IIIIII KANTON solothurn

Regierungsratsbeschluss

vom 14. Januar 2014

Nr. 2014/72
KR.Nr. I 222/2013 (STK)

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

---

1. Vorstosstext

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, 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?

2. Begründung

Im Vorstosstext enthalten.

3. Stellungnahme des Regierungsrates

3.1 Einleitende Bemerkungen

Bundesrat und Parlament haben die Strategie zur schrittweisen und kontrollierten Einführung von Vote électronique (VE) im März 2007 gutgeheissen und die nötigen Rechtsgrundlagen auf Bundesebene geschaffen. Die Bundeskanzlei ist einerseits damit beauftragt, die Koordination der kantonalen VE-Projekte sicherzustellen und die Kantone bei der Einführung der elektronischen Stimmabgabe zu unterstützen; überdies ist sie für das Bewilligungsverfahren von VE-Versuchen und für die Kontrolle der Einhaltung der bundesrechtlichen Anforderungen zuständig. Das VE-Projekt ist in die vom Bundesrat am 24. Januar 2007 verabschiedete nationale E-Government-Strategie Schweiz eingebettet und gilt als priorisiertes Vorhaben.

Am 14. Juni 2013 hat der Bundesrat seinen dritten Bericht zu Vote électronique verabschiedet. Gestützt auf die Evaluation der Versuchsphase 2006-2012 definierte er darin die Bedingungen für die Ausdehnung der elektronischen Stimmabgabe. Mit dem Ziel der flächendeckenden Einführung des dritten, komplementären Stimmkanals beschloss der Bundesrat, in einem ersten Schritt die rechtlichen Grundlagen für die Durchführung von Versuchen mit der elektronischen Stimmabgabe anzupassen. Die Rechtsgrundlagen für die elektronische Stimmabgabe via Internet wurden im Lichte der gesammelten Erfahrungen und zum Zweck der Anpassung an die neusten, vor allem technischen Entwicklungen revidiert und ergänzt.

Der Kanton Solothurn führt sein VE-Projekt im Rahmen eines Consortiums mit 7 anderen Kantonen (Aargau, Freiburg, Graubünden, Schaffhausen, St. Gallen, Thurgau und Zürich) auf der Basis der von der UNISYS AG für den Kanton Zürich entwickelten VE-Lösung. Hier konnten die im Stimmregister registrierten und zu VE zugelassenen Auslandschweizerinnen und Auslandschweizer seit Beginn der VE-Versuche im September 2010 an 10 Urnengängen elektronisch abstimmen. Diese Urnengänge sind alle erfolgreich durchgeführt worden.

3.2 Zu den Fragen

3.2.1 Zu Frage 1:

Teilt der Regierungsrat die Einschätzung, dass Sicherheitsrisiken bei der elektronischen Stimmabgabe das Potenzial haben, das Vertrauen in die demokratischen Prozesse zu erschüttern?

Vertrauen spielt eine bedeutende Rolle bei der Ausübung der politischen Rechte, insbesondere bei der elektronischen Stimmabgabe. Zwischenfälle können das Vertrauen in die demokratischen Prozesse erschüttern. Die Sicherheit bei der elektronischen Stimmabgabe hat für Bund und Kantone oberste Priorität. Für die Weiterentwicklung gilt der Grundsatz ‚Sicherheit vor Tempo'. Fehlfunktionen im Wahl- und Abstimmungsverlauf und systematische Missbräuche müssen erkannt und verhindert werden.

Der Bundesrat hat am 13. Dezember 2013 noch höhere Sicherheitsanforderungen für die künftigen Systeme bestimmt. Erst nach Umsetzung der erhöhten Sicherheitsanforderungen kann die Anzahl der Stimmberechtigten, die an den VE-Versuchen teilnehmen darf, erhöht werden. Zusätzlich zur Umsetzung der individuellen Verifizierbarkeit und weiterer Sicherheitsanforderungen müssen die Systeme strenge Sicherheitsprüfungen (Audits) bestehen, die durch unabhängige, vom Bund akkreditierte Stellen

durchgeführt werden. Die Einhaltung der Sicherheitsanforderungen wird durch eine spezialisierte, externe Stelle bestätigt. Nebst der Grundbewilligung des Bundesrates prüft die Bundeskanzlei zusätzlich vor jedem Urnengang, ob die Voraussetzungen für einen VE-Versuch erfüllt sind. Bis zur Umsetzung der neuen Anforderungen gelten die Limiten von 30% des kantonalen und 10% des gesamtschweizerischen Elektorats als Massnahmen zur Risikominimierung.

