Curia Vista - Geschäftsdatenbank

13.3812 – Motion

Kein unsicheres E-Voting. Nur Systeme mit Verifizierbarkeit und offenem Source Code zulassen

Eingereicht von	 Glättli Balthasar
Einreichungsdatum	26.09.2013
Eingereicht im	Nationalrat
Stand der Beratung	Erledigt

Eingereichter Text

Der Bundesrat wird beauftragt, die Artikel 27a bis 27q VPR folgendermassen anzupassen:

1. Er stoppt E-Voting-Versuche mit Systemen der ersten Generation.

2. Zugelassen sind per sofort nur Systeme, welche nicht nur die Sicherheit und Anonymität der Stimmabgaben gewährleisten, sondern die es auch ermöglichen, dass der bzw. die Stimmberechtigte persönlich die korrekte Übertragung seiner bzw. ihrer Stimme überprüft und dass die Abstimmungsresultate ohne Bruch des Stimmgeheimnisses nachträglich verifiziert werden können (Systeme der zweiten Generation).

3. Ausnahmen von den Ziffern 1 und 2 sind allenfalls übergangsweise für die Stimmabgabe von Auslandschweizern und -schweizerinnen vorzusehen.

4. Der Quellcode sämtlicher verwendeter Systeme muss zudem vollständig offengelegt werden (Open Source), um allen Interessierten die Überprüfung von Schwachstellen und Sicherheitslücken zu ermöglichen.

Begründung

Die Medien haben kürzlich darüber berichtet, dass ein Hacker das Genfer E-Voting-System hacken konnte. Zum Glück geschah dies aus pädagogischer und nicht aus böswilliger Absicht. Der Hacker hat eine Fehlkonstruktion des Systems ausgenützt, welche als "Ursprungsfehler" dieses Systems der ersten Generation betrachtet wird. Ein solches Risiko für die Demokratie darf nicht geduldet werden.

Parallel hat der Bundesrat in seinem dritten Bericht des Bundesrates zu Vote électronique angekündigt, dass er bereits per 1. Januar 2014 den Kantonen eine Erhöhung der Grenze des zu elektronischer Stimmabgabe zugelassenen Elektorats erlauben will. Gleichzeitig bleiben Systeme der ersten Generation zugelassen. Leider findet die Sicherheitsprüfung der erwähnten Lücke im Genfer System erst nach diesem Termin statt. Daher gibt es die Gefahr, dass eine grosse Anzahl von Stimmabgaben einer Manipulation ausgesetzt wird. Dadurch könnten eine oder mehrere Volksabstimmungen gefälscht werden.

Das Vertrauen in korrekte Wahlresultate ist für die Akzeptanz von Wahl- und Abstimmungsresultaten aber zentral. Um dieses notwendige Vertrauen in Vote électronique zu schaffen, muss einerseits der Quellcode der verwendeten Systeme unbedingt offengelegt werden, damit er auch von Dritten auf mögliche Sicherheitslücken überprüft werden kann. Andererseits muss die Verifizierbarkeit der individuellen Resultate - wie zum Beispiel Norwegen -, aber auch der Gesamtresultate gewährleistet sein.

Stellungnahme des Bundesrates vom 06.11.2013

Es gab keinen erfolgreichen Hackerangriff auf das Genfer System der elektronischen Stimmabgabe. Fakt ist, ein Hacker hat das Genfer System lediglich nachgebaut und darauf unter Laborbedingungen die Wirkungsweise von Schadsoftware demonstriert. Dies kann z. B. damit verglichen werden, dass bei der brieflichen Stimmabgabe im Rahmen einer fiktiven Abstimmung von einem eingeweihten Postboten verlangt wird, er solle ein Ja zu einem Nein ändern, bevor er den Brief der Gemeinde ausliefere. Vom Prinzip her greift die Schadsoftware bei beliebigen Applikationen, die auf moderner Webtechnologie basieren. Das Problem liegt denn auch bei den eingesetzten Plattformen (etwa PC, Tablet oder Smartphone) und nicht beim von den Behörden kontrollierbaren Teil des Systems. Von einem Konstruktionsfehler des Genfer Systems kann daher keine Rede sein. Vielmehr bestätigt die Demonstration die allgemeine Erkenntnis, dass Computer gegen Cyberangriffe nicht zu 100 Prozent geschützt werden können. Dieser Umstand wurde bereits im Vorfeld der ersten Versuche mit der elektronischen Stimmabgabe vor über zehn Jahren berücksichtigt.

