Christian Folini
Ringstrasse 2
3629 Kiesen

folini@netnea.com

Melchior Limacher
Schönauring 80
8052 Zürich

melchior@limafast.ch

Bundeskanzlei
Sektion Politische Rechte
Bundeshaus West
3003 Bern

Bern, 26. April 2019

Stellungsnahme zur Änderung des Bundesgesetzes über die politischen Rechte

Sehr geehrter Herr Bundeskanzler

Wir schreiben Ihnen als eine Gruppe von Personen, die sich mit der Sicherheit von Wahlen und Abstimmungen beschäftigen. Unsere Gruppe eint Kritiker und Befürworter der elektronischen Stimmabgabe. Für die Kritiker besteht ein Interesse daran, sicherzustellen, dass die elektronische Stimmabgabe möglichst sicher implementiert wird, wenn sie nicht gestoppt werden kann. Für die Befürworter besteht ein Interesse, die Argumente der Kritiker zu berücksichtigen und die elektronische Stimmabgabe möglichst sicher zu implementieren.

Wir haben den Schlussbericht der Expertengruppe Elektronische Stimmabgabe (EXVE), den erläuternden Bericht der Bundeskanzlei zur Vernehmlassung und die Revisionsvorlage zum Gesetz für die politischen Rechte (E-BPR) am 6. und 7. April in einer Kerngruppe intensiv und systematisch diskutiert. Dabei sind uns einige Punkte aufgefallen, auf die wir Sie gerne aufmerksam machen und die wir unten Artikel für Artikel erläutern.

Eine besondere Wichtigkeit messen wir folgenden Punkten zu:

1. Die durch mehrere Forschergruppen publizierten Schwachstellen des E-Voting Systems der Schweizerischen Post und ihres spanischen Partners Scytl hat die Schwächen des Entwicklungsprozesses der Software und des Zertifizierungsprozesses offengelegt. Die schwerwiegendsten Befunde wurden durch die Publikation des Quellcodes des Systems überhaupt erst ermöglicht. Wir erachten die Unabhängigkeit der Kontrolle und die Transparenz der eingesetzten Systeme deshalb für mindestens genauso wichtig, wenn nicht sogar für wichtiger, als den Zertifizierungsprozess. Diese Erkenntnis hat unsere unten aufgeführten Kommentare zum Gesetzestext wesentlich geleitet. Im Übrigen sind wir überzeugt, dass dieselben Massstäbe für unabhängige Kontrollen und Transparenz auch auf weitere elektronische Hilfsmittel, namentlich die kantonal eingesetzten Ergebnisermittlungsverfahren, anzuwenden sind.

2. Wir halten die statistische Plausibilisierung der Ergebnisse der Auszählungen von elektronisch eingereichten Stimm- und Wahlzettel für sinnvoll. Eine zentrale Form der Plausibilisierung ist der Vergleich mit anderen Stimmkanälen.

3. Bei einer Beeinträchtigung des E-Voting-Systems kann es vorkommen, dass überdurchschnittlich viele Stimmberechtigte an der Urne abstimmen wollen. Darauf müssen die Stimmlokale am Wahl- und Abstimmtag vorbereitet sein. Dies ist eine Herausforderung für die Gemeinden, weil in der Revisionsvorlage zu Recht ein Abgleich der eingehenden Stimmrechtsausweise mit dem Stimmregister vorgesehen ist. Darüber hinaus muss auch verhindert werden, dass Stimmberechtigte ihre Stimme mehrfach abgeben. Ferner ist zu beachten, dass bei einem Ausfall des E-Voting-Systems, je nach Implementierung, nicht nur das elektronische Abstimmen unmöglich wird, sondern auch Auswirkungen auf andere Kanäle hinzukommen können. So kann das System etwa keine Auskunft mehr darüber geben, welche Stimmberechtigten ihre Stimmen bereits elektronisch abgegeben haben. Den Stimmlokalen müssen deshalb rechtzeitig Informationen zur Verfügung gestellt werden, anhand deren sie lokal überprüfen können, ob jemand bereits elektronisch abgestimmt hat.

Es folgen nun Kommentare zu individuellen Gesetzesartikeln des BPR und E-BPR.

