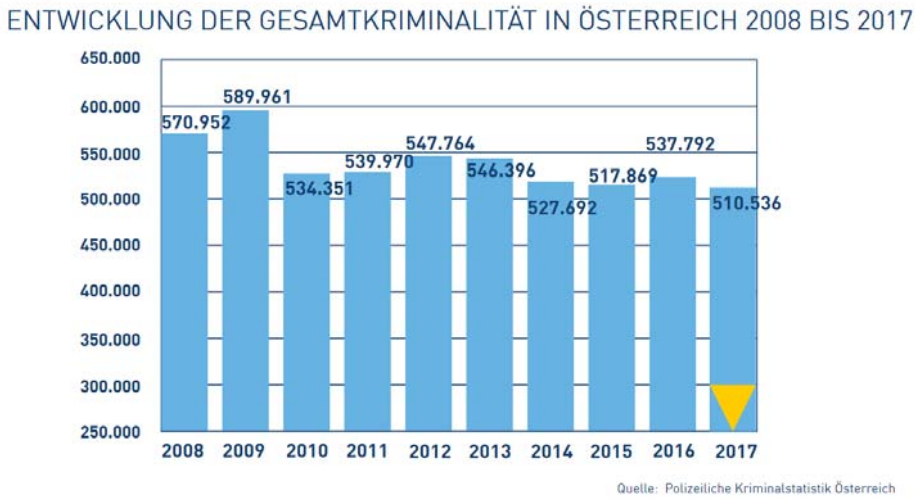
Überwachungspaket

Roland Giersig



Die Bundesregierung hat die bereits von der ÖVP/SPÖ Koalition diskutierten Maßnahmen, die als Sicherheitspaket tituliert wurden, im Ministerrat beschlossen. Das Gesetzespaket soll nun ohne weitere Begutachtung durch den Nationalrat beschlossen werden. Mit beinhaltet in diesem Paket sind teilweise schwerwiegende Maßnahmen, die schwere Eingriffe in die Freiheitsrechte erfordern. Die Kritik an diesen Maßnahmen ist nicht nur seitens der Digital Society groß.

Braucht es die Maßnahmen?

Die Regierung argumentiert, dass diese Maßnahmen aufgrund des subjektiven Sicherheitsgefühls der Bürger erforderlich sind. Die Bürger fühlen sich also unsicher. Zurecht? Hier ein kurzer Blick in die Kriminalstatistik des Innenministeriums:

Im letzten Jahr (2017) wurden also die wenigsten Anzeigen der letzten 10 Jahre verzeichnet. Gleichzeitig ist auch die Aufklärungsquote von 38,1% in 2008 auf 50,1% in 2017 gestiegen.

Es werden also von weniger angezeigten Verbrechen mehr aufgeklärt. Gleichzeitig fühlt sich aber die Bevölkerung unsicher, und gleichzeitig fordern unsere Politiker drastische Überwachungsmaßnahmen, um die Kriminalität eindämmen zu können. Irgendetwas scheint hier fundamental falsch zu laufen.

Das Überwachungspaket der Bundesregierung sieht folgende Maßnahmen vor, zu denen wir wie folgt Stellung nehmen:

Bundestrojaner

Worum geht es eigentlich bei der Online Durchsuchung (in den Medien "Bundestrojaner“ genannt)? Strafverfolgungsbehörden durften seit jeher Kommunikation Verdächtiger abhören. Da dies ein starker Eingriff in die Grundrechte ist und war, war dafür eine richterliche Anordnung erforderlich. Also, um Telefongespräche abhören zu dürfen, musste ein Verdachtsmoment vorliegen, und ein Richter hat dieses geprüft. Erst danach durfte die Polizei eine Telefonleitung anzapfen und diese abhören.