3.2.2 Zu Frage 2:

Wie beurteilt der Regierungsrat die Tatsache, dass ein Hacker öffentlich eine Sicherheitslücke im Genfer VE-System aufgedeckt hat?

Bis zum heutigen Zeitpunkt gibt es keine Hinweise darauf, dass infolge einer Attacke Stimmen manipuliert worden wären. Entgegen gewisser Schlagzeilen in den Medien gab es keinen echten Hackerangriff auf das Genfer System. Fakt ist, dass ein Hacker anlässlich einer Konferenz in Paris im Juni 2013 die Wirkungsweise von Schadsoftware unter Laborbedingungen demonstriert hat. Anhand eines Nachbaus des Genfer Systems simulierte er, wie man eine Stimme auf der Plattform eines Stimmberechtigten vor dem Abschicken unbemerkt ändern könnte. Von einem Konstruktionsfehler des Genfer Systems kann daher keine Rede sein. Vielmehr bestätigte die Demonstration die allgemeine Erkenntnis, dass Computer gegen Cyberangriffe nicht zu 100 Prozent geschützt werden können. Im Zentrum der neuen Sicherheitsstandards steht deshalb die individuelle Verifizierbarkeit. Damit können die Stimmenden künftig zuverlässig kontrollieren, ob ihre Stimme das System unverändert erreicht hat (bzw. dass sie nicht durch ein Schadprogramm auf dem verwendeten Computer manipuliert wurde).

3.2.3 Zu Frage 3:

Besteht diese oder eine ähnliche Sicherheitslücke auch im System, das der Kanton Solothurn momentan nutzt?

Das Genfer E-Voting-System ist anders als das vom Kanton Solothurn bzw. vom Consortium verwendete System aufgebaut. Eine der Demonstration ähnliche Attacke kann es beim System des Consortiums nicht geben. Die Consortiumskantone sind sich aber bewusst, dass theoretisch auch auf ihrem System Hackerangriffe durchgeführt werden könnten. Schwachstellen der betroffenen Art sind der seitens des Bundes für das Projekt verantwortlichen Bundeskanzlei und den Verantwortlichen in den Kantonen denn auch längst bekannt. Um die Risiken, die mit solchen Attacken in Verbindung stehen, genügend gering zu halten, ist die elektronische Stimmabgabe bei eidgenössischen Urnengängen derzeit auf maximal 10 Prozent des gesamtschweizerischen Elektorats beschränkt. Auf kantonaler Ebene dürfen zudem nicht mehr als 30 Prozent der Stimmberechtigten in einen Versuch mit der elektronischen Stimmabgabe einbezogen werden. Effektiv zugelassen waren bisher bei eidgenössischen Urnengängen nur gerade rund 3 Prozent aller Stimmberechtigten.

3.2.4 Zu Frage 4:

Wann ist für den Kanton Solothurn die nächste Generation der VE-Systeme verfügbar, welche die volle (individuelle und universelle) Verifizierbarkeit zulässt?

Die individuelle Verifizierbarkeit wird schon mit dem Einsatz des Systems der zweiten Generation ab 2015 möglich sein. Die universelle Verifizierbarkeit ist geplant und wird ab 2018 verfügbar sein. Sie gewährleistet in Zukunft, dass die korrekte Verarbeitung sämtlicher für die Ergebnisermittelung relevanter Daten mit systemunabhängigen Mitteln überprüft werden kann.