Artikel 6

Art. 6 Abs. 1 lit. a E-BPR gilt neu auch für die persönliche Stimmabgabe an der Urne. Dies impliziert in jedem Fall einen Abgleich der abgegebenen Stimmen mit dem Stimmregister, was bislang nicht der Fall ist. Wir begrüssen diese Neuerung.

Art. 6 Abs. 1 lit. d E-BPR erfordert ein Abgleich der brieflichen und der an der Urne abgegebenen Stimmen mit den vorgängig elektronisch eingegangenen Stimmen. DDoS Angriffe auf das elektronische Wahlsystem gefährden diesen Abgleich, namentlich im Hinblick auf Art. 8e Abs 1 lit b E-BPR, wo im Fall einer Beeinträchtigung des E-Voting Systems mit einer unerwartet hohen Zahl von Stimmberechtigten an der Wahlurne gerechnet werden muss. Diesem Schwachpunkt muss begegnet werden. Dies kann etwa dadurch erreicht werden, dass die Gemeinden bereits am Vorabend nach dem Schluss der elektronischen Wahlurne mit einem Export der Listen versorgt werden, anstatt am Wahl- und Abstimmungstag direkt auf das E-Voting-System zuzugreifen.

Art. 6 Abs. 2 E-BPR ermöglicht unter Umständen die Ableitung eines Rechtsanspruches auf barrierefreies Wählen und Abstimmen via den elektronischen Kanal. Dies ergibt sich unseres Erachtens im Zusammenspiel mit Art. 6 Abs. 1 lit b E-BPR (Stimmgeheimnis). Allerdings steht dieses im Widerspruch zu den Aussagen im erläuternden Bericht zur Vernehmlassung, der einen solchen neuen Rechtsanspruch verneint.

Artikel 7

Art. 7 Abs. 1 E-BPR und Art. 8e Abs. 1 lit. b E-BPR definieren die persönliche Stimmabgabe an der Urne in jedem Fall als gewährleistet, namentlich im Fall eines Systemausfalls der brieflichen oder elektronischen Stimmabgabe. Die Kantone müssen deshalb darum besorgt sein, dass die nötigen Kapazitäten vorsorglich bereit gestellt werden. Dies namentlich im Hinblick auf eine mögliche zukünftige Volldigitalisierung. Art. 7 Abs. 1 E-BPR ist deshalb dahingehend zu erweitern, dass die Kantone darum besorgt sein müssen, die entsprechenden Kapazitäten vorzuhalten. Diese Herausforderung wird bei der vollständigen Dematerialisierung der elektronischen Stimmabgabe zusätzlich vergrössert.

Artikel 8a

Art. 8a Abs. 1 E-BPR verlangt eine Bewilligung durch den Bundesrat. Wir erachten diese Bewilligung als sinnvolle Ergänzung zur Transparenz der eingesetzten Systeme. Wir sehen aber, dass das Bewilligungsverfahren zu einer hohen Markteintrittshürde und damit zur Monopolbildung eines Systemanbieters beiträgt. Zu einem späteren Zeitpunkt könnte es deshalb sinnvoll sein, dieses Bewilligungsverfahren aufzuheben.

Artikel 8b

Art. 8b Abs. 2 E-BPR nennt das Stimmgeheimnis nicht, während es in Art. 8b Abs. 3 E-BPR ausdrücklich genannt wird. Uns ist unklar weshalb das Stimmgeheimnis in einem Absatz aber nicht im anderen erwähnt wird.

Art. 8b Abs. 2 E-BPR erwähnt kryptografische Beweise nicht, während sie in Art. 8b Abs. 3 E-BPR ausdrücklich stipuliert werden. Uns ist unklar, weshalb die Beweise in einem Absatz ausdrücklich kryptographischer Natur sein müssen, nicht aber im anderen.

Art. 8b Abs. 2 E-BPR umreisst die Unabhängigkeit der Komponenten zu wenig genau. Der Artikel ist in diesem Punkt zu präzisieren. Als wünschenswert erachten wir eine weitestmögliche Unabhängigkeit der Komponenten, die deutlich weiter geht als die gegenwärtigen in der VEleS formulierten Anforderungen (verschiedene Programmiersprachen, verschiedene Hersteller/Entwickler, verschiedene Technologie-Stacks). Ebenfalls wünschenswert wäre es, wenn Interessierte eigene, separat geprüfte und bewilligte Kontrollkomponenten beitragen und betreiben könnten.

