piratenpartei
www.piratenpartei.ch

Piratenpartei Schweiz, 3000 Bern

Vernehmlassungsantwort zur Änderung des Bundesgesetzes über die politischen Rechte (Überführung der elektronischen Stimmabgabe in den ordentlichen Betrieb)

Sehr geehrter Herr Bundeskanzler Thurnherr
Sehr geehrte Damen und Herren

Obschon sich die Piratenpartei bekanntlich bei der elektronischen Stimmabgabe, den bisherigen Vernehmlassungen (z.B. bei der Revision der Verordnung über die politischen Rechte (VPR) im 2013) und den laufenden Tests des E-Votings wiederholt stark engagiert hat, wurden wir von Ihnen zur dieser Vernehmlassung leider nicht offiziell eingeladen. Bezugnehmend auf Ihre Vernehmlassungseröffnung vom 19. Dezember 2018 nehmen wir dennoch gerne Stellung und würden es zukünftig sehr begrüssen, wenn wir in Ihre Adressatenliste aufgenommen werden.

Gerne platzieren wir hiermit auch noch einen Hinweis: Wir finden es sehr bedenklich, dass Sie für die Stellungnahme auch ein proprietäres Dateiformat verlangen (Word der Firma Microsoft), wo es doch heute zahlreiche offene und freie Dokumenten-Formate gibt. Dennoch entsprechen wir Ihrem Wunsch.

Grundsätzliches

Die Piratenpartei Schweiz setzt sich seit Jahren für eine humanistische, liberale und progressive Gesellschaft ein. Dazu gehören auch die Privasphäre der Bürger sowie die Transparenz des Staatswesens, inklusive Abbau der Bürokratie und Open Government Data, den Diskurs zwischen Bürgern und Behörden, aber auch die Abwicklung alltäglicher Geschäfte. Jede neue digitale Schnittstelle und Applikation bedingt aber eine umfassende Risikoanalyse und Folgeabschätzung.

Im Grundsatz widerspricht eine limitierte elektronische Stimmabgabe diesen Grundsätzen nicht, doch die vom Bund vorangetriebenen Grundlagen, insbesondere die Verordnungen und die diversen Umsetzungsversuche durch private und staatliche Akteure waren und sind dermassen ungenügend, dass die Piratenpartei einen sofortigen Übungsabbruch fordert. **Die elektronische Stimmabgabe, wie sie heute im "Versuchsbetrieb" von der Bundeskanzlei bewilligt wird, muss eingestellt werden und die entsprechenden Verordnungen sind aufzuheben.**

Erfahrungen und Versuchsbetrieb

Gerne erinnern wir an einige Erfahrungen und Eckdaten aus dem bisherigen Versuchsbetrieb mit der elektronischen Stimmabgabe:

