Chaos Computer Club Schweiz CCC-CH
Birsfelderstrasse 6
4132 Muttenz
E-Mail: vorstand@ccc-ch.ch
URL: https://www.ccc-ch.ch/

Chaos Computer Club Schweiz CCC-CH, Birsfelderstrasse 6, 4132 Muttenz

Schweizerische Bundeskanzlei BK
Z. Hd. Beat Kuoni
Bundeshaus West
3003 Bern
E-Mail: beat.kuoni@bk.admin.ch

30. April 2019

Vernehmlassungsantwort E-BPR: E-Voting ist ein Hochrisikoprojekt

Liebe Damen
Liebe Herren

Der Chaos Computer Club Schweiz (kurz: CCC-CH) ist Teil der (inter-)galaktischen Gemeinschaft von Lebewesen, die sich vertieft mit Computertechnik und ihren gesellschaftlichen Implikationen befassen.

Im Rahmen von Technikfolgenabschätzungen weist der CCC-CH auf Chancen und Gefahren datenverarbeitender Technologien hin und propagiert andernfalls den schöpferischen und verantwortungsbewussten Umgang mit Technologie (vgl. CCC-Hackerethik[1]). Gegründet wurde der CCC-CH 2012. Er besteht aus neun Verbandsmitgliedern – die meisten davon Hackerspaces mit regelmässigen, öffentlichen Treffen für alle Interessierten.

Uns schliessen sich Menschen an, die kompromisslos freiheitsliebend sind und die auch weiterhin in einer freiheitlichen Gesellschaft leben möchten. Für eine Gesellschaft auf

[1] `https://www.ccc.de/hackerethik` (Abruf: 30.4.2019)

freiheitlich-demokratischer Grundlage, die nicht nur nach der Mehrheitsregel Macht verteilt, sondern auch auf (unterliegende) Minderheiten Rücksicht nimmt, ist es unabdingbar, dass nicht nur die GewinnerInnen, sondern auch die VerlierInnen von den Ergebnissen von Abstimmungen und Wahlen überzeugt sind. Das ist insbesondere dafür wichtig, dass *einerseits* nur *legitime Vertretungen* in den repräsentativ-demokratischen Organen Einsitz nehmen und dass *andererseits* auch bei emotionsgeladenen Sachfragen, wo StimmbürgerInnen Selbstvertretung üben, die *befriedende Funktion* der Abstimmungsdemokratie erhalten bleibt. Diese Funktion sehen wir mit der weiteren Verbreitung der *elektronischen Stimmabgabe* (auch: E-Voting) als eklatant gefährdet an.

Entsprechend:

Der CCC-CH lehnt die Etablierung von E-Voting als ordentlichen dritten Stimmkanal resolut ab.

Im Folgenden begründen wir unsere ablehnende Haltung – sowohl in genereller als auch spezieller Hinsicht. Wir tun dies auf Basis der konkret vorgeschlagenen gesetzlichen Grundlagen und einigen externen Ressourcen, die in Fussnoten verlinkt werden.

Kritik am Revisionsentwurf E-BPR

Änderungsvorschläge an den konkreten Artikeln sind dann von Interesse, sofern die eidgenössischen Räte auf die Vorlage überhaupt eintreten. Sie können auch dann von Belang sein, wenn auf das Bundesgesetz über die Politischen Rechte (BPR) insofern eingetreten wird, als dass es darum geht, die bereits existierende Papierwahl zu stärken.

Tatsächlich würdigen wir in dem Kontext auch einige der vorgeschlagenen Änderungen und liefern hierfür konstruktive Anregungen. So z. B. für das Recht der AuslandschweizerInnen ihr Stimmrecht *im Ausland* ausüben zu können; aber auch punkto zwingenden Massnahmen zur statistischen Kontrolle von Abstimmungs- und Wahlzetteln, die primär elektronisch unterstützt – mit sogenanntem *E-Counting* – ausgezählt werden.

