Kommentar zum Schlussbericht EXVE

Management Summary

Man kommt nicht um den Eindruck herum, dass diese Expertengruppe zu nichts anderem aufgeboten wurde als zur Absegnung der bereits existierenden Verordnung 161.116, die E-Voting regelt, mit dem Zweck, den gegenwärtigen Versuchsbetrieb in den sog. „ordentlichen Betrieb" mit gesetzlichen Grundlagen zu überführen. Detailliert gezeigt werden einzig juristische Varianten, wie die Bewilligungspraxis vereinfacht werden könnte, und wie sie möglichst optimal in die gegebenen Abgrenzungen Bund/Kantone hineinpassen.

Kostenfolgen werden nur für das volle Dematerialisierungsszenario aufgeführt, obwohl dieses zu einer ungelösten sicherheits-technischen Herausforderung führt. Und dies auch, obgleich erkannt wird, dass die gemachte Rechnung solcher Kostenfolgen völlig ungenügend ist und dass mit generellen Einsparungen überhaupt nicht gerechnet werden darf. Es ist als einziger Punkt klar geworden, dass dem Bund keinerlei zusätzliche Kosten erwachsen sollen, d.h. aber, dass alle Mehrkosten an den Kantonen hängenblieben.

Der Begriff der Verifizierbarkeit wird strapaziert bis zu einem Punkt, wo man ihn mit Sicherheit verwechseln könnte. Weder die individuelle noch die universelle Verifikation sind in ihrem ursprünglichen Sinn erreichbar. Nur die unzulässige Koppelung von Stimmabgabeüberprüfung (lokal) und Stimmauswertungsüberprüfung (zentral) ergeben den Eindruck von Sicherheit. Die beiden Prüfkomponenten sind aber gegenseitig abhängig und keiner allein ist sicher, so auch die Kombination erst recht nicht.

Zwar wird da und dort auf diverse Problemkreise und Herausforderungen aufmerksam gemacht. Zu diesen werden aber nicht inhaltliche Vorschläge unterbreitet sondern nur verfahrenstechnische mit teils zweifelhaftem Inhalt. Die Krux der Herausforderungen sind aber im Bereich des technisch-organisatorischen Umfeldes und in der Sicherheit zu suchen und diese werden bloss angedeutet und im Bedarfsfalle an die Kantone abgeschoben.

Über die Sicherheitsanforderungen an E-Voting sagen diese Experten (sie sind keine Techniker): „Es gibt kein Anpassungsbedarf, sie sind dem aktuellen Stand der Technik angemessen". Über die technisch-operativen Konsequenzen daraus sagen sie gar nichts.

Man kann sagen, der Bericht entspricht den Erwartungen, die man an eine so zusammengesetzte Expertengruppe haben darf.

1. Zusammensetzung der Expertengruppe

Die Expertengruppe umfasst:

- 3 Rechtswissenschaftler und 1 Informatikprofessor als Wissenschaftsvertreter
- 5 Kantons- und 3 Bundesvertreter, wobei letztere die Stimme ihres Chefs vertreten
- 1 Delegierter für Gleichstellungsfragen (Menschen mit Behinderungen)
- 2 Vertreter der beteiligten Industrie

Es fehlen unabhängige Experten für Cybergefahren und aus der IT Praxis. Ein einziger Vertreter aus dem ISB hat Kenntnisse darüber, der ist dürfte aber auch die Interessen des obersten Verwaltungsvertreters vertreten, welcher sich mit diesem Projekt persönlich identifiziert. 18 Jahre Investition sind ein Hindernis, neuere Erkenntnisse mit entsprechenden Konsequenzen zu versehen. Man nennt das Investitionsschutz.

2. Zielsetzung

Die Aufführung einer so detaillierten Ausgangslage lässt den Schluss zu, dass gar keine neuen Erkenntnisse mit in die Überführung in den ordentlichen Betrieb einfliessen sollen. Das einzige, was neu erkennbar ist, ist, dass man unbedingt auch noch die völlige Dematerialisierung anstrebt, wohl um wenigstens eine materielle Rechtfertigung zu haben, das ganze Projekt E-Voting retten zu können.

2.1 Dematerialisierung:

Folgende Problemkreise werden zwar erkannt und erwähnt:

1) Kompromittierung des Sicherheitskonzeptes, durch einen 2. Kanal (Briefpost) die Codes zu verschicken zu können.
2) Entkoppelung der Abstimmungskanäle (der Stimmende hat nicht mehr die freie Wahl bis zur Abstimmung, was eine sehr starke Einschränkung darstellt und die Akzeptanz gefährdet!)
3) Störung der elektronischen Wege im letzten Augenblick vor der Abstimmung
4) Verfälschung der offiziellen Unterlagen durch Cyberangriffe

Sie werden aber zum Schluss entweder in die Hoheit der Kantone delegiert, in die Forschung (1), oder es wird ein schrittweises Vorgehen mit Versuchsbetrieben vorgeschlagen. Schliesslich empfiehlt man, die E-Voting Plattform auch als Unterlagenplattform anzubieten, da sie die sicherste von allen vorgeschlagenen sei. Ein Verzicht ist offenbar nie eine Option.
Ausgiebig werden Kostenersparnisse durch Einsparung der Druckkosten berechnet, gleichzeitig wird aber eingestanden, dass diese Rechnung unvollständig ist und mit Einsparungen eigentlich gar nicht gerechnet werden darf. Auch wird betont, dass für (1) gar noch keine sicherheitstechnisch akzeptable Lösung in Sicht ist.

