Thesen Kontra

Key Escrow

Ein Key Escrow Verfahren bedingt eine zentrale Stelle, welche die jeweiligen Schlüssel sammelt. Durch diese zentrale Stelle gehen mehrere Gefahren aus. Zum einen ist eine solche Stelle ein sehr attraktives Ziel von Kriminellen. Ein Einbruch in eine solche Stelle kann für verschiedene weitere kriminelle Tätigkeiten weiterverwendet werden wie z.B. Wirtschaftsspionage oder verschiedene Arten von Betrug. Ein anderes Gefahrenpotential geht von den Angestellten dieser Stelle aus oder sogar von Staat direkt. Es ist ein Trugschluss zu glauben, dass die Daten korrekt behandelt werden und nicht an Unbefugte gelangen.

Vorratsdatenspeicherung

Ein häufiges Argument der Befürworter einer Vorratsdatenspeicherung ist, dass ja nur unter gewissen Umständen der Zugriff auf solche Daten erlaubt sei. Ein richterlicher Beschluss oder öhnliches ist immer nötig um solche Daten in einem Verfahren verwenden zu dürfen.

Das mag zwar alles stimmen. Das Problem ist aber, wenn die Daten einmal gespeichert sind, hat der Bürger keine Kontrolle mehr darüber. Was hindert ein Staat daran, die Gesetze anzupssen, so dass diese plötzlich länger gespeichert werden oder auch bei leichtem Verdacht bereits verwendet werden dürfen? Die Daten sind ja schon da ...

Sicherheit der Daten

Eine Überwachung wie wir sie heute kennen generiert eine grosse Menge an Daten. Damit diese verwendet werden können, müssen diese gespeichert werden. Dies führt jedoch zu einigen Problem.

Die gespeicherten Daten sind nicht nur für den Staat interessant. Diese können auch für kriminelle Zwecke verwendet werden. Und da die Daten nun an einem zentralen Ort gespeichert werden, macht diesen zu einem lukrativen Ziel. Somit stellt sich die Frage, können die gespeicherten Daten überhaupt genug sicher abgelegt werden?

Es zeigt sich immer wieder, dass selbst grosse Unternehmen Ziel von Angriffen werden. Es gibt erschreckende Beispiele:

- RSA Security, ein Hersteller von Sicherheitssoftware
- Lockeed Martin, ein Rüstungsunternehmen und Lieferant der amerikanischen Armee
- Mitsubishi Heavy Industries, ebenfalls ein Rüstungsunternehmen und Lieferant der amerikanischen Armee

Die Dunkelziffer wird sehr gross sein. Aber nur schon die bekannt gewordenen Fälle sind Grund zur Beunruhigung. Das zeigt doch, wie proffessionell Kriminelle heutzutage vorgehen.

Es ist durchaus auch vorstellbar, dass solche Angriffe nicht nur krimineller Energie entstammen, sondern auch durch verfeindete Staaten durchgeführt werden. Cyber-War wird wohl eine immer grössere Bedeutung haben.

Es stellt sich also die Frage, wer alles auf diese Daten Zugriff hat! Ein ungutes Gefühl ...

Videoüberwachung

Die Videoüberwachung mag ein veritables Mittel gegen die Verbrechensbekämpfung sein. Jedoch wirkt die Abschreckung nur in überwachten Gebieten. Das heisst, die Kriminalität verlagert sich in andere Gebiete und kann dort dafür umso brutaler werden. Diesem Umstand könnte man nur mit einer totalen Überwachung entgegenwirken, was jedoch tunlichst zu vermeiden ist!

Ein weiterer wichtiger Punkt der in Betracht gezogen werden muss: Die Freiheit des Individuums wird eingeschränkt. Es wird einfacher, Personen auszugrenzen. Es wird einfacher, Randgruppen der Gesellschaft noch mehr an den Rand zu drängen. Anonymität erlaubt es Personen, welche mit einem sozialen Stigma behaftet sind, z.B. Aidskranke, Alkoholiker o.a. sich auszutauschen, ohne von der Gesellschaft ausgegrenzt und benachteiligt zu werden.

Bundestrojaner

Es kann nicht garantiert werden, dass eine installierter Bundestrojaner nur von den befugten Behörden verwendet wird. Untersuchungen haben gezeigt, dass auch das Stück Software fehlerhaft sein kann und so von unbefugten Dritten für den Zugriff auf ein System des Verdächtigen erlaubt. Dies erlaubt z.B. das Unterschieben von falschen Informationen welche dann fälschlicherweise gegen den Verdächtigen benutzt werden können.

Es kann nicht garantiert werden, dass eine installierter Bundestrojaner nur von den befugten Behörden verwendet wird. Untersuchungen haben gezeigt, dass auch das Stück Software fehlerhaft sein kann und so von unbefugten Dritten für den Zugriff auf ein System des Verdächtigen erlaubt. Dies erlaubt z.B. das Unterschieben von falschen Informationen welche dann fälschlicherweise gegen den Verdächtigen benutzt werden können.