Man möchte meinen, die Enthüllungen rund um Edward Snowden hätten wenig Effekt gehabt. Eines hat sich jedoch verändert. Verschiedenste Hersteller von Internet Kommunikationssystemen haben ihre Kommunikation umgestellt. So haben beispielsweise Anbieter von gängigen Instant -Messaging Apps in eine sogenannte End to End Encryption umgestellt. Das heißt, die Kommunikation zwischen Absender und Empfänger über die Leitung erfolgt nur noch verschlüsselt. Früher konnte entweder auf der Leitung die Kommunikation mitgehört werden, oder die Nachrichten wurden am Server entschlüsselt und wieder neu verschlüsselt zum Empfänger weitergeleitet.

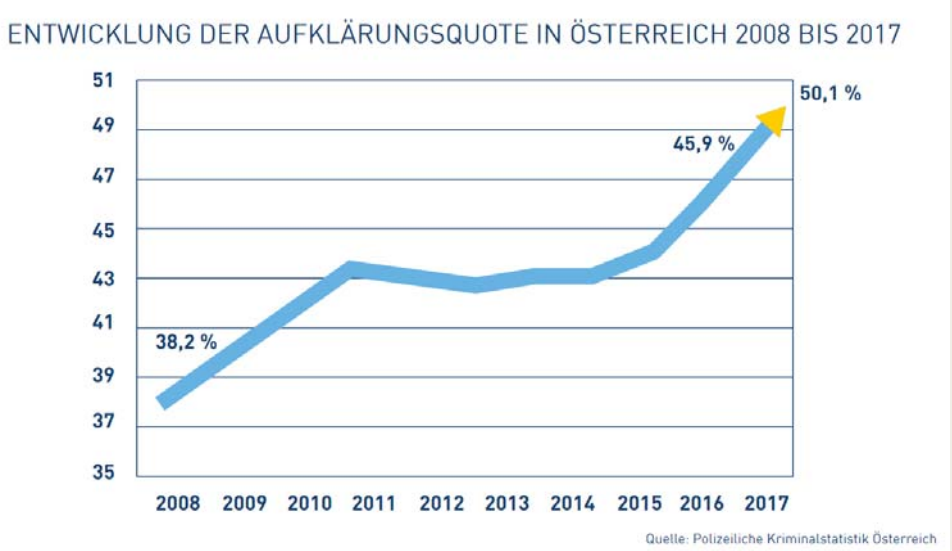
Da die Nachrichten nun vom Absender verschlüsselt werden – und nur vom Empfänger (ohne erheblichen Aufwand) entschlüsselt werden können, kann weder der Anbieter des Nachrichtendienstes (z.B. WhatsApp) noch der Netzwerkbetreiber mehr Nachrichten bei der Übertragung lesen. Es ist daher auch für Strafverfolgungsbehörden technisch so gut wie unmöglich, auf diese Kommunikation zuzugreifen. Auch ein richterlicher Befehl hilft hier wenig, denn wenn Daten nicht vorliegen, kann man sie auch nicht herausgeben.

Lösungsweg Online Durchsuchung

Diese Situation ist für die Polizei nun unbefriedigend. Früher konnte man Kommunikation abhören. Normale Handykommunikation ist sogar so unsicher, dass sie im Grunde von jedem ohne großen Aufwand und Kosten abgehört werden kann (auch wenn das illegal ist). Bei der elektronischen Kommunikation über Nachrichtenapps, die End-To-End-Verschlüsselung anbieten, ist das aber nun im Grunde unmöglich geworden. Die Behörden befürchten, dass sie dadurch gegenüber den Verbrechern ins Hintertreffen geraten – und suchen dafür eine Lösung.