- Seit 2002 gibt es gesetzliche Grundlagen für Versuche mit der elektronischen Stimmabgabe. Bis heute wurde von der Bundeskanzlei teilweise eine Bewilligung für einen **"Versuchsbetrieb" mit bis zu 50 Prozent** der Stimmbürger gegeben und die Ausweitung auf 100 Prozent der Stimmbürger für dieses Jahr in Aussicht gestellt.
  Das Ausmass von Tests wurde auf Gesetzesebene nie exakt definiert sondern nur als **«zeitlich, sachlich und örtlich begrenzt»** (siehe Bundesgesetz über die politischen Rechte BPR, SR 161.1).
  Die Ausweitung der Versuche (Verordnung über die politischen Rechte VPR; SR 161.11) auf 30, 50 und 100 Prozent des Elektorates **widerspricht unseres Erachtens klar dem Gesetz**.
- Von Experten und Kryptologen gibt es Konzepte für sicher geltende E-Voting-Lösungen. Diese Konzepte werden aber immer noch laufend überarbeitet. Eine Umsetzung in Code, Systeme und den produktiven Betrieb ist im Vergleich dazu eine unglaublich komplexe Aufgabe. Praktisch alle Entwickler sind bis heute daran gescheitert. Zusätzlich sind viele Teil-Prozesse von diesen kryptologischen Konzepten ausgenommen, wie z.B. das sichere Handling und der Druck von Codes.
- Bereits im 2009 warnte die Berner Fachhochschule vor Manipulationen in den bestehenden E-Voting-Systemen, durch interne oder externe Akteure. Der massenhafte **digitalen Stimmenkauf**, die **unzähligen Angriffsvektoren** auf die E-Voting-Systeme und -Schlüsselpersonen sowie die **intransparenten Systeme und Prozesse** waren Dauerkritikpunkte von allen unabhängigen Experten.
- Im Juli 2013 wurde bei der CHVote Lösung der Kantone Genf, Bern, Luzern und Basel-Stadt von einem Informatiker eine **schwerwiegende Sicherheitslücke** festgestellt. Im Anschluss daran wurde der Code der Genfer CHVote Lösung im 2015 dank der Expertise und der engen Zusammenarbeit mit der BFH und der Piratenpartei vorbildlich unter einer quelloffenen Lizenz publiziert.
  Leider wurde diese öffentliche Publikation seit einiger Zeit nicht mehr aktualisiert, aus uns unerklärlichen Gründen.
- Im 2015 wurde dem grössten E-Voting-Anbieter, dem «Consortium Vote électronique» die Bewilligung nicht mehr erteilt, da dieses System den Schutz des **Stimmgeheimnisses nicht gewährleisten** konnte. In 9 Kantonen wurde dieses "hackbare" System vorgängig bereits mehrfach im Testbetrieb eingesetzt. Da dieser Fehler nur schwer zu beheben war, wurde als Folge davon der Betrieb dieses Systems komplett eingestellt.
- Im 2018 wurde durch diverse simple Demo-"Hacks" präsentiert, wie das Stimmgeheimnis der zwei verbliebenen E-Voting-Systeme auf den unsicheren Endgeräten ausgehebelt oder über sogenannte MITM-Attacken die **Stimmabgabe sogar manipuliert** werden könnte.

- Die Berner Fachhochschule entwickelt seit mehreren Jahren eine Spezifikation für ein zumindest theoretisch kryptologisch sicheres System. Doch auch solche rein theoretischen Grundlagen werden häufiger überarbeitet, als wir Abstimmungstermine in der Schweiz haben.
- Diese Spezifikationen der BFH sollten die Basis bilden für die neue Version der Genfer CHVote-Systems, welches aber **nicht mehr weiterentwickelt** wird. Die technische Umsetzung des zumindest theoretisch sicheren Konzepts scheint also auch für den Kanton Genf ein Ding der Unmöglichkeit. Der Betrieb des alten CHVote Systems wird in einigen Monaten ebenso eingestellt.
- In der Zwischenzeit wird ein von einer ausländischen Firma entwickeltes System, welches durch die Schweizerische Post an die Kantone verkauft wird, als einziges übrig bleibendes E-Voting System gehandelt. In Ihrem Bericht schreibt die Bundeskanzlei kein einziges Mal den Namen des Spanischen Lieferanten Scytl, und auch die Post verschweigt diese Abhängigkeit möglichst immer, ausser bei Schuldzuweisungen. Durch bekanntgewordene Fehler im Code wurde bekannt, dass die Post sogar einfachste Code-Korrekturen vom Lieferanten erledigen lässt, also selbst keinerlei Möglichkeiten hat, das System zu kontrollieren und korrigieren.
- Mit starkem politischen Lobbying der Post und der Positionierung ihres E-Voting-Produkts als "für Geschäftskunden" konnte die Post in den letzten Jahren viele Kantone gewinnen. Die Website und der Blog sprechen eine deutliche kommerziell orientierte Marketing-Sprache. Auf technische Probleme oder Risiken wird kaum eingegangen und Grundlagen wie z.B. die Zertifizierungsunterlagen, Prozesse oder technischen Details der E-Voting-Umsetzung werden nicht oder nur sehr zögerlich publiziert. Das Sicherheitskonzept der Post besteht also primär aus "**security by obscurity**", was bei einem für die Demokratie essentiellem System inakzeptabel ist. Die Post als Staatsbetrieb ist gleichzeitig der Hauptprofiteur vom Versand der Stimm- und Wahl-Unterlagen und das schwindende Briefversands-Geschäft soll nun offensichtlich mit einem neuen Geschäftsbereich aufgefangen werden.
- Aufgrund einer nicht eingesehenen und im Detail überprüften Zertifizierung der privaten Firma KPMG hat die Bundeskanzlei diesem System der Post bereits eine Freigabe für bis zu 50 Prozent des Elektorats erteilt. Zur Ausweitung auf 100 Prozent des Elektorats musste die Post den Code offenlegen. Diese "Offenlegung" geschah im Februar 2019 und sollte gemäss VEleS Art. 7 nach besten Praktiken aufbereitet und dokumentiert sein: Das System und dessen Betrieb müssen dokumentiert sein, jeder und jede sollte den Quellcode zu ideellen Zwecken untersuchen, verändern, kompilieren und ausführen sowie dazu Studien verfassen und diese publizieren können. Doch die Post knüpfte den Zugang zum Code an inakzeptable Nutzungsbedingungen und Geheimhaltungserklärungen und erfand dazu eine neue, sehr einseitige Lizenzform.