Art. 5: Grundsätze der Stimmabgabe

Wir fordern die Streichung der Möglichkeit, die Stimme elektronisch abzugeben. Dies

gilt sowohl für die aktuelle, seit 2004 im praktischen "Versuchsbetrieb"[2] befindliche, Form des *Internet-Voting* (kurz: I-Voting) als *Web-Voting*, bei dem BürgerInnen mit beliebigen und eigenen Geräten auf zentralisierten Webseiten ihre Stimme abgeben, als auch für Formen der *elektronischen Stimmabgabe*, die sich stärker lokalisiert abspielen – namentlich den z. B. in Brasilien oder den USA weitverbreiteten *Wahlmaschinen* (auch: *Wahlcomputer*).

Web-Voting mit skalierbaren und ungelösten Angriffsmöglichkeiten

Der CCC-CH hat ab Mitte 2018 begonnen, auf skalierbare Angriffsrisiken aufmerksam zu machen, die mit dem Umstand zusammenhängen, dass die Schweiz ihre E-Voting-Systeme auf unsichere Endgeräte und angreifbare sowie vornehmlich fremdkontrollierte Netzwerkinfrastrukturen des Webs und Internets abstellt.[3]

Wir stellen die faktische *Beherrschbarkeit* dieser für das "Schweizer" E-Voting wichtigen Basistechnologien sowohl für die Bundeskanzlei als auch für die Kantone sowie für die E-Voting-AnbieterInnen (wie z. B. der Schweizerischen Post) grundsätzlich in Frage und haben zur Veranschaulichung bisher zwei Angriffe demonstriert, welche Bund, Kantone und SystembetreiberInnen nicht gelöst haben:

- Angriff durch ein bösartiges Add-On auf der Seite der StimmbürgerInnen. Dieses Szenario ist dazu geeignet, das Stimmgeheimnis zu brechen und eignet sich auch dazu, StimmbürgerInnen daran zu hindern, ihre Stimmen abzugeben. Durch *Social-Engineering* sind zudem auch Manpulationen denkbar, die konkrete Abstimmungs- und Wahlpräferenz zu mutieren.[4]
- Angriff auf die zentralisierte, unsichere Namensauflösung *Domain-Name-System* (kurz: DNS), auf die die Bundeskanzlei und die Kantone setzen; dieses Szenario ist dazu geeignet, in die *Man-In-The-Middle*-Position (kurz: MITM) zu kommen, das Stimmgeheimnis für alle betroffenen BenutzerInnen (das kann ganze Länder einschliessen) zu brechen und eignet sich ebenfalls dazu, StimmbürgerInnen daran

[2] `https://www.bk.admin.ch/bk/de/home/politische-rechte/e-voting/versuchsuebersicht.html` (Abruf: 30.4.2019)

[3] Vgl. CCC-CH in Spiegel-Online, 9.2.2019: `https://www.spiegel.de/netzwelt/netzpolitik/e-voting-in-der-schweiz-widerstand-gegen-elektronische-abstimmungen-a-1252013.html` (Abruf: 30.4.2019)

[4] Vgl. CCC-CH in der SonntagsZeitung, 17.6.2018: `https://www.tagesanzeiger.ch/abstimmungen/EVoting-Fragiles-Stimmgeheimnis/story/27100992` (Abruf: 30.4.2019)

zu hindern, ihre Stimmen abzugeben.[5] Auch hier sind durch gefälschte Angaben auf der Mittelsseite, d. h. durch *Social-Engineering*, Manipulationen an der konkreten Abstimmungs- und Wahlpräferenz denkbar, sofern sie darauf setzen, von StimmbürgerInnen zu verlangen, vom vorgesehenen Prozess (leicht) abzuweichen. Erfahrungen aus dem Bereich *Phishing* (gerade auch beim E-Banking) lassen nicht darauf schliessen, dass die Schweizer Stimmbevölkerung besonders immun gegen *Social-Engineering* ist.