Art. 8b Abs. 3 E-BPR sieht nicht explizit vor, dass Interessierte eigene "Verifier" zur Verfügung stellen können, welche von den Kantonen zusätzlich eingesetzt werden sollen. Der Artikel ist dahingehend zu ergänzen, dass dies sichergestellt ist.

Art. 8b E-BPR ist ferner um einen eigenen Absatz zu ergänzen, dass das Aufsetzen der Wahl und die Generierung der Schlüssel auf mehrere unabhängige Komponenten verteilt werden muss. Auch hier ist vorzusehen, dass Interessierte eigene, separat geprüfte und bewilligte Komponenten beisteuern können.

Artikel 8c

Art. 8c E-BPR umreisst die wesentlichen Anforderungen an die Öffentlichkeit der Informationen und des Betriebs. Dabei wird spezifiziert, was offengelegt werden muss (namentlich der Quellcode sowie die wesentlichen betrieblichen Abläufe). Dies brachte bis dato nicht das gewünschte Mass an Transparenz; namentlich in Bezug auf die Prüfberichte der KPMG oder die Dokumentation des Quellcodes. Ziel ist es, die Entwicklung der Software und die Konfigurationen des Systems nachvollziehen zu können. Darüber hinaus ist die Publikation der Dokumentation sowie sämtlicher Prüfberichte wünschenswert, so dass die Systeme für Forschungszwecke und zur Prüfung so weit wie möglich reproduziert werden können. Der Artikel ist dahingehend umzuformulieren, dass sämtliche Informationen offenzulegen sind, ausser wenn wesentliche Gründe dagegen sprechen.

Artikel 8d

Art. 8d E-BPR beschreibt die Voraussetzungen zur Bewilligung der elektronischen Stimmabgabe. Die Transparenz und die Offenlegung des Quellcodes etc. sind nicht explizit genannt, sollten aber als Teil der Zertifizierung überprüft werden. Dabei ist der Nachweis zu erbringen, dass Anreize gemäss besten Praktiken geschaffen wurden, um die interessierte Öffentlichkeit bei der (Weiter-)Entwicklung eines sicheren Systems einzubeziehen (Bug Bounty, Source Code Community, universitäre Auseinandersetzung mit den Abstimmungsprotokollen, etc.)

Artikel 8e

Art. 8e Abs. 1 lit. b E-BPR impliziert eine Beweislast auf Seiten des Stimmberechtigten. Dies widerspricht dem erläuternden Bericht zur Vernehmlassung, der einen Wechsel des Stimmkanals ohne Angabe von Gründen auch für Stimmberechtigte vorsieht, die sich für die elektronische Stimmabgabe angemeldet haben. Der Nachsatz "wenn die elektronische Stimmabgabe nicht möglich ist" ist zu streichen.

Art. 8e Abs. 1 lit. b E-BPR erlaubt es, DDoS Angriffe auf das elektronische Wahlsystem dadurch aufzufangen, dass die Stimmberechtigten am Wahl- und Abstimmungstag persönlich an der Urne abstimmen. Für Stimmberechtigte, die sich für die dematerialisierte Stimmabgabe angemeldet haben, führt dies dazu, dass ad-hoc physikalisches Stimmmaterial erzeugt werden muss. Die entsprechenden Kapazitäten sind in Art. 7 Abs. 1 vorzusehen. Ferner ist sicherzustellen, dass die Stimmberechtigung und die Einmaligkeit der Stimmabgabe lokal auf jeden Fall bei der Stimmabgabe geprüft werden kann (auch bei einem Ausfall des E-Voting Systems). Dies kann etwa dadurch erreicht werden, dass die Gemeinden bereits am Vorabend (nach dem Schluss der elektronischen Wahlurne) mit einem Export der Listen versorgt werden, anstatt am Wahl- und Abstimmungstag direkt auf das E-Voting System zuzugreifen.

Art. 8e Abs. 2 E-BPR gibt dem Bundesrat das Recht zur Einführung der vollständigen Dematerialisierung. Wir halten dies für deutlich verfrüht. Stattdessen soll dem Bundesrat

die Kompetenz eingeräumt werden, mit der vollständigen Dematerialisierung im beschränkten Rahmen Versuche durchzuführen.