- Bei dem im Anschluss durchgeführte Public-Intrusion-Test (PIT) wurden zahlreiche Angriffsvektoren von Beginn an verboten. Zahlreiche Personen und Firmen haben diese Konditionen nicht akzeptiert und aus Kreisen von Sicherheitsexperten bestand Konsens:
  Diese eingeschränkte Offenlegung und der PIT ist eine reine Marketingaktion der Post.
- Die ersten Meldungen von wichtigen Sicherheitslücken der Post-E-Votings wurden relativ schnell publik, da sie **"unerlaubte" Angriffsvektoren** betrafen und somit nicht der Geheimhaltung unterlagen. Sehr schnell wurde auch über **mangelnde Codequalität** und **fehlende Dokumentation** debattiert und nach einigen Tagen wurde der verfügbare Code "befreit". Das bedeutet, irgend Jemand hat ihn öffentlich zugänglich gemacht, also indirekt die VEleS Art. 7 Bedingungen erfüllt.
- Nun hagelte es auch öffentlich Kritik am System: Die unabhängige kanadische Sicherheitsforscherin Sarah Jamie Lewis schrieb, der Code sei **unnötig komplex und unübersichtlich** und somit **stark fehleranfällig**. Matthew Green, ein renommierter Professor für Kryptografie erklärte, dass dieser Code nicht "best practices" der Software-Entwicklung entspricht und kaum seriös auditiert werden kann. Und die Post wiegelte ab und erklärte der Welt in Communiquées und auf Social Media, dass solche Leute Vieles nicht richtig begriffen hätten.
- Innert kürzester Zeit wurde jedoch dank diesen externen, nicht am Post-PIT teilnehmenden Experten, eine erste **gravierende Sicherheitslücke** öffentlich bekannt: Der Kern der neuen Entwicklung, die sogenannte universelle Verifizierbarkeit, konnte **unbemerkt manipuliert** werden. Die Sicherheitslücke war der Post scheinbar seit 2017 bekannt, wurde aber seither nicht behoben. Ein Qualitätsmanagement bei den verantwortlichen Firmen war also inexistent.
- Keine zwei Wochen später wurde die nächste grosse Sicherheitslücke im Post-E-Voting bekannt, welche auch das bereits im Betrieb stehende System betraf: Die sogenannte **individuelle Verifizierbarkeit wurde kryptografisch gebrochen**.
- Damit wurde von unabhängigen Experten ohne finanzielle Interessen innert weniger Tage die **vollständige Verifizierbarkeit als Farce** entlarvt. Kurz darauf erklärte die Post, ihr System stehe für die kommende Abstimmung nicht zur Verfügung.

Erkenntnisse

Die Geschichte des Schweizer E-Votings zeigt exemplarisch, **dass eine sichere, vertrauenswürdige und nachvollziehbare elektronische Stimmabgabe heute immer noch eine Illusion ist**.

In allen aufgelisteten Vorfällen redeten die betroffenen Firmen oder Behörden die Probleme klein. Unabhängige und externe Expertisen werden systematisch schlechtgeredet und als irrelevant abgekanzelt. In zahlreichen Fällen wurden Hacker oder Überbringer der schlechten Botschaften persönlich oder sogar juristisch angegangen oder ein Maulkorb verhängt. Diese ganze Entwicklung war absolut **nicht vertrauensfördernd**.