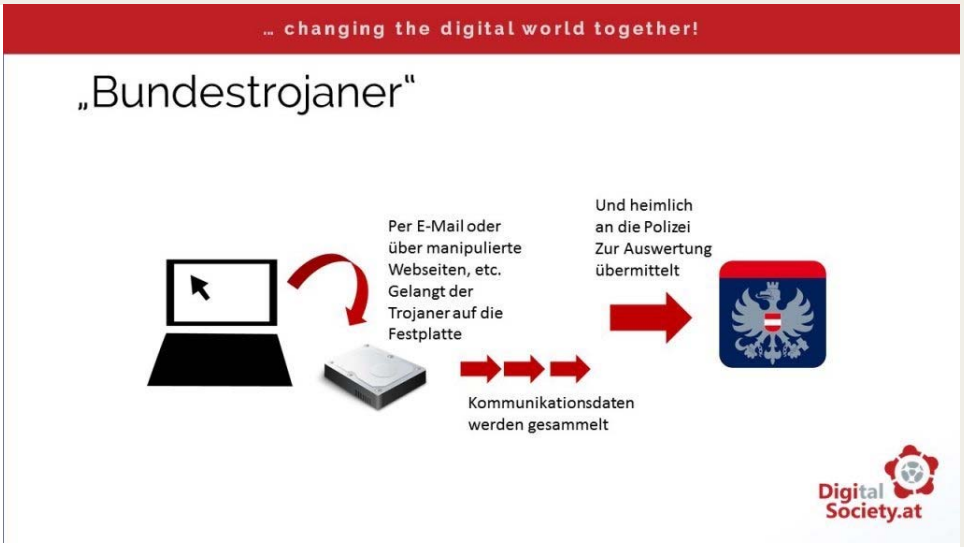
Da es technisch beinahe unmöglich ist, verschlüsselte Kommunikation bei der Übertragung abzuhören, versucht man den Weg zu gehen, die Übertragung auf dem Gerät des Senders oder Empfängers abzufangen bevor die Kommunikation verschlüsselt wird. Dazu ist ein Eindringen auf das entsprechende Gerät notwendig (Smartphone, PC oder Spielekonsole). Eine Software muss ohne das Wissen des Betroffenen installiert werden. Diese Software muss die Kommunikation (Text oder Sprache) abfangen, bevor sie verschlüsselt wird – und heimlich an die Polizei senden.

Dieses Unterfangen ist nicht ganz einfach, denn wie schafft man es, eine App auf das Gerät eines potentiellen Verbrechers zu installieren, ohne dass der das bemerkt und Verdacht schöpft. Freiwillig wird es vermutlich nicht machen. Ein gangbarer



Weg ist also, in das Gerät des Betroffenen einzubrechen. Aber auch das ist im Normalfall nicht simpel. Geräte sind im Normalfall ja mit technischen Maßnahmen gegen solche Einbrüche geschützt (sonst würde es ja ständig passieren).

Daher müssen die Behörden in diesem Fall ähnlich vorgehen wie es Hacker machen. Sie nutzen Schwachstellen der Software – in den meisten Fällen des Betriebssystems (vor allem Windows Android oder iOS) aus und dringen über diese Fehler im Betriebssystem in das Gerät ein. So eingedrungen, installieren sie eine Schadsoftware auf dem Gerät. Diese führt dann die Online Durchsuchung durch. Solche Schwachstellen nennt man im Fachjargon *„Zero Day Exploits“* – und Betriebssystemhersteller unternehmen alles Erdenkliche, um solche Lücken möglichst bald zu patchen. Sobald aber eine Lücke geschlossen wird, ist sie natürlich nicht mehr nutzbar.



Resultierende Probleme

Es wird daher in Zukunft verstärkt so sein, dass diese Lücken nicht an Betriebssystemhersteller gemeldet werden. Es gibt schon einen – und wird in Zukunft noch häufiger – Handel mit derartigen Lücken geben. Denn jetzt kaufen schon Verbrecher solche Lücken, um sie für ihre Zwecke auszunutzen. In Zukunft ist wohl zu befürchten, dass auch Behörden solche Lücken kaufen, beziehungsweise, wenn ihnen solche gemeldet werden, diese nicht an die Betriebssystemhersteller weitergegeben werden.

