30. Mai 2018

Vote électronique: Offenlegung des Quellcodes

Erläuternder Bericht zur Anpassung der Verordnung der Bundeskanzlei über die elektronische Stimmabgabe (VEleS)

1 Ausgangslage

An seiner Sitzung vom 5. April 2017 hat der Bundesrat die nächsten Schritte zur flächendeckenden Einführung der elektronischen Stimmabgabe beschlossen. Im Fokus standen Massnahmen im Bereich der Transparenzbildung sowie die Überführung der elektronischen Stimmabgabe von der derzeitigen Versuchsphase in den ordentlichen Betrieb.

Als Massnahme zur Transparenzbildung hat der Bundesrat beschlossen, die Offenlegung des Quellcodes zur bundesrechtlichen Voraussetzung für den Einsatz des elektronischen Stimmkanals zu erheben. Der Bundesrat hat die Bundeskanzlei beauftragt, die Verordnung der Bundeskanzlei über die elektronische Stimmabgabe (VEIeS; SR 161.116) entsprechend anzupassen.

2 Forderung nach mehr Transparenz

Mit der individuellen und der vollständigen Verifizierbarkeit (Art. 4 bzw. 5 VEleS) stellt der Bund Anforderungen im Bereich der Transparenz. Auf der Grundlage der während eines Urnengangs anfallenden Daten erlaubt es die vollständige Verifizierbarkeit nachzuvollziehen, dass die Stimmen korrekt registriert sowie verarbeitet wurden. Erst nach der Umsetzung der vollständigen Verifizierbarkeit und der Zertifizierung der Systeme sind die rechtlichen Voraussetzungen für den flächendeckenden Einsatz der elektronischen Stimmabgabe erfüllt. Die Entwicklung der vollständigen Verifizierbarkeit ist im Gang und sollte gemäss der Planung der Systemanbieter per Ende 2018 abgeschlossen sein.

Im Rahmen der Beantwortung resp. Beratung parlamentarischer Vorstösse hat der Bundesrat mehrfach der Bundesversammlung versichert, „die Frage des Zugangs zum Quellcode mit den Kantonen vertieft abzuklären mit der Absicht, diesen als Voraussetzung für die Zulassung der Systeme im Rahmen der nächsten Revision der Rechtsgrundlagen aufzunehmen“.[1] Zudem wurde in der Debatte zur Motion 13.3808 Schwaab „Nichts überstürzen bei der Ausdehnung von Vote électronique“ zugesichert, dass Bund und Kantone die Durchführung öffentlicher Intrusionstests prüfen werden. Diese Prüfung ist im Rahmen der Unterarbeitsgruppe „Transparenz und Öffentlichkeit“ (UAG) im Jahr 2016 erfolgt. Die Systemanbieter haben im Bereich der Transparenzbildung bereits Schritte unternommen und Informationen zur Funktionsweise der Systeme offengelegt.

[1] Motion 15.3492 Romano (Darbellay) „Pour un système de vote électronique public et transparent“, Motion 15.4237 Reimann „E-Voting. Ja, aber nur mit Transparenz“ sowie Anfrage 16.1076 Schwaab “Un test *grandeur nature* de la sécurité du vote électronique?“.

3 Die Bestimmungen im Einzelnen

Beim Quellcode handelt es sich um den Text eines Computerprogrammes. Er wird von Menschen geschrieben, ist für Menschen lesbar und beschreibt die Funktionsweise des Computerprogrammes. Die Offenlegung des Quellcodes ist von der Umsetzung der vollständigen Verifizierbarkeit klar zu unterscheiden. Der Quellcode dokumentiert, *wie* die Stimmen vom System registriert und verarbeitet werden *sollen*. Die für die vollständige Verifizierbarkeit erhobenen Informationen dokumentieren, *dass* die Stimmen tatsächlich korrekt registriert und verarbeitet *wurden*.