2.2 Limitierung des Evoting Elektorats aufheben

Die Überführung in den ordentlichen Betrieb impliziert quasi die Aufhebung der Limiten, denn es ist rechtlich nicht zu rechtfertigen, dass einige Leute diesen 3. Stimmkanal nutzen können und andere nicht. Zwar wird die Risikominimierung durch die Limitierung angesprochen, aber offenbar ist diese jetzt – im ordentlichen Betrieb - völlig unnötig, ohne dass man hier ein Argument dafür lesen könnte. Es wird einzig auf die lange Testphase verwiesen, **nicht aber darauf, dass in dieser Phase wegen der geringen Beteiligung kaum ein Anreiz für einen ernsthaften Gegner bestand, mit Cyberwaffen abzugreifen.**

2.3 Der Verifizierbarkeitsbegriff

Obwohl dieser Begriff offenbar nicht wissenschaftlich anerkannt ist, wird er hier verwendet, um die Sicherheit der Anlage glaubhaft zu machen. Man sollte aber eigentlich nur von Verifizierbarkeit reden, wenn sie End-to-End erfüllt ist. Individuell: **Ich** kann meine Stimmabgabe und die Auswertung überprüfen. Universell: **Jeder** kann die korrekten Stimmabgaben und –auswertungen überprüfen. Leider geht das nicht unter der Wahrung des Abstimmungsgeheimnisses und deshalb greift man zum Kunstbegriff: „Vollständig“ mit folgendem Inhalt: Ich überprüfe die Abgabe und die Zentrale überprüft die Auswertung. Leider weiss aber die Zentrale genausowenig, ob ich wirklich überprüft habe wie ich auch nicht weiss, ob die Zentrale richtig überprüft. Darum habe weder ich noch die Zentrale eine Gewissheit. Wie sog. „Begleitgruppen“ sicherstellen sollen, dass die Zentrale richtig auswertet ist genauso unklar, wie die Frage, was macht man mit all denen, die Codeüberprüfung nicht 100%ig richtig vornehmen.

2.4 Abgrenzung Bund/Kantone

Aus juristischer Sicht ist vor allem die Abgrenzung zw. Bund und Kantonen eine Herausforderung, waren doch die Abstimmungen bis anhin vor allem eine kantonale Aufgabe.

2.4.1 Bundesaufgaben

Der Bund erteilt Zertifikate für die Hersteller und gibt Bewilligungen für die Kantone, wenn sie neben einem zertifizierbaren System auch noch die rechtlichen Anforderungen erfüllen. Dabei wird technisch gefordert:

1) Keine unverschlüsselten Daten dürfen je auf dem Eingabegerät vorkommen

   ➔ Diese Anforderung kann nicht wirklich eingehalten werden. Unverschlüsselt sind die Daten immer bei der Bearbeitung. Ein Trojaner kann diese genau dann kopieren und irgendwohin in die Welt senden.

2) Unabhängige Mittel müssen eingesetzt werden

   ➔ Es wird nicht definiert, was *unabhängige* Mittel sind. Im Extremfall müsste man alle einzelnen Module von verschiedenen Herstellern haben und mit verschiedenen Betreibern betreiben lassen. Jeder IT Fachmann würde so eine Forderung als komplett unrealistisch zurückweisen.

3) Offenlegung Quellcode

   ➔ Selbst wenn dies der Fall ist, - es ist heute noch nicht der Fall -, so stellt dies zwar eine Notwendigkeit dar, ist aber nicht hinreichend. Neben der Applikation gibt es noch zahlreiche andere Hilfsmittel, deren Quellcode ebenso offengelegt werden müsste, es aber niemals wird. Ausserdem ist so eine Überprüfung eine riesige Forschungsarbeit, die u.U. Jahre dauern könnte. In dieser Zeit kann sich der Quellcode bereits wieder ändern.