Es ist daher zu befürchten, dass es in Zukunft viel mehr solche nicht geschlossenen Sicherheitslücken gibt, und es einen schwunghaften Handel mit derartigen Lücken geben wird. Auch kann man nicht ausschließen, dass derartige Lücken den Behörden abhandenkommen. Die Basis für den Ausbruch der WannaCry Ransomware, der unter anderem in UK das Gesundheitssystem beinahe lahm gelegt hat, waren Betriebssystemlöcher, die der Behörde abhandengekommen waren.

Es ist also klar, dass die Behörden auf der einen Seite gerne Zugriff auf die Kommunikationskanäle von Verbrechern hätten. Auf der anderen Seite macht man die Büchse der Pandora auf und macht all unsere Computersysteme dramatisch unsicherer. Das kann im schlimmsten Fall zu einem gesamten Zusammenbruch eines Großteils der IT-Systeme führen. Zum anderen können solche Betriebssystemlöcher natürlich auch für andere Zwecke von Verbrechern genutzt werden. Wenn man die Schlösser an einer Wohnung abmontiert, dann kann nicht nur die Polizei in die Wohnung, sondern sie wird voraussichtlich eher von Verbrechern leergeräumt werden.

Mobilfunküberwachung durch "IMSI-Catcher"

IMSI-Catcher simulieren eine Funkzelle eines beliebigen Netzbetreibers und bringen dadurch alle umliegenden Handys dazu, sich in diese private Funkzelle (die in diesem Fall von der Polizei betrieben wird) einzuwählen.

Es werden daher neben der Lokalisierung des Verdächtigen auch Standortdaten von Unbeteiligten erhoben und gespeichert. Im vorliegenden Gesetzesvorschlag fehlt aber eine explizite Einschränkung für die Speicherung der Standortdaten Unbeteiligter. Weiters ist es mit den IMSI-Catchern auch möglich, Verbindungsdaten sowie den Inhalt von Gesprächen und Datenübertragungen mitzuschneiden, ebenfalls von Unbeteiligten. Es kann also jedes beliebige mobile Telefongespräch abgehört und mitgeschnitten werden.

Das Gesetz sieht derzeit keine Regelung vor, wie mit Verbindungsdaten, Gesprächen und Datenübertragungen Unbeteiligter umgegangen wird.

Quick Freeze

Quick Freeze ist der Versuch die vom Verfassungsgerichtshof gekippte Vorratsdatenspeicherung grundrechtskonform wieder einzuführen. *Quick Freeze* sieht dabei vor, dass anlassbezogen die Speicherung von Daten durch die Telekommunikationsanbieter bis zu 12 Monte lang angeordnet werden können. In dieser Zeit muss dann der Verdacht gegen einen Verdächtigen erhärtet werden und zu einer Anklage führen.

Der Gesetzesentwurf weist aber aus unserer Sicht schwerwiegende Mängel auf. Es ist nicht klar definiert, welche Daten in welchem Umfang einem *Quick Freeze* unterworfen werden können sollen. Dem Wortlaut nach kann die Staatsanwaltschaft im Rahmen eines einzelnen Strafverfahrens auch anordnen, alle Daten aller (!) Kunden des Betreibers für 12 Monate aufzuzeichnen, was einer unzulässigen Vorratsdatenspeicherung gleichkäme.

Sollten im Rahmen eines Quick-Freeze auch Daten von nicht direkt Verdächtigen gespeichert und ausgewertet werden, so ist es notwendig, dass diese Betroffenen analog zu einer Überwachung durch Abhören von diesem Grundrechtseingriff informiert werden. Im Gesetzestext fehlt diesbezüglich eine entsprechende Regelung.

Allgemeine Videoüberwachung

Der hier vorgesehene Zugriff auf private Videoüberwachungsdaten des öffentlichen Raums ist aus grundrechtlicher Sicht höchst problematisch. Die Formulierung *„für die Zwecke der Vorbeugung wahrscheinlicher ... Angriffe“* ist zu unbestimmt und quasi ein Freibrief für einen beliebigen Zugriff auf diese Daten, dies im Besonderen, da der Zugriff keiner richterlichen Kontrolle unterliegt. Auch ist keine vorherige Zustimmung des Rechtschutzbeauftragten notwendig, sondern das Gesetz sieht einen Freibrief für drei Tage vor. Zudem würde ein solchermaßen extrem erleichterter Zugang zu Videodaten die Kontrollkapazitäten des Rechtsschutzbeauftragten unabhängig von der Drei-Tages-Frist wohl schnell überfordern und damit den eigentlich damit vorgesehenen Rechtsschutz untergraben.