Selbst ohne Ansätze des *Social-Engineering* ist bereits die Möglichkeit zu den oben genannten Angriffen problematisch, weil *einerseits* die massenhafte Aufhebung des Stimmgeheimnisses als auch *andererseits* die massenhafte Verhinderung von Stimmabgaben, Abstimmungs- und Wahlmanipulationen darstellen: Konkret verfälschen sie die amtlichen Endergebnisse, entweder durch Effekte der *sozialen Erwünschtheit* oder aber gegeben durch den Umstand, dass BürgerInnen – z. B. AuslandschweizerInnen oder InlandschweizerInnen auf Ferien oder in anderen Gebieten der Schweiz – nicht erfolgreich ihre Stimme abgeben können. Ferner ist problematisch, dass die beiden Angriffsszenarien bis heute ungelöst sind und weiterhin Abstimmungen und Wahlen mit E-Voting-Systemen durchgeführt werden, welche diese skalierbaren Manipulationsmöglichkeiten bieten. Konkret kommt im Mai 2019 das Genfer System beispielsweise weiterhin in sechs Kantonen zum Einsatz.

Der E-Voting-Abstimmungskanal ist inhärent intransparent

Wir fordern den Verzicht auf die gesetzliche Verankerung eines Abstimmungskanals, das Stimmabgaben in vollelektronischer Form erfasst und darüber hinaus auf automatisierte Weise – ohne dass beliebige Menschen daran beteiligt sein können oder den Prozess unmittelbar beobachten könnten – "zählt".

Blockchain- und andere P2P-Systeme lösen das Vertrauensproblem nicht

E-Voting-Systeme haben als wichtige gemeinsame Eigenschaft, dass sämtliche Stimmabgaben ohne jede Handschriftlichkeit erfolgen, so dass prinzipiell nicht feststellbar ist, ob und wieviele der Stimmabgaben überhaupt von konkreten Menschen stammen. Darüber hinaus verschwindet die "Auszählung" in einem undurchsichtigen Meer von Bits und

[5] Vgl. CCC-CH im SRF, 2.11.2018: `https://www.srf.ch/news/schweiz/elektronische-abstimmungen-hacker-finden-schwachstelle-im-groessten-schweizer-e-voting-system` (Abruf: 30.4.2019)

Bytes – Nachzählungen werden faktisch abgeschafft. Mögliche Zweifel an den Endergebnissen – ob emotionsgeladen oder statistisch begründet – können nur mit Wahlwiederholungen beantwortet werden. An dieser Eigenschaft ändern auch dezentralisierte E-Voting-Systeme (einschliesslich *Blockchain*-Systemen), welche die Daten verteilt speichern, prinzipiell nichts. Abgesehen davon vergrössern solche Systeme die Gefahr, dass das Stimmgeheimnis nachträglich und auf Jahre rückwirkend gebrochen werden könnte – sind z. B. kryptografische Baufehler vorhanden oder wird die Kryptografie anderweitig (in der Zukunft) gebrochen. (Problem der *Everlasting-Privacy*)

Zentralisierte E-Voting-Systeme sind nicht robust

Auch sind aktuelle zentralisierte E-Voting-Systeme gegenüber dem analogen System der Papierwahl von mangelnder Robustheit geprägt: gezielte Störangriffe in Soft- und Hardware sowie massive Überlastungsangriffe über das Internet, die auch *Einzelne* ausführen können, sind geeignet, die Glaubwürdigkeit der Schweizer Abstimmungsdemokratie gezielt zu schwächen. Das sind Ausgangsbedingungen, die bei der Papierwahl ihresgleichen suchen. Dem CCC-CH ist es unverständlich, dass auch nach 19 Jahren Arbeit am Projekt *Vote électronique*, staatspolitischen Risiken noch immer nicht genügend Rechnung getragen werden.

Wir erachten es entsprechend als verantwortungslos, nun sogar den Plan umsetzen zu wollen, E-Voting in der Schweiz flächendeckend zu verbreiten.

Art. 6: Anforderungen an das Verfahren der Stimmabgabe

Öffentliche Kontrolle und echte Nachzählbarkeit geboten

In **Abs. 1** fehlen wichtige Anforderungen, die mit der *Vertrauenswürdigkeit* von Abstimmungen und Wahlen zusammenhängen: etwa dass Abstimmungen und Wahlen grundsätzlich der *öffentlichen Kontrolle* unterliegen sollten und man sich von der *Richtigkeit* einer Abstimmung oder Wahl überzeugen kann, auch ohne *besondere Sachkenntnisse* zu besitzen – insbesondere müssen *Nachzählungen* prinzipiell von beliebigen BürgerInnen durchgeführt werden können, und nicht etwa von (denselben) ComputerexpertInnen sklavisch abhängen.

