E-Voting CH: Was wird eigentlich getestet seit 14 Jahren ?

Es wird von der Bundeskanzlei aus immer wieder behauptet, es seien bis jetzt „alle 200 Versuche erfolgreich“ verlaufen. D.h. man hat also keine Cyberangriffe bemerkt. Wenn das so ist und es offenbar keine Probleme gibt, was will man denn mit dem Weiterführen des Testbetriebs verbessern können? Das einzige, was nämlich wirklich getestet wird, ist die Anzahl der Abstimmenden mit E-Voting. Wenn die aufwärts geht, so muss offenbar das Projekt ein Erfolg sein.

- Kann man aber daraus auch schliessen, dass E-Voting sicherer wird und somit das Weiterführen des Testbetriebs sinnvoll?
- Welche Erkenntnisse will man den aus den jahrelangen „Versuchen“ schliessen, wenn die Schwachstellen und die Risiken ja schon auf dem Papier offensichtlich und damit bekannt sind?
- Welche Firma würde Produkte in der Produktionsumgebung (mit echten Kunden) testen, deren Risiken sie bereits kennt?
- Braucht es wirklich einen Super-Gau, damit man die Risiken auch in der Politik wirklich zur Kenntnis nimmt?

Welche Gründe könnte es haben, dass man sagen kann, es habe bisher keine Verfälschungen gegeben?

	Fall	Hinweise, die dafür sprechen
1	Es hat tatsächlich niemand angegriffen, weil der Anreiz der Abstimmungsrelevanz einerseits und/oder die Erfolgsaussichten aufgrund der bisher kleinen Anzahl von E-Votern andererseits nicht gross genug war.	Die Anzahl der E-Voters war bis vor kurzem tatsächlich nur einige wenige Prozent.
2	Eine technisch-operative Sensorik für Cyberangriffe ist gar nirgends wirklich implementiert.	a) Die Cyber-Kompetenzen sind in der Schweiz generell rar und bei den Kantonen wohl noch gar nicht vorhanden. b) Die Hersteller werden sich hüten, Angriffe publik zu machen. c) Auch bei Kantonen und der Bundeskanzlei dürfte das Interesse an schlechter Publizität nicht dominieren.
3	Es haben Angriffe stattgefunden und niemand hat etwas davon bemerkt, weil diese geschickt genug vorgetragen wurden.	
4	Es haben Angriffe stattgefunden und Techniker haben etwas bemerkt, können es aber nicht sicher zuordnen und so werden von Verantwortlichen die Spuren kleingeredet, um nicht als inkompetent zu erscheinen.	
5	Es haben Leute reklamiert wegen Abweichungen von der Originalprozedur des E-Voting, aber sie wurden als digitale Anfänger eingeordnet.	Die Hotline hat bei Problemen als Generalantwort: „Die Briefwahl kann benutzt werden.“ Wieso soll man sich da mit IT Fragen herumschlagen?

Wie verordnet man Sicherheit per Gesetz?

Unbestritten ist, dass man Anforderungen an technische Systeme ins Gesetz schreiben kann. Juristen werden das so formulieren, dass sie selbst eine Vorstellung haben, wann eine Anforderung erfüllt ist und wann nicht. Die technische Umsetzung ist aber fast immer so komplex, dass sie einen technischen Experten brauchen, der ihnen das eine oder andere beweist. So lange aber kein sichtbarer Schaden vorliegt, wird nie ein Gericht darüber befinden, ob der Experte Recht hatte. Das führt zum Schluss, dass mit dem Verdecken des Schadens auch zugleich ein Freibrief für jede Art von Expertise entsteht. Weil mit falschen Abstimmungen via E-Voting kaum je ein Schadenfall bewiesen werden kann, (der Aufwand wäre massiv zu gross), ist die Expertise und damit auch so ein Gesetz absolut wertlos[1].

E-Voting wichtiger als Transparenz?

[1] In Genf hatte man versucht zu beweisen, dass das E-Votng System die Anforderungen des Gesetzes nicht erfüllt, indem ein Hacker bewies, dass er es überlisten konnte. Resultat: Der Hacker wurde verurteilt, das System belassen.