Die private Videoüberwachung des öffentlichen Raumes ist durch Datenschutzvorgaben streng reglementiert und eingeschränkt. So sind Aufzeichnungen von Personen nur zulässig, wenn entsprechende Einwilligungen der Betroffenen vorliegen. Es erscheint sehr zweifelhaft, dass hier überhaupt Videoaufzeichnungen von privater Hand rechtmäßig weitergegeben werden können.

Grundsätzlich erscheint es fraglich, ob durch diesen erleichterten Zugriff wesentliche Präventions- oder Fahndungserfolge erreicht werden können. Das Beispiel Großbritannien zeigt, dass auch eine flächendeckende Videoüberwachung zu keinen nennenswerten Erfolgen führt. Keiner der Terroranschläge konnte durch die Videoüberwachung verhindert werden. Auch erscheint das Begehren nach mehr Videoüberwachungsdaten seltsam, wenn an 15 von 17 Standorten in Österreich im Laufe der letzten Jahre polizeiliche Videoüberwachungs-kameras demontiert wurden, da kein Nutzen für die Verbrechensbekämpfung erkennbar war.

Aus technischer Sicht ist die mögliche Echtzeitüberwachung zu kritisieren. Be-

treiber wie ÖBB und Wiener Linien betreiben ihre Videoüberwachungsanlagen teilweise offline und damit datenschutzfreundlich. Eine durch die Unbestimmtheit des Gesetzes mögliche Verpflichtung zur Umrüstung auf Echtzeitzugriff wäre mit enormen Mehrkosten verbunden oder technisch gar nicht möglich.

Videoüberwachung des Straßenverkehrs

Die Zusammenführung von Überwachungsdaten aus Section Control, Videomaut und Radargeräten erlaubt eine weitreichende Überwachung des Straßenverkehrs sowie auf Grund der langen Speicherfrist von zwei Wochen die Erstellung von Bewegungs- und Verhaltensprofilen. Dies ist grundrechtlich höchst problematisch, da hierdurch alle Autofahrerinnen und Autofahrer unter Generalverdacht gestellt werden. Im Besonderen ist problematisch, dass die im Gesetzesvorschlag vorgesehene Einschränkung auf *„Abwehr und Aufklärung gefährlicher Angriffe“* kaum eine Einschränkung darstellt. Auch gibt es keine Vorkehrungen, den Kreis der betroffenen Personen einzuschränken und die Weitergabe der Information an EKIS ist nicht geregelt. Daher stellen diese Maßnahmen einen Grundrechts-eingriff der höchsten Intensitätsstufe dar, dem kein klar erkennbarer Nutzen in der Sicherheit gegenüber steht.

Auch hier ist auf die fehlende grundrechtliche Bewertung und Argumentation in den Erläuterungen hinzuweisen. Es gibt sowohl seitens VfGH wie EuGH Rechtsprechung, die einen solchen grundrechtlichen Eingriff als nicht angemessen einstuft. Ohne entsprechende Argumentation hinsichtlich der grundrechtlichen Angemessenheit, die auf die bestehenden Erkenntnisse eingeht, ist diese Gesetzesänderung abzulehnen.

SIM-Karten-Registrierung

In Zukunft soll es keine anonymen Telefonwertkarten mehr geben. Die Identitätsfeststellung und Registrierung von Prepaid -SIM-Karten ist für die Netzbetreiber kostenintensiv, eine Abgeltung der Kosten ist nicht vorgesehen. Aus den Stellungnahmen der Mobilfunkanbieter ist daher davon auszugehen, dass die Kosten für diese Prepaid-SIM-Karten, die vor allem von Menschen mit geringem Einkommen derzeit genutzt werden steigen werden.