E-Voting: ein Sonderling unter den E-Systemen

Solche Anforderungen für das E-Voting gegenüber anderen E-Systemen wie E-Banking, E-Commerce oder E-Mail zu verlangen (wo die zugrundeliegenden Prozesse auch komplex und nicht allgemeinverständlich sind), sind nicht etwa politischer Natur, sondern haben fundamental mit dem möglichen Angriffsrisiko, dem potenziellen Schadensmass und der Nachvollziehbarkeit des Systems auf der Outputseite – d. h. der Zweckmässigkeit der entsprechenden Digitalisierung zur Zielerreichung – zu tun; sie haben überdies mit der Beherrschbarkeit des Systems unter *Safety*- und *Security*-Gesichtspunkten der IT-Sicherheit zu tun. Unsere ablehnende Haltung folgt also einer erklärbar *rationalen Logik*. Denn: auch der CCC-CH lehnt die blosse Idee, elektronisch abstimmen und wählen zu können – als Computer- und Hackerclub notabene – nicht ideell ab, sehr wohl aber aus praktischen Gründen, die mit dem Wunsch nach dem Erhalt der Glaubwürdigkeit und des Vertrauens in die Schweizer Abstimmungsdemokratie zu tun haben. In jedem Fall ist es uns fremd, uns in blosse *Technikgläubigkeit* zu flüchten und blind dem Gefühl nach zu urteilen, ob E-Voting nun sicher und vertrauenswürdig ist. Es gibt Gründe, wonach geurteilt werden kann, dass E-Voting unsicher ist und bleibt; es sollte zumindest ein Leichtes sein, zu erkennen, dass ein E-Voting-System schwerlich vertrauenswürdig sein kann.

In Sachen Sicherheit: Safety und Security nicht dasselbe

Während selbst die aktuell im Einsatz befindlichen E-Voting-Systeme *sicher* im Sinn der *Safety* – oder *Betriebssicherheit* – sein können, so wäre es naiv anzunehmen, dass sie unter dem Gesichtspunkt der *Security* – d. h. in Betrachtung der Existenz von internen und externen AngreiferInnen – organisiert-kriminellen Zusammenhängen (im Auftragsverhältnis) oder staatlichen AngreiferInnen widerstehen könnten und entsprechend sicher sind. Es zeugt von geringem *Realitätssinn*, die Behauptung aufzustellen, die Staatskanzlei Genf oder die Schweizerische Post – die zwei zur Zeit (noch) real existierende Anbieterinnen – seien gefeit vor der Angriffspalette potenteter Geheimdienste, die nicht nur mit erheblichen *SIGINT*-Kapazitäten aufwarten, sondern – notfalls – auch Bodenpersonal (sogenannte *HUMINT*) zum Einsatz bringen können. Die Schweiz und ihre kritische Infrasturktur hängt schon heute in entscheidendem Masse von US-amerikanischer und chinesischer Gnade ab – betrachtet man z. B. die Lieferketten praktisch der gesamten in der Schweiz eingesetzten Hardware. Mit *Supply-Chain-Attacken* – d. h. Angriffen auf die Lieferkette – sollte bei Systemen, welche entsprechenden Profit und/oder Ein-

fluss versprechen – auf jeden Fall gerechnet werden.[6] Dazu gehören auch selbstredend ans Internet angeschlossene Abstimmungs- und Wahlsysteme, die zudem volleketronisch Stimmabgaben erfassen und daraus Ergebnisse erzeugen. Gemäss NSA bettelten solche Systeme danach, ausgebeutet zu werden – die Ansage dürfte deutlich genug sein.[7] Dass praktisch die gesamten eingesetzten Hard- und Softwarekomponenten aus dem Ausland geliefert werden, erleichtert Angriffe auf die Lieferkette deutlich.