Die Offenlegung von Informationen hat das Potenzial, Vertrauen in der Öffentlichkeit aufzubauen und nachhaltig zu festigen. Zum einen dient sie fachkundigen Kreisen dazu, sich jederzeit von der Sicherheit und der Qualität der Systeme überzeugen zu können. Umgekehrt erhalten die Behörden die Möglichkeit, frühzeitig Verbesserungen vorzunehmen, sollten externe Fachleute Mängel feststellen. Zudem trägt die Offenlegung von Informationen zu einer sachlichen Debatte bei und wirkt der Abhängigkeit von einzelnen Personen und Organisationen entgegen.

Artikel 7 Absatz 2 Bst. f und Abs. 3 VEleS

In Art. 7 VEleS betreffend die Überprüfung wird eine Differenzierung eingeführt. Diese steht in direktem Zusammenhang mit den neuen Bestimmungen zur Offenlegung des Quellcodes in Art. 7a und 7b VEleS. Die Offenlegung des Quellcodes soll *nach* Erreichung der vollständigen Verifizierbarkeit und *nach* der Zertifizierung stattfinden. Die Änderung von Art. 7 VEleS stellt zunächst den Grundsatz klar, wonach für den Einsatz eines vollständig verifizierbaren Systems unabhängig von der beantragten Limite Zertifizierungen erforderlich sind. Sollen jedoch höchstens 30 Prozent des kantonalen Elektorats zu einem Versuch zugelassen werden, kann sich die Zertifizierung auf das System und dessen Betrieb auf Seiten der Systemanbieter beschränken. Die Zertifizierung der kantonalen Prozesse, der Druckerei sowie der Software des Behördenportals ist in dieser Konstellation jedoch nicht erforderlich (vgl. insb. die Einschränkungen gemäss Art. 7 Abs. 3 Bst. b und c VEleS).

Artikel 7a Absatz 1 VEleS

Der Quellcode der Software des Systems muss in gut lesbarer Form offengelegt werden. „Software“ bezeichnet die Umsetzung des kryptografischen Protokolls für die vollständige Verifizierbarkeit auf applikativer Ebene. Damit sind insbesondere die Generierung der kryptografischen Geheimelemente, die Gültigkeitsprüfung, die Registrierung der eingehenden Stimmen, das kryptografische Mischen der registrierten Stimmen, die Entschlüsselung der Stimmen sowie die Erstellung der Beweise, die unter Einsatz der Kontrollkomponenten aus der vollständigen Verifizierbarkeit gemäss Art. 5 VEleS resultieren, betroffen.

Vor der Gesuchstellung der Kantone um die Grundbewilligung müssen interessierte Personen genügend Zeit gehabt haben, um die Unterlagen zu analysieren und ihre

Ergebnisse gegenüber den Behörden sowie gegenüber den Systemanbietern zu unterbreiten.

Artikel 7a Absatz 2 VEleS

Der Quellcode der Systeme soll *nach* Erreichung der vollständigen Verifizierbarkeit und *nach* der Zertifizierung offen gelegt werden. Dieser Zeitpunkt für die Offenlegung wird durch den Verweis auf die Regelung in Art. 7 Abs. 2 und 3 VEleS festgelegt. Die Offenlegung hat das Potential, Fragen in der Öffentlichkeit auszulösen (z.B. Fake news). Mit einer glaubwürdigen Vorprüfung lässt sich erreichen, dass die Chancen der Offenlegung die inhärenten Risiken übersteigen.

Artikel 7a Absatz 3 VEleS

- Buchstabe a: Der Einsatz proprietärer Standardkomponenten (Betriebssysteme, Datenbanken, Webserver, Applikationsserver, Rechteverwaltungssysteme, Firewall, Router) soll auch ohne die Offenlegung von deren Quellcode möglich sein. Dabei ist vorbehalten, dass die Standardkomponente breit zum Einsatz kommt und dementsprechend laufend aufdatiert wird. Zudem muss die Konfiguration der Standardkomponente in der System- und Betriebsdokumentation soweit als relevant für die Vertrauensbildung beschrieben werden.