Gleichzeitig wurde und wird von Lieferanten, Kantonen und auch von der Bundeskanzlei immer noch Schönfärberei betrieben: Es wird von "sicheren Systemen" geredet, von mehreren hundert erfolgreichen E-Voting-Versuchen und von zuverlässigen professionellen Zertifizierungen. Eine Expertengruppe (EXVE), die unseres Erachtens **absolut nicht repräsentativ** ist, erklärt nun gemäss Bericht der Bundeskanzlei, dass der elektronische Stimmkanal dank der vollständigen Verifizierbarkeit sicher und vertrauenswürdig angeboten werden kann.

Tatsache ist aber, **dass**

- **die individuelle und die universelle Verifizierbarkeit des elektronischen Wahl- und Abstimmungsprozesses bis heute nicht funktionieren,**
- **die Wahrung des Stimmgeheimnisses wegen unsicheren Geräten und Software nicht garantiert werden kann, insbesondere wenn auf Code-Voting verzichtet wird,**
- **keinerlei Transparenz der Systeme für die elektronische Stimmabgabe und der betrieblichen Abläufe herrscht,**
- **die Zertifizierung der Systeme für die elektronische Stimmabgabe nicht funktioniert und intransparent ist,**
- **kaum ein Bürger die wesentlichen Schritte der elektronischen Stimmabgabe verstehen oder überprüfen kann,**
- **keine Gewissheit besteht, dass die Stimmen korrekt gezählt werden, wie sie gemäss dem freien und wirklichen Willen der Stimmberechtigten entsprechen und**
- **keine Teilergebnisse der elektronischen Stimmabgabe eindeutig und unverfälscht ermittelt sowie nötigenfalls in Nachzählungen ohne besondere Sachkenntnis zuverlässig überprüft werden können.**

Diesbezüglich ist ebenso zu beachten, dass

- sich dank Schweizer Gesetzen wie BÜPF und NDG und internationalen nachrichtendienstlichen Aktivitäten die Sicherheit von Geräten und Netzwerken aufgrund von geheimgehaltenen Sicherheitslücken zunehmend verschlechtert,
- die Datenübertragung von Anbietern oder staatlichen Akteuren systematisch infiltriert wird,
- wegen Un-Sicherheitskonzepten bei Infrastrukturprojekten viele Behörden, fast alle Schulen und zahlreiche Firmen die Verschlüsselungstechniken mittels HTTPS-Inspection aushebeln um den Internetverkehr zu lenken und zu filtern, somit also die für die elektronische Stimmabgabe notwendige verschlüsselte Kommunikation zunehmend unterwandert wird,
- insbesondere die Endgeräte und Netzwerke von Auslandschweizern in zahlreichen Ländern bei der elektronischen Stimmabgabe von Überwachungen und Manipulationen betroffen sind,
- der Zusatznutzen des elektronischen Stimmkanals bezüglich Wahlbeteiligung marginal wenn nicht sogar irrelevant ist,
- Manipulationen stark skalierbar sind aber kaum erkannt werden können,
- die Post in der heutigen Anbieterlandschaft bereits eine Quasi-Monopolartige Stellung inne hat, und mit dem Druck von Stimmunterlagen, dem Versand und der ganzen Umsetzung einer elektronischen Stimmabgabe eine inakzeptable Machtposition erlangt und
- dass bei individueller oder universeller Manipulation der elektronischen Stimmabgabe die Suppe für alle Bürger, also auch die konventionell stimmenden, irreversibel versalzen wird und das Vertrauen in den gesamten demokratischen Prozess zerstört wird.

Organisatorisches

Heute werden die Verantwortlichkeiten beim E-Voting zwischen Bund, Kantonen und Lieferanten auf eine inakzeptable Art und Weise umher geschoben: Verantwortlich für die Abstimmungen und Wahlen, also auch für E-Voting-Systeme, sind eigentlich die Kantone. Da sie bezüglich elektronischer Stimmabgabe aber keine Expertise oder Ressourcen haben, verweisen sie bezüglich der Sicherheit immer auf die Bundeskanzlei, welche Vorgaben macht, die Systeme zertifiziert und die Bewilligungen erteilt.

Gleichzeitig werden in den Kantonen die Code-Generierung, das Handling, der Druck und die Auszählung der elektronischen Stimmen an externe Akteure übergeben, so dass der gesamte Abstimmungsprozess somit verwaltungstechnisch outgesourced wird.