Absehbar: Schwarzmarkt Abstimmungs- und Wahlergebnisse

Wer sich mit der Idee wenig anfreunden mag, dass ausländische Regierungen in der Schweiz Abstimmungen und Wahlen fälschen wollen könnten, kann auch den Blick auf Schwarzmärkte für Abstimmungs- und Wahlergebnisse richten – wo ein Geschäftsfeld für Abstimmungs- und Wahlfälschungen im industriellen Massstab lockt, wovor wir bereits Ende 2013 gewarnt haben.[8] Auf einem solchen können sich sowohl in- als auch ausländische Akteure, mit und ohne Geheimdienstverbindungen, tummeln. Angesichts auch in der Schweiz bereits mehfach erprobter Abstimmungs- und Wahlfälschungen wäre es naiv davon auszugehen, dass alleine im Inland das Mindset, Abstimmungen und Wahlen fälschen zu wollen, nicht existieren würde. Tatsächlich spielt E-Voting Akteuren in die Hand, die Abstimmungen und Wahlen fälschen möchten, weil es erstmals möglich wird, dies skalierend und schweizweit zu realisieren. Je nach Werkzeugkasten der AngreiferInnen ist weder eine Präsenz auf Schweizer Boden noch ein besonderer Bezug zur Schweiz zwingend erforderlich. Das Geschäftsfeld für AnbieterInnen von Abstimmungs- und Wahlfälschungen wird damit prinzipiell weltweit geöffnet.

GAU-Sicht: E-Voting ist einem AKW ähnlicher als E-Banking

Selbst Banken sehen sich – trotz Milliarden-Investionen in IT-Sicherheit – erfolgreichen Angriffen ausgesetzt. Im Unterschied zum E-Voting ist dort der Schaden aber unmittelbar ersehbar: In Fläche ist es nicht möglich, Banksaldi zu plündern ohne transparent Nachweis über Finanztransaktionen gegenüber den involvierten Parteien zu führen. Finanzieller Schaden ist zudem konkret in Geldwerten mess- und entsprechend versicherbar. Solche Verhältnisse wie beim Banking treffen bei der Demokratie nicht zu: Viel eher

[6] Vgl. CCC-CH im Tages-Anzeiger, 22.11.2018: `https://www.tagesanzeiger.ch/schweiz/standard/alle-evotingsysteme-der-schweiz-sind-unterwandert/story/31191771` (Abruf: 30.4.2019)

[7] `https://evote-net.ch/` (Abruf: 30.4.2019)

[8] Vgl. CCC-CH in der NZZ, 19.11.2013: `https://www.nzz.ch/zuerich/bald-ein-schwarzmarkt-fuer-wahlergebnisse-1.18187786` (Abruf: 30.4.2019)

ist das mögliche Schadensmass – der Vertrauensverlust in Abstimmungs- und Wahlergebnisse – eher vergleichbar mit einem GAU-Szenario des Betriebs von Atomkraftwerken. Naturgemäss ist der Schaden an der Demokratie, ähnlich wie bei einem erheblichen Unfall – z. B. mit nuklearem Fallout – ein *kollektives Risiko*. Der Schaden ist gesamtgesellschaftlich zu tragen; in Geld ist er nicht mess- oder aufwiegbar – entsprechend auch nicht versicherbar. Hingegen hat eine erfolgreiche Abstimmungs- oder Wahlmanipulation sehr wohl einen Marktpreis und kann so zur Handelsware krimineller Kreise werden.

Briefwahl und E-Voting: keine vergleichbare Skalierbarkeit

Auch bei anderen Verfahren des *Remote-Votings* – wie bei der Briefwahl – sind Einschränkungen hinsichtlich den Anforderungen **Bst b.** (Wahrung Stimmgeheimnis) und **c.** (Erfassung aller Stimmen) denkbar. Trotzdem ist ein Szenario schwerlich vorstellbar, indem bei den herkömmlichen Stimmkanälen schweizweit skalierend das Stimmgeheimnis gebrochen wird oder systematisch Stimmzettel nicht befördert bzw. von Postmitarbeitenden oder BeamtInnen vernichtet werden. Oder: Unter solchen Annahmen der massenhaften Unterwanderung unserer Gesellschaft ist nicht glaubhaft zu machen, ein Abstimmungsverfahren wie E-Voting sei in irgendeiner Form vertrauenswürdig zu betreiben. Schliesslich wird auch ein E-Voting-System von Menschen installiert und betrieben und kann von diesen in seinen Sicherheitseigenschaften entkernt bzw. bedeutend geschwächt werden.