4) Intrusion Tests

   ➔ Intrusion Tests gehören zu jeder Entwicklung, sie geben aber keine Gewähr für Sicherheit. Sie geben aber erstens nur eine Momentaufnahme, die schon nach dem nächsten Update jedes Moduls obsolet sein könnte. Ausserdem decken sie zweitens nur die bereits bekannten Schwachstellen ab, und auch davon nur einen ausgewählten Teil. Dazu kommt drittrens, dass die Gegnerschaft vor allem aus Amateuren besteht, die in ihrer Freizeit sich im Hacken versuchen. Die richtigen Gegner, vor denen man sich schützen sollte, werden bei so einem Ereignis niemals auftreten. Es gäbe mit 250 KFr. Preisgeld auch nicht genügend Budget, professionelle Kräfte dafür einzusetzen.

2.4.2 Kantonsaufgaben

Die Kantone sorgen für die Einhaltung der Sicherheitsbestimmungen, die so allgemein formuliert sind, dass man zwar nichts dagegen sagen kann, aber die nie und nimmer umsetzbar sind.

1) Transparenz und Nachvollzug Prüfprozess

   ➔ Wird gefordert, aber nicht definiert. Die komplexen Vorgänge bei der Auszählung darzustellen und den Kantonsbeamten oder Wahlkommissionen verständlich zu machen dürfte für die beteiligten Informatiker ein Ding der Unmöglichkeit werden. Es besteht die akute Gefahr, dass dies zu einem wertlosen Ritual wird.

2) Begleitgruppen

➔ Werden gefordert aber nicht definiert. Wer will Verantwortung übernehmen, um etwas zu prüfen, was er nicht verstehen kann? Was ist so eine Überprüfung wert?

3) Alle eingegangenen Stimmen müssen korrekt gezählt werden

➔ Was ist mit den verhinderten Stimmen, die vom Abstimmenden nicht als Manipulation erkannt wurden?

4) Der Umgang mit Rückmeldungen

➔ Es wird gefordert, dass dies geregelt werden muss, aber es gibt keine Empfehlungen, wie. Es wird nicht bedacht, dass dies schnell zu aufwendigen Kontrollen führt, die in ihrem Ausmass nicht abgeschätzt werden können. Es ist auch unklar, bei welchen Limiten man welche Massnahmen treffen muss. Dies führt zu Unsicherheiten oder sogar zu Willkür. Was, wenn ein Kanton das Abstimmungsergebnis nicht beglaubigen kann? Geht man dann davon aus, dass nur dieser Kanton betroffen ist? Bei wieviel Meldungen rechnet man mit wieviel Manipulation?

3. Verbleibende Unklarheiten aus Sicht der Expertengruppe

1) Folgende Bereiche haben auch gemäss EXVE noch Klärungsbedarf

- Wie der Bund mit der gegenwärtigen Monopolsituation (POST als einziger Anbieter) umgehen soll, ist auch der Expertengruppe – bestehend vor allem aus Juristen - unklar.

Folgende Problemkreise sollen die Kantone (irgendwie) regulieren:

- Kommunikation mit Publikum (Fachleute sind nicht inbegriffen)
- Begleitgruppen und Prüfprozesse
- Krisenvereinbarungen: Umgang mit Unregelmässigkeiten

2) Vorgehen bis zur vollständige Dematerialisierung
Hier empfiehlt man:

- Stufenweises Vorgehen, bis Stufe 4 offenbar kein Problem, die E-Voting Plattform sei die sicherste.

➔ Die Attacke auf CHVote ist der Beweis dafür, dass dies keine Lösung ist!

- Bei Stufe 5 braucht es noch ein zu definierendes Sicherheitselement. Nach diesem soll geforscht werden. Man erkennt die Auslandabhängigkeit als Problem.

➔ Wer anders als die „Expertengruppe“ soll dafür eine Lösung vorschlagen?

- Permanente Wahlfreiheit der Kanäle umstritten, da Einsparungen nur mit entkoppelten Kanälen funktionieren, ohne solche Wahlfreiheit ist aber die Akzeptanz gefährdet.

➔ Hier werden die Probleme zwar genannt, aber Konsequenzen werden keine gezogen.

3.1 Generische Lösungsansätze der Expertengruppe für die ungelösten Fragen

Es fällt auf, dass Probleme zwar erkannt werden, aber auf eine Weise gelöst werden sollen, die für die Administration möglichst einfach funktioniert und ja nichts an der bestehenden Zielsetzung ändert. Die inhaltliche oder politische Dimension fehlt meist.

Vorgeschlagene Lösungsansätze der Expertengruppe:

- Die Kantone sollen es regeln, es braucht Spielraum für die Kantone, auch wenn unterschiedliche Rechtssetzungen in den Kantonen für die Ausübung der politischen Rechte keine Berechtigung haben

- Der Benutzer muss halt aufpassen

- Die Anforderung wird ins Gesetz geschrieben, auch wenn niemand diese prüfen kann

- Man soll in Teilschritten auf das ungelöste Problem zugehen (Dema) und im Notfall einen Versuchsbetrieb einrichten

➔ Untauglich!

24.12.2018/dr