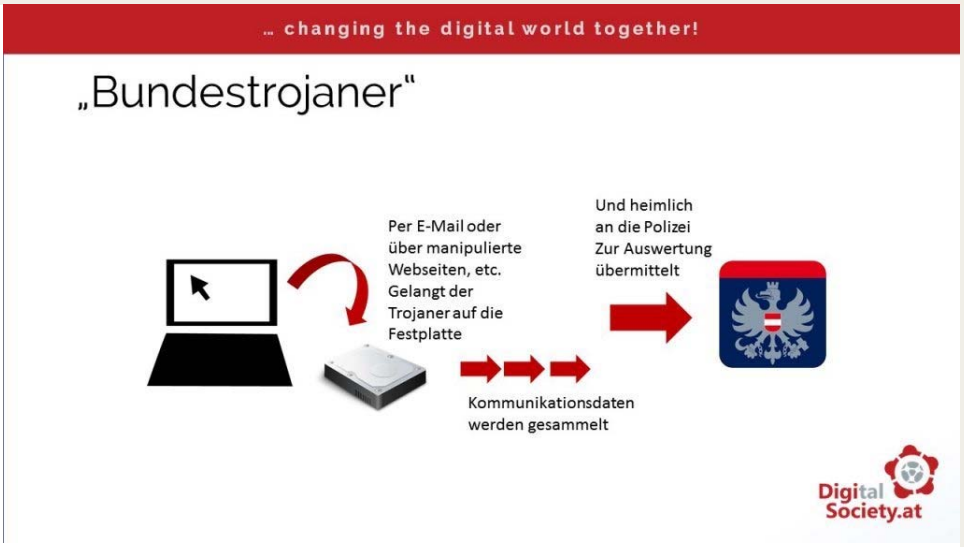
Weg ist also, in das Gerät des Betroffenen einzubrechen. Aber auch das ist im Normalfall nicht simpel. Geräte sind im Normalfall ja mit technischen Maßnahmen gegen solche Einbrüche geschützt (sonst würde es ja ständig passieren).

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-