Papierwahl mit hohem Entdeckungsrisiko für AngreiferInnen

Ein wesentlicher Unterschied gegenüber der Papierwahl ist zudem, dass ein E-Voting-System von nur sehr wenigen Akteuren entscheidend kontrolliert wird. Entsprehend erscheinen Angriffe durch Korruption oder Epressung gegenüber sehr wenigen Akteuren als sehr viel wahrscheinlicher als gegenüber breitester gesellschaftlicher Schichten, von denen nicht ernsthaft angenommen werden kann, dass sie sich schweizweit im Rahmen übergreifender Verschwörungen *unbemerkt* absprechen. Um diese Eigenschaft in einem Abstimmungs- und Wahlsystem zu bewahren, ist es entsprechend auch wichtig, dass die Auszählungen der Öffentlichkeit unterliegen und sich auch regional keine fixen Netzwerke bilden, die erst solche Absprachen – wenn auch kleinräumig – ermöglichen würden.

AuslandschweizerInnen: Stimmabgaben im statt vom Ausland

Insbesondere bei AuslandschweizerInnen erscheinen Angriffe nach **Bst. b.** und **c.** als

wahrscheinlicher, da ihre Stimmabgaben *transnational* erfolgen und bekannt ist, dass einige Länder auch Postsendungen systematisch überwachen. Auch können dortige Akteure bei entsprechendem Ressourceneinsatz Zustellungen in die Schweiz verhindern. Deswegen, und um Probleme mit der (beidseitigen) und zeitnahen Postzustellung zu mindern, sollte *einerseits* geprüft werden, wie Stimmabgaben nicht primär *vom*, sondern vielmehr *im Ausland* stattfinden können und *andererseits* geprüft werden, ob amtliche Stimm- und Wahlzettel unterstützt durch *E-Government* so zur Verfügung gestellt werden können, dass eine Zusendung ins Ausland optional wird. Als stark beschränkende Eigenschaft Missbräuche entsprechend **Bst. e.** zu begehen, bestünde – nach wie vor – die Handschriftlichkeit.

Bei E-Voting ist keine sinnvolle Aufklärung von Manipulationen möglich

Massenhafte Missbräuche bei *tatsächlichen* Stimmabgaben sind beim E-Voting hingegen

1. viel schwieriger zu erkennen, da jede Handschriftlichkeit entfällt und
2. in ihrem Ausmass viel schwieriger aufzuklären, da ihre Erkennung forensisch – durch die gleichzeitige Anforderung, das Stimmgeheimnis zu wahren – stark erschwert ist.

Es sind beim E-Voting schliesslich keine handschriftlich ausgefüllten Papierzettel vorhanden, auf deren Basis forensische Analysen des Schriftbilds vollzogen werden könnten. Den im System registrierten Stimmabgaben ist – als blosse elektronische Daten – zuletzt weder anzusehen, ob sie nur von stimmberechtigten Menschen entsprechend der Anforderung von **Bst. a.**, geschweige denn, ob sie überhaupt von einer entsprechenden Anzahl unterschiedlicher Menschen abstammen.

Massenhafte Abstimmungs- und Wahlmanipulationen mit E-Voting

Insbesondere für organisierte Kriminelle und staatliche Akteure eröffnet E-Voting ganz neue, realistische Angriffsvektoren, wonach unter massenhaftem Missbrauch der Stimmberechtigung (sogenannte *Impersonation*[9]) und vielfach entgegen der Anforderung von **Bst. e.**, wonach Missbrauch zu verhindern sei, Abstimmungen und Wahlen *grossflächig*

[9] Vgl. CCC-CH in der Datenschleuder (Vorabzug), April 2019: `https://chaosticino.ch/docs/ds100_auszug_cybervoting.pdf` (Abruf: 30.4.2019)

und *kantonsübergreifend* manipuliert werden können; dies konkret unter Ausnutzung einer oder mehreren der folgenden Arten, an die benötigten E-Voting-Codes zu gelangen:

- (Transnationales) Abfangen der E-Voting-Codes, die per Briefpost versandt werden.
- Kopieren der E-Voting-Codes (in ihrer Gesamtheit) bei den kantonalen Druckzentren – durch Unterwanderung der erstellenden Computer bzw. der Drucker und der Organisation von entsprechendem Datenabfluss an die Angreifenden.

