Neuausrichtung des E-Voting durch die Bundeskanzlei

Es ist gewiss zu begrüssen, dass die Bundeskanzlei eingesehen hat, dass man E-Voting nicht einfach durch eine Verordnung einführen kann und glauben, dass man damit eine (permanente) Sicherheit gewährleistende Zertifizierung der elektronischen Abstimmung bekommen kann.

Die durch ausländische Experten entdeckten Sicherheitsmängel bei der Applikationsimplementation des Post/Scytl –Systems hätten durch inländische Experten entdeckt werden müssen. Dass dies nicht geschehen ist, kann auf eine zu wenig kritische und zu naive Haltung aller Beteiligten zurückgeführt werden: Bund, Kantone, Anbieter, Prüfinstanz. Der Verdacht liegt nahe, dass es mehr dem Umschwung in der Politik zu verdanken ist, dass die Problematik jetzt doch zu Konsequenzen geführt hat.

Sicherheitsbedenken gelten auch für einen Testbetrieb, bei dem doch schon eine stattliche Menge der normalen Stimmbürger teilnehmen soll. Die Auslandschweizer machen 10% des Elektorats aus, sie sind eine nicht zu vernachlässigende Minderheit, die ein besonderes Risiko darstellen durch deren überwiegende Nutzung von E-Voting.

Die Schwachstellen eines E-Voting sind mitnichten nur auf die schwache Implementation der Applikation begrenzt zu sehen. Mit der gleichen Durchschnittlichkeit ist auch die gesamte übrige am E-Voting beteiligte IT implementiert. Die sog. „vollständige Verifizierbarkeit“, die immer wieder bemüht wird, ist keineswegs eine Kontrolle – weder für den Einzelnen noch für eine zentrale Instanz - für die sichere Abbildung des Wählerwillens[1]. Die Applikation allein ist nicht in der Lage, dies zu gewährleisten. Es müssten sämtliche Betriebsprozesse für den Abstimmungsprozess (von der Erstellung der Codes bis zur Auswertung der *ballots*) gesichert werden können, d.h. unter Kontrolle gegen Outsider- und Insider-Angriffe gebracht. Und das ist ausgesprochen schwierig, da nur wenige Leute überhaupt das Prozedere so verstehen, dass sie in der Lage wären, es zu kontrollieren. Dabei stellen diese Leute selber wieder ein Risiko dar, das es abzudecken gälte. Darüber hinaus wird der Anbieter selbst kaum daran interessiert sein, allfällige negative Ergebnisse einer solchen Kontrolle zu finden oder gar publik zu machen. D.h. eine öffentliche Kontrolle – wie z.B. eine Wahlkommission das tut – müsste diese internen hochtechnischen Elemente und Prozesse überwachen können. Wie soll das geschehen?

Die eingesetzten Wissenschaftler sind gewiss kompetent genug, um Anforderungen an die Sicherheit zu definieren, wie sie notwendig wären. Damit ist aber die Frage der Umsetzung und Kontrolle noch nicht beantwortet. Diese Wissenschaftler werden in der fraglichen Zeit nicht am fraglichen Ort präsent sein. Sicherheitsspezialisten müssten lückenlos diese Anforderungen in konkrete, überwachte, nachvollziehbare Abläufe umsetzen können. Sie dürften dabei aber keinerlei privatwirtschaftlichen Interessen dienen.

Aufgrund des bisherigen langwierigen, dauerhaft unbefriedigenden Prozesses E-Voting einzuführen, ist die Skepsis und eine genaue Verfolgung des weiteren Geschehens weiterhin angebracht.

[1] https://www.noevoting.ch/public/downloadable/arg_d/Verifizierbarkeit.pdf

4.7.2020/dr