Die Strategie des Bundesrates "Sicherheit vor Tempo" zwingt zu einem verantwortungsbewussten Umgang mit Risiken. In diesem Sinne wurde in der Verordnung über die politischen Rechte festgelegt, dass höchstens 30 Prozent des kantonalen und höchstens 10 Prozent des bundesweiten Elektorats ihre Stimme elektronisch abgeben können. In der Praxis wurden bislang nie mehr als 3 Prozent zugelassen. Dank dieser Limiten und dank verschiedener Sicherheitsmassnahmen sind die Restrisiken, die mit Schadsoftware in Zusammenhang stehen, als gering einzustufen. Es besteht deshalb aus Sicht des Bundesrates kein Anlass, die Versuche zu unterbrechen.

Die Erhöhung der Limiten erfordert zusätzliche Sicherheitsmassnahmen. Diese übertreffen die geläufigen Mechanismen, die bei anderen, ebenfalls sicherheitskritischen Applikationen angewendet werden, bei Weitem. Konkret müssen die Stimmenden nachvollziehen können, dass ihre Stimme weder auf der zur Stimmabgabe verwendeten Plattform noch im Internet verändert wurde (individuelle Verifizierbarkeit). Erst dann können maximal 50 statt 30 Prozent eines kantonalen Elektorats zur elektronischen Stimmabgabe zugelassen werden. Diese Bestimmung wird in der geplanten Verordnung der Bundeskanzlei über die elektronische Stimmabgabe (Veles) festgehalten. Diese soll voraussichtlich am 1. Januar 2014 in Kraft treten. Allerdings wird das erste individuell verifizierbare System nicht vor Ende 2014 im Einsatz sein. Bis dahin bleiben die heute geltenden Limiten bestehen. Zusätzlich zur Umsetzung der individuellen Verifizierbarkeit und weiterer Sicherheitsanforderungen müssen die Systeme Sicherheitsprüfungen bestehen, die durch unabhängige, vom Bund akkreditierte Stellen durchgeführt werden. Die Limiten können erst dann aufgehoben werden, wenn zusätzlich zur individuellen Verifizierbarkeit die korrekte Verarbeitung sämtlicher für die Ergebnisermittlung relevanter Daten mit systemunabhängigen Mitteln überprüft werden kann (vollständige Verifizierbarkeit). Dazu müssen sichere kryptografische Methoden zum Einsatz kommen, wie sie aus der technischen Wissenschaft bekannt sind. Vertreter der technischen Wissenschaft wurden bei der Erarbeitung der Sicherheitsstandards wie auch der geplanten Rechtsgrundlagen einbezogen.

Die Verifizierbarkeit bietet noch mehr Einsicht in den elektronischen Urnengang als die Offenlegung des Quellcodes. Während der Quellcode Aufschluss darüber gibt, wie die Daten verarbeitet werden sollen, gibt die Verifizierbarkeit Aufschluss darüber, wie die Daten tatsächlich verarbeitet wurden. Dennoch wollen die Kantone die Möglichkeiten einer Offenlegung des Quellcodes prüfen. Hier gilt es jedoch zu berücksichtigen, dass eine Umsetzung mit verschiedenen Herausforderungen verbunden ist. Diese hängen nicht zuletzt mit den unterschiedlichen rechtlichen Voraussetzungen in den Kantonen sowie mit den Verträgen zwischen den Kantonen und ihren Dienstleistern zusammen.

Im Übrigen wird auf die Stellungnahme des Bundesrates zur Motion Schwaab 13.3808 verwiesen.

Antrag des Bundesrates vom 06.11.2013
Der Bundesrat beantragt die Ablehnung der Motion.

Dokumente

Amtliches Bulletin - die Wortprotokolle

Chronologie / Wortprotokolle

Datum	Rat	
02.06.2014	NR	Ablehnung.

Erstbehandelnder Rat
Nationalrat

Mitunterzeichnende (33)
Amarelle Cesla Badran Jacqueline Borer Roland F. Brunner Toni Chevalley Isabelle Fehr Hans Fridez Pierre-Alain Friedl Claudia Gilli Yvonne Girod Bastien Glättli Balthasar Heer Alfred John-Calame Francine Kaufmann Hans Leuenberger Ueli Leutenegger Oberholzer Susanne Müller Geri Nordmann Roger Pardini Corrado Piller Carrard Valérie Reimann Lukas Rickli Natalie Simone Rutz Gregor A. Rytz Regula Schelbert Louis Schwaab Jean Christophe Thorens Goumaz Adèle Tornare Manuel Trede Aline van Singer Christian Vischer Daniel Weibel Thomas Wermuth Cédric

Deskriptoren: Hilfe
erleichterte Stimmabgabe Datenschutz Computerkriminalität Akzeptanz Software angewandte Informatik

Ergänzende Erschliessung:
34;04

Zuständig

Bundeskanzlei (BK)