Artikel 14

Art. 14 BPR wird in der Revisionsvorlage nicht erwähnt. Art. 14 Abs. 3 BPR fordert die Vernichtung der Stimmzettel nach der Erwahrung des Abstimmungsergebnisses. Es ist unklar, inwieweit sich das auch auf die elektronische Stimmabgabe bezieht und welche Daten davon betroffen sind. Der Artikel ist zu präzisieren.

Artikel 47

Art. 47 Abs. 1ter E-BPR setzt für die Eintragung der Kandidaten auf dem elektronischen Wahlkanal die Veröffentlichung gemäss Art. 47 Abs. 1bis BPR voraus. Im Falle der Veröffentlichung gemäss Art. 47 Abs. 1bis BPR ist die Eintragung auf dem elektronischen Wahlkanal aber nur fakultativ. Sie sollte in diesem Fall zwingend sein.

Artikel 84

Art. 84 Abs. 1 BPR wird in der Revisionsvorlage nicht erwähnt. Art. 84 Abs. 1 BPR erlaubt es dem Bundesrat die Regelung des E-BPR zur elektronischen Stimmabgabe im Umfang einzuschränken oder ausser Kraft zu setzen. Dieser Artikel ist zu streichen oder im Umfang einzuschränken.

Art. 84 Abs. 2 E-BPR nennt neben den Wahl- und Abstimmungsverfahren die Ergebnisermittlungsverfahren nicht explizit. Sie sind zu ergänzen, um die verschiedenen kantonalen, elektronischen Ergebnisermittlungsverfahren der Regulierung zu unterstellen. Es ist technisch nicht begründbar, weshalb der Bundesrat sicherheitstechnische Vorgaben für den elektronischen Stimmkanal erlassen muss, während die elektronischen Ergebnisermittlungsverfahren anderer Stimmkanäle nicht reguliert werden. Die Regulierung dieser Verfahren sollte sich an den Massstäben des elektronischen Stimmkanals orientieren, insbesondere, was die Transparenzanforderungen betrifft. Der erläuternde Bericht weist darauf hin, dass der Bundesrat sich bei der Regulierung auf diejenigen Systeme beschränken will, welche für die Gewährleistung der Vertrauenswürdigkeit zentral sind und eine besondere Sorgfaltspflicht erfordern. Unserer Ansicht nach fallen die elektronischen Ergebnisermittlungsverfahren in diese Gruppe und wir halten eine Regulierung deshalb für angezeigt.

Art. 84 Abs. 3 E-BPR fordert die Plausibilisierung der elektronisch eingegangenen Stimmen. Diese Plausibilisierung ist auf sämtliche Stimmkanäle auszudehnen und es ist darauf zu achten, dass die Plausibilisierung auch zwischen den Kanälen erfolgt. Dies schliesst die Plausibilisierung der brieflichen Stimmabgabe gegenüber der Stimmabgabe an der Urne explizit ein. Die Plausibilisierung hat nach mathematisch statistischen besten Praktiken zu erfolgen. Die Plausibilisierung der beiden konventionellen Stimmkanäle gegeneinander macht nur dann Sinn, solange genügend

Stimmberechtigte ihre Stimme an der Urne abgeben. Es ist deshalb zu überlegen, inwieweit die Stimmabgabe an der Urne zu fördern wäre.

Wir danken Ihnen für die Gelegenheit zur Stellungnahme und die Berücksichtigung unserer Kommentare. Gerne stehen Christian Folini und Melchior Limacher für Fragen zur Verfügung.

Mit freundlichen Grüssen

Umberto Annino, ISSS - Information Security Society Switzerland, Präsident
Aarno Aukia, VSHN AG
Dr. Christian Folini, netnea AG
Dr. Stefan Frei, Department of Computer Science, ETH Zürich
Christian Killer, Communication Systems Group Universität Zürich
Stefan Koring, Schweizerische Post AG
Melchior Limacher, Limacher Informationssicherheit GmbH
Simon Monai, Baumer Group
Dr. Stephan Neuhaus, School of Engineering ZHAW
Dr. Raphael Reischuk, Zühlke Group
Prof. Dr. Burkhard Stiller, Communication Systems Group Universtität Zürich
Simon Studer, netnea AG
Prof. Dr. Bernhard Tellenbach, School of Engineering ZHAW

Die Namen der Mitglieder der Kerngruppe sind fett gesetzt.