entstehen enorme finanzielle Kosten für eingriffsintensive Maßnahmen, die die Sicherheit erwiesenermaßen für alle vermindern.
8. Der Rechtsschutz ist in vielen Punkten der Entwürfe nicht ausreichend gewährleistet.
9. Es wird Raum für zusätzliche Kriminalität geschaffen und die Internetkriminalität durch aktive Beteiligung mit Steuergeldern befeuert.

[5] GSMA The Mandatory Registration of Prepaid SIM Card Users - A White Paper https://www.gsma.com/publicpolicy/wp-content/uploads/2016/09/GSMA2013_WhitePaper_MandatoryRegistrationofPrepaidSIM-Users.pdf

Chaos Computer Club Wien (C3W)
buero@c3w.at

Fazit

Wir lehnen das Überwachungspaket als deutlich überschießenden Eingriff in Grundrechte zur Gänze ab und fordern stattdessen:

Sicherheit und Grundrechtsschutz für Alle

- Überprüfung und Evaluierung bestehender Überwachungsgesetze hinsichtlich ihrer Grundrechtskonformität und Wirksamkeit vor Erlassung neuer Überwachungsmaßnahmen
- Schutz der BürgerInnen vor Bedrohung und Übergriffen insbesondere im Bereich technischer Infrastruktur und digitaler Privatsphäre; dazu gehört auch – nach Information der Hersteller – Veröffentlichung aller bekannten Sicherheitslücken
- Rigorose Umsetzung der Datenschutzgrundverordnung (DSGVO) sowie ausreichende materielle und qualifizierte personelle Dotierung der Datenschutzbehörde (Besetzung mit Juristen und Technikern)
- Sicherstellung, dass Amtsträger und Behördenvertreter auch persönlich für Grundrechtserstöße und Datenschutzvergehen haften
- zwingendes Ablaufdatum (“Sunset Clauses” mit wissenschaftlicher Überprüfung der Wirksamkeit/Evaluierung und Rücknahme wirkungsloser Maßnahmen) bei allen Überwachungsgesetzen
- mehr spezifisch ausgebildete Polizeikräfte statt mehr Überwachung
- verbesserte Analysekapazitäten für Sicherheitsbehörden: Mehr speziell ausgebildete Datenanalysten statt mehr Daten
- mehrsprachige Polizeikräfte bzw. mehr und qualifizierte Dolmetscherkapazitäten
- mehr Präventionsarbeit gegen Radikalisierungstendenzen
- breite öffentliche Diskussion und Berücksichtigung der Stellungnahmen von Experten und Zivilgesellschaft
- bessere Vernetzung mit Communities und Zivilgesellschaft als vertrauensbildende Maßnahmen und zur frühzeitigen Erkennung radikaler Tendenzen
- Verankerung der Integrität informationstechnischer Systeme und Schutz der digitalen Privatsphäre in der Verfassung

Für Rückfragen stehen wir gerne zur Verfügung.

Mit freundlichen Grüßen,

Chaos Computer Club Wien (C3W), ZVR 656204875

Auszüge aus der öffentlichen, zivilgesellschaftlichen Diskussion zum Thema und Stellungnahmen von anerkannten Fachleuten sowie qualifizierten Institutionen

Abschließend möchten wir beispielhaft einige der der zahllosen kritischen Stellungnahmen der letzten Jahre von anerkannten Fachleuten sowie wichtigen qualifizierten Institutionen zitieren.

Christof Tschohl, Jurist, Techniker und Obmann von epicenter.works:

> „Kein belegter Nutzen, gewaltige KollateralschädenWir brauchen eine Sicherheitspolitik, die tatsächlich geeignet ist, den Problemen unserer Zeit zu begegnen. Die Politik übt sich in gefährlichem Aktionismus, der keine Lösungen bringt. Im Gegenteil: Hier werden elementare Grundrechte ausgehöhlt und im Falle des Bundestrojaners und der damit verbundenen Nutzung und Finanzierung von Sicherheitslücken sogar die gesamte kritische Infrastruktur des Landes gefährdet"[6]

Reinhard Kreissl, Kriminalsoziologe:

> „Der Sinn dieses Überwachungspakets ist eher symbolischer Natur", sagt der renommierte Kriminalsoziologe Reinhard Kreissl zur „Krone": „Man dramatisiert die Situation und schiebt dann spektakulär ein Gesetzespaket hinterher, um die vermeintliche Bedrohung zu bekämpfen. Die Frage, was die Sicherheit Österreichs gefährdet, wird dabei nur schlampig beantwortet." Mit Argumenten wie „Migranten", „Extremisten" und „Cybercrime". Bundestrojaner oder das „Quick Freeze" sind laut Kreissl für die Polizeiarbeit von marginaler Bedeutung.[7]

Die Österreichischen Rechtsanwälte (Österreichischer Rechtsanwaltskammertag, ÖRAK) :

> "Neben der Tatsache, dass dieser Gesetzesentwurf völlig unverhältnismäßig in die Grundrechte eingreift, stellt sich auch die Frage, wer die in die Grundrechte eingreifenden Organwalter wie überwacht."[8]

Stellungnahme des Obersten Gerichtshofs:

> „Ein solches staatlich veranlasstes Einschleusen von im genannten Sinn gezielt wirkender Schadsoftware (nämlich „durch Installation eines Programms in einem Computersystem … ohne Kenntnis dessen Inhabers oder sonstiger Verfügungsberechtigter", wie es im vorgeschlagenen § 134 Z 3a StPO heißt, in der öffentlichen Diskussion gelegentlich mit dem Schlagwort „Bundestrojaner" verknüpft), ist, wie bspw die ausführliche Stellungnahme des Instituts für Angewandte Informationsverarbeitung und Kommunikationstechnologie der TU Graz (7818/SN-325/ME XXV. GP) veranschaulicht, zum einen de facto kaum machbar und zum anderen mit gravierenden negativen Begleiterscheinungen verbunden."[9]

[6] https://epicenter.works/thema/ueberwachungspaket#VDS
[7] http://www.krone.at/1670622
[8] https://www.parlament.gv.at/PAKT/VHG/XXVI/SN/SN_00008/index.shtml
[9] 1 Präs. 1619-2514/17t, https://parlament.gv.at/PAKT/VHG/XXV/SNME/SNME_29473/imfname_666692.pdf