- Buchstabe b: Der Quellcode eines E-Governmentportals, über das die verschlüsselten Stimmen zum System zur elektronischen Stimmabgabe gelangen, muss nicht offengelegt werden, sofern die für die Erfüllung von Art. 5 VEleS wesentlichen Operationen im System zur elektronischen Stimmabgabe durchgeführt werden.

Artikel 7b Absatz 1 VEleS

Diese Bestimmung regelt, in welcher Art und Weise der Quellcode offenzulegen ist. Dazu wird auf beste Praktiken verwiesen, wie sie beispielweise in Bezug auf die Lesbarkeit und Struktur des Quellcodes oder bezüglich der Möglichkeiten für Rückmeldungen üblich sind:

- Damit der Quellcode von interessierten Personen gelesen und verstanden werden kann, muss er gängigen Kriterien der Lesbarkeit genügen. Diese betreffen unter anderem die Formatierung, die Kommentierung und die Komplexität von einzelnen Code-Abschnitten.

- Die Gesamtstruktur des Codes sollte klar ersichtlich sein. Dazu können zusätzliche Dokumentationen und Illustrationen beitragen.

- Die Offenlegung des Quellcodes hat unter anderem zum Zweck, der Öffentlichkeit Gelegenheit zu geben, Schwächen aufzudecken. Dazu sollte bei der Offenlegung erklärt werden, wie interessierte Personen Rückmeldungen geben können. Indem zeitnah veröffentlicht wird, wie die einzelnen Rückmeldungen verwertet werden, kann das Vertrauen in den Quellcode weiter gefördert werden.

Vote électronique: Offenlegung des Quellcodes, Anpassung der VEleS

Artikel 7b Absatz 2 VEleS

Der Zugriff auf den Quellcode soll für interessierte Personen möglichst ohne Erschwernisse erfolgen. Wer sich entscheidet, den Quellcode aus dem Internet herunterzuladen, soll dies möglichst unmittelbar tun können. Die Erhebung einer Gebühr ist ausgeschlossen (vgl. Art. 86 BPR).

Artikel 7b Absatz 3 VEleS

Nicht alle Aufgaben, die für die Sicherheit eines Systems relevant sind, können auf der Ebene der Software gelöst werden. Der Quellcode allein gibt keinen Aufschluss darüber, in welcher Infrastruktur und unter welchen organisatorischen Sicherheitsvorkehrungen ein System betrieben und gewartet wird. Zur Schaffung von Transparenz, die es Fachkreisen ermöglicht, eine Einschätzung über die Vertrauenswürdigkeit des Systems zu treffen, muss der Quellcode kontextualisiert werden.

Artikel 7b Absatz 4 VEleS

Die Kantone werden nicht zur Publikation der Software unter einer Open Source-Lizenz verpflichtet, da die entsprechenden Kriterien über die Vertrauensbildung hinausgehen. Im Interesse der Vertrauensbildung muss es jedoch bei der Verwendung proprietärer Software möglich sein, den Quellcode der Programme leicht über das Internet zu beziehen und ihn im privaten Bereich zu analysieren. Dies muss die Möglichkeit einschliessen, ihn – wie mit Open Source Software – straffrei verändern, kompilieren und ausführen sowie auf dessen Grundlage wissenschaftlich arbeiten zu dürfen. Die Copyright-Bestimmungen der Urheber müssen dementsprechend ausgestaltet sein. Der Eigner des Quellcodes kann die Nutzung des Quellcodes zu anderen Zwecken, beispielsweise zur Durchführung von Urnengängen, erlauben oder an Bedingungen knüpfen.

Anhang Ziff. 2.7.2

Diese Bestimmung verbietet es, die einzelnen Stimmen aufzubewahren. Gleichzeitig ist die Aufbewahrung der Stimmen bis zum Ablauf der Erwahrungsfrist nötig. Beispielsweise setzt die Prüfung der aus der Erfüllung von Artikel 5 VEleS resultierenden kryptografischen Beweise das Vorliegen der einzelnen Stimmzettel voraus. Die vertrauliche Behandlung der vorgängig anonymisierten Stimmzettel wird bereits durch Ziffer 2.8.6 VEleS Anhang sichergestellt.