Und beispielsweise bei der Zertifizierung des Post-Systems haben für die Bewilligung weder die Bundeskanzlei noch die Kantone das nachgewiesenermassen unbrauchbare Zertifikat der Firma KPMG hinterfragt, die Dokumente eingesehen oder die Sicherheit der E-Voting-Lösung selbst überprüft.

E-Voting-Systeme müssen aber auch in die bestehende Infrastruktur der Kantone eingebunden werden und bereits hier zeigen sich bereits zahlreiche Fehlerquellen: Es gibt Vorfälle, wo Bürger gleichzeitig über die konventionellen Stimmkanäle sowie elektronisch abstimmen konnten. Diese Probleme bestehen auch bei Wohnortwechseln, aber in viel kleinerem Ausmass. Viele Kantone, Gemeinden oder Verwaltungseinheiten machen heute keinen Abgleich der Stimmausweise mit dem Stimmregister. Einige Gemeinden und Kantone delegieren viele Aufgaben an Dritte und machen somit aus der Stimmabgabe oder -zählung einen simplen Verwaltungsakt. Auch bei der konventionellen Stimmabgabe an der Urne oder bei der brieflichen Stimmabgabe gibt es also heute ein grosses Verbesserungspotential.

Alle diese organisatorischen Unzulänglichkeiten müssen unseres Erachtens vor einer Neu-Evaluation und einer Einführung der elektronischen Stimmabgabe bereinigt und massiv verbessert werden.

Schlussfolgerungen

Die elektronische Stimmabgabe respektive der Versuchsbetrieb des Bundes und der Kantone muss sofort eingestellt werden und die entsprechenden Verordnungen sind diesbezüglich anzupassen respektive aufzuheben. Es sollen keine Versuchsbetriebe mit einer nationalen gesetzlichen Grundlage erlaubt werden, bis Anbieter offene und transparente E-Voting Systeme vorzeigen, die sich ausserhalb des politischen Einsatzes bereits umfassend bewährt haben.

Das Bundesgesetz über die politischen Rechte sowie die diesbezüglichen Verordnungen müssen aber angepasst werden, so dass

- Abgleiche mit den Stimmregistern vorgeschrieben werden,
- automatisierte Stimmzählungen umfassend geprüft und plausibilisiert werden,
- alle technischen Hilfsmittel bei Wahlen und Abstimmungen, insbesondere Computer und Software, sicherheitstechnischen Minimalstandards entsprechen,
- dabei immer auf freie und offene Standards gesetzt wird, so dass Quellcode, Systeme und Prozesse der Wahlen und Abstimmungen komplett offengelegt werden und durch Bürger überprüft werden können,
- Verträge mit Dritten offengelegt werden,
- jede Unregelmässigkeit und Fehler umgehend öffentlich protokolliert werden und die Verwendung von betroffenen Systemen oder Prozessen bis zu einer unabhängigen und öffentlichen Überprüfung vermieden wird und
- die Mitarbeitenden von Behörden und Verwaltung ausreichend geschult werden, um mit den technischen Hilfsmitteln und Sicherheitsprotokollen transparente und zuverlässige Ausmittlungen vornehmen zu können.

Kommentare zu einzelnen Artikeln

Hinweis: Sofern wir auf Anmerkungen zu einzelnen Regelungen verzichten, ist damit ausdrücklich keine Zustimmung der Piratenpartei verbunden!

- **Art. 5, Art. 8, Art. 12, Art. 38, Art. 47, Art. 49 et al.:** Alles bezüglich «elektronischer Stimmabgabe» ist zu streichen.
- **Art. 84:** Anforderungen bezüglich sicherheitstechnischen Minimalstandards, anerkannter freier und offener Hard- und Software sowie die umfassende Offenlegung bezüglich verwendeter Quellcodes, Systeme, Prozesse und Verträge mit Dritten müssen bereits auf Gesetzesstufe vorgeschrieben werden. Gerne helfen wir hier aktiv mit an der Ausarbeitung eines entsprechenden Artikels.

Im Weiteren sind alle Verordnungen bezüglich «elektronischer Stimmabgabe» aufzuheben.

Wir danken für die Kenntnisnahme Berücksichtigung unserer Stellungnahme.

———

Piratenpartei Schweiz, Arbeitsgruppe E-Voting, 30. März 2019