Es darf auf Grund von internationalen Beispielen bezweifelt werden, dass diese Registrierung auch einen brauchbaren Nutzen zur Strafverfolgung und -Prävention bietet. Mehrere europäische Länder haben eine geplante Einführung der Registrierpflicht wieder ausgesetzt. Mexiko hat die bereits eingeführte Registrierpflicht nach drei Jahren wieder aufgehoben, da sie zu keinem konkreten Nutzen bei der Strafverfolgung geführt hat. Im Gegenteil wurden teilweise Ermittlungen behindert und verzögert, da durch den Schwarzmarkt für registrierte SIM-Karten die Ermittler auf falsche Fährten gelockt wurden.

Die Einführung einer Registrierungspflicht für SIM-Karten ist daher abzulehnen.

Fazit

Die technischen und auch grundrechtlichen Probleme rund um den Bundestrojaner zeigen, dass es in Zukunft sehr wichtig sein wird, neben der finanziellen Wirkungsfolgenabschätzung eine solche auch hinsichtlich der grundrechtlichen und der technischen Auswirkungen von Gesetzesvorhaben durchzuführen.

Weiters ist es empfehlenswert, bei solch techniklastigen Themen nicht nur juristische, sondern auch technische Experten in Expertengruppen einzuladen. Nur so kann sichergestellt werden dass Gesetzesvorschläge sich nicht später als technisch nicht umsetzbar erweisen.

Bei Betrachtung der technischen Sicherheitsrisiken für die Allgemeinheit und des fraghaften Nutzens erscheint es wie Hohn, wenn diese Gesetzesänderung als „Sicherheitspaket“ bezeichnet wird. Ohne eine detaillierte Analyse der technischen Umsetzbarkeit kann nur mit aller Schärfe gefordert werden, von der legistischen Umsetzung zum jetzigen Zeitpunkt Abstand zu nehmen.

Auch die anderen Punkte des „Sicherheitspakets“ sind höchst problematisch und stellen schwerwiegende Eingriffe dar, zeigen sie doch klare Tendenzen, Österreich in einen Polizei- und Überwachungsstaat umzuwandeln, ohne erkennbare Vorteile, dafür aber mit finanziellen Mehrbelastungen für die Bevölkerung.

Weiterführende Links

Ausschussbegutachtung: Strafprozessrechtsänderungsgesetz 2018 (53/SN)
https://www.parlament.gv.at/PAKT/VHG/XXVI/SN/SN_00053/index.shtml#tab-Uebersicht

Ausschussbegutachtung: Sicherheitspolizeigesetz, Straßenverkehrsordnung 1960 und Telekommunikationsgesetz 2003 (52/SN)
https://www.parlament.gv.at/PAKT/VHG/XXVI/SN/SN_00052/index.shtml

Digital Society

Die Digital Society ist ein gemeinnütziger Verein, der 2015 gegründet wurde, und sich für die positive Nutzung der Digitalisierung unserer Gesellschaft einsetzt. Unsere Vision ist eine freie digitale Welt von der alle Mitglieder unserer Gesellschaft profitieren.

Die Digital Society setzt sich für die Rechte der Bürger und eine positive Nutzung digitaler Technologien ein und gibt daher regelmäßig Stellungnahmen zu Gesetzesänderungen ab und steht mit ihrer Expertise für Diskussionen zur Verfügung. Wir wollen die digitale Transformation nutzen, um unser gesellschaftliches System zu unserem Nutzen zu verändern, frei nach unserem Motto *„...changing the digital world together!“*. Wir können das nicht alleine schaffen und benötigen dazu Deine Unterstützung. Du kannst uns durch Mitarbeit, durch eine Spende aber auch durch eine Mitgliedschaft unterstützen. Nähere Informationen dazu findest Du unter
https://DigiSociety.at

Überwachung