3.2.5 Zu Frage 5:

Ist geplant, eine Ausdehnung von VE im Kanton Solothurn erst vorzunehmen, wenn diese Verifizierbarkeit sichergestellt ist? Wenn nein, weshalb nicht?

In einem ersten Ausdehnungsschritt sind ab 2015 VE-Versuche mit Stimmberechtigten aus 5 Pilotgemeinden geplant. Diese Ausdehnung erfolgt zeitgleich mit der Einführung des VE-Systems der zweiten Generation, d.h. zusammen mit der individuellen Verifizierbarkeit. Die Stimmenden können dann mittels Codes überprüfen, ob ihre Stimme gemäss ihrer Absicht abgegeben wurde (Code-Voting). Eine weitere Ausdehnung der Versuche auf alle Stimmberechtigten des Kantons Solothurn ist erst möglich mit der Einführung eines Systems mit sowohl individueller als auch universeller Verifizierbarkeit. Dieses wird gemäss aktueller Planung erst ab 2018 verfügbar sein.

3.2.6 Zu Frage 6:

Könnte die Veröffentlichung des Quellcodes der verwendeten Software und die damit einhergehende Überprüfungsmöglichkeit der Sicherheitsarchitektur das öffentliche Vertrauen in VE stärken?

Der Quellcode gibt Aufschluss darüber, wie die Daten verarbeitet werden sollen. Sowohl die Offenlegung des Quellcodes als auch die Verifizierbarkeit können das Vertrauen in die elektronische Stimmabgabe stärken.

3.2.7 Zu Frage 7:

Ist der Regierungsrat bereit, sich für die Veröffentlichung des Quellcodes der verwendeten Software einzusetzen?

Wir sind bereit, uns für die Offenlegung des Quellcodes einzusetzen. Die Vertreter der Kantone aller drei Systeme prüfen zur Zeit die Möglichkeiten und planen, den Zugang zum Quellcode für die Systeme der zweiten Generation zu ermöglichen. Eine Umsetzung ist jedoch mit verschiedenen Herausforderungen verbunden. Diese hängen mit den unterschiedlichen rechtlichen Voraussetzungen sowie mit den Verträgen zwischen den Kantonen und ihren Dienstleistern zusammen. Entsprechende Abklärungen sind bereits im Gange.

3.2.8 Zu Frage 8:

Mit welchen Mitteln kann verhindert werden, dass allfällige Malware auf dem Computer der Abstimmenden zur Manipulation der Stimmabgabe führt?

Direkt können wir keinen Einfluss auf die Computer der Stimmenden nehmen. Deshalb können wir auch nicht verhindern, dass Computer im Einsatz sind, welche durch Malware beeinflusst werden. Wir weisen jedoch die Stimmberechtigten in den Unterlagen wiederholt darauf hin, dass sie ihr System ausreichend gegen Viren und andere Schadsoftware schützen sollten. Durch den Fingerprint auf dem Stimmrechtsausweis können die Stimmenden sicherstellen, dass sie mit dem korrekten Server kommunizieren. Ausserdem macht das individuelle Verifizierungs-Symbol auf dem Stimmrechtsausweis das korrekte Ankommen der Stimmabgabe überprüfbar.

3.2.9 Zu Frage 9:

Ist der Regierungsrat bereit, den Ausbau der VE zu sistieren oder gar rückgängig zu machen, wenn sich Missbrauchsmöglichkeiten zeigen sollten?

Die Strategie des Bundesrates und der Kantone sowie der Grundsatz ‚Sicherheit vor Tempo' zwingen uns zu einem verantwortungsbewussten Umgang mit Risiken und zu einem vorsichtigen und etappierten Vorgehen. Falls trotz aller Sicherheitsvorkehren Missbräuche feststellbar sind, werden wir die Lage prüfen und die nötigen Massnahmen ergreifen. Nötigenfalls werden wir auch den VE-Ausbau sistieren.

Andreas Eng
Staatsschreiber

Verteiler

Staatskanzlei (Eng, Stu, Rol, Wyl)
Parlamentsdienste
Traktandenliste Kantonsrat