

Rathaus / Barfüssergasse 24
4509 Solothurn
Telefon 032 627 20 79
Telefax 032 627 22 69
pd@sk.so.ch
www.parlament.so.ch

I 222/2013 (STK)

Interpellation Daniel Urech (Grüne, Dornach): Ist die Sicherheit der elektronischen Stimmabgabe gewährleistet? (18.12.2013)

Das Vertrauen der Öffentlichkeit in die Sicherheit der Stimmabgabe über das Internet ist in letzter Zeit in Frage gestellt worden. Es hat sich gezeigt, dass grenzenlose nachrichtendienstliche Aktivitäten im Internet eine saubere Verschlüsselungstechnologie für sensible Daten erfordert. In einem konkreten (glücklicherweise öffentlichen) Versuch hat in diesem Jahr ein Hacker aufgezeigt, wie das System der elektronischen Stimmabgabe des Kantons Genf überlistet werden kann.

Die Einführung von E-Voting (respektive gemäss Bund: Vote électronique; VE) darf nur weiter verfolgt und ausgedehnt werden, wenn Sicherheitsbedenken komplett ausgeräumt werden. Der Bund hat dies grundsätzlich auch anerkannt, will aber die höheren Anforderungen (insbesondere Verifizierbarkeit, Systeme zweiter Generation), den Kantonen noch nicht für den aktuellen Ausdehnungsschritt sondern erst längerfristig vorschreiben.

Der Regierungsrat wird in diesem Zusammenhang darum gebeten, folgende Fragen zu beantworten:

1. Teilt der Regierungsrat die Einschätzung, dass Sicherheitsrisiken bei der elektronischen Stimmabgabe das Potenzial haben, das Vertrauen in die demokratischen Prozesse zu erschüttern?
2. Wie beurteilt der Regierungsrat die Tatsache, dass ein Hacker öffentlich eine Sicherheitslücke im Genfer VE-System aufgedeckt hat?
3. Besteht diese oder eine ähnliche Sicherheitslücke auch im System, das der Kanton Solothurn momentan nutzt?
4. Wann ist für den Kanton Solothurn die nächste Generation der VE-Systeme verfügbar ist, welche die volle (individuelle und universelle) Verifizierbarkeit zulässt?
5. Ist geplant, eine Ausdehnung von VE im Kanton Solothurn erst vorzunehmen, wenn diese Verifizierbarkeit sichergestellt ist? Wenn nein, weshalb nicht?
6. Könnte die Veröffentlichung des Quellcodes der verwendeten Software und die damit einhergehende Überprüfungsmöglichkeit der Sicherheitsarchitektur das öffentliche Vertrauen in VE stärken?
7. Ist der Regierungsrat bereit, sich für die Veröffentlichung des Quellcodes der verwendeten Software einzusetzen?
8. Mit welchen Mitteln kann verhindert werden, dass allfällige Malware auf dem Computer der Abstimmenden zur Manipulation der Stimmabgabe führt?
9. Ist der Regierungsrat bereit, den Ausbau der VE zu sistieren oder gar rückgängig zu machen, wenn sich Missbrauchsmöglichkeiten zeigen sollten?

Begründung (18.12.2013): Im Vorstosstext enthalten.

Unterschriften: 1. Daniel Urech, 2. Barbara Wyss Flück, 3. Fabian Müller, Rudolf Hafner, Christian Thalmann, Marguerite Misteli Schmid, Franziska Roth, Albert Studer, Beat Wildi, Marianne Meister, Felix Wettstein, Christine Bigolin Ziörjen, Bruno Vögtli, Simon Esslinger, Evelyn Borer, Urs Huber, Mathias Stricker, Anna Rüefli, Doris Häfliger, Felix Lang, Brigit Wyss, Markus Knellwolf, Beatrice Schaffner, Nicole Hirt, Michael Ochsenbein, Peter Brotschi (26)