Zu betonen sei, dass insbesondere beim zweiten Angriffsszenario auch Inside-Angreifende in den Druckzentren in Frage kommen, die im Rahmen von *HUMINT*-Operationen eingeschleust oder – zum Beispiel gegen grössere Geldsummen – korrumpiert werden können. Insbesondere seit den Snowden-Enthüllungen ab Mitte 2013 dürfte auch der Bundesrat zur Einschätzung kommen, dass Geheimdienstekomplexe einer Grossmacht wie den USA, die im industriellen Massstab und mit Jahresbudgets in der Grössenordnung dutzender Milliarden US-Dollar Angriffe gegen ganze Länder und ICT-Dienste planen und umsetzen, fähig sind, auch kantonale Druckzentren erfolgreich zu verwanzen – in Mehrzahl dadurch begünstigt, dass es darum geht, einen industriell angelegten Angriff (z. B. im Rahmen sogenannter *Advanced-Persistent-Threats* (kurz: APTs)) je Kanton (mit ähnlicher Infrastruktur) zu wiederholen.

"Individuelle" und "universelle Verifizierbarkeit": nutzlos

Gleichzeitig funktionieren diese Angriffsarten auch unter den hypothetischen Bedingungen, dass das E-Voting-System an und für sich mitsamt allen seinen Abhängigkeiten, sowie alle Endgeräte der beteiligten BürgerInnen, absolut sicher gegen Angriffe wären. Diese Angriffe passieren die vorgesehenen Verifikationsmechanismen komplett, da sie darauf basieren, an die Stelle der BürgerInnen zu treten und für diese abzustimmen oder zu wählen. Anders als bei Angriffen auf die Endgeräte real abstimmender BürgerInnen, wo es erforderlich sein kann, auf die Kollaboration mit den BürgerInnen durch *Social-Engineering* zu setzen, können bei dieser Angriffsart massenhaft Stimmabgaben erfolgen, die dem System nach – in sowohl sogenannt *individueller* als auch *universeller Verifizierbarkeit* – "gültig" sind, in grosser Menge den *Volkswillen* aber verzerren. Unter Bedingungen von Korruption und Erpressung erlauben sie insbesondere auch Behörden bzw. BeamtInnen, Abstimmungen und Wahlen im grossen Stil zu fälschen, so sie an eine Kopie der entsprechenden E-Voting-Codes gelangen. Das ist eine Eigenschaft, die – selbst wenn nie angewandt – in ein Abstimmungs- und Wahlsystem zur Machtverteilung

und zur Fällung grundlegender Richtungsentscheidungen für ein Land wie die Schweiz aus unserer Sicht nicht exisieren darf. Ein solcher *Single-Point-of-Failure* (kurz: SPoF), welcher die gesamten Sicherheitsschranken unnütz macht, ist für ein derart wichtiges System wie das der Schweizer Demokratie nicht opportun.

Die Wahlwiederholung ist keine Alternative zur Nachzählung

In der Risikobeurteilung besonders schwer wiegt, dass eine sinnhafte Aufklärung, wie bei anderen E-Systemen – z. B. dem E-Banking – nicht möglich ist. Externe AngreiferInnen können natürlich stümperhaft vorgehen und Spuren hinterlassen, wonach sie massenweise Stimmabgaben von nur wenigen Geräten oder Netzwerken abgeben. Auch internen AngreiferInnen können Fehler unterlaufen, so dass es ihnen nicht gelingt, die Historie erfolgreich zu fälschen. In keinem Fall ist aber sinnvoll und allgemeinverständlich diskutierbar, wie gross eine Manipulation tatsächlich war – selbst ExpertInnen werden sich gegenseitig widersprechen. Auch eine eigentliche Nachzählung kann nicht stattfinden – die (gefälschten) Endergebnisse bleiben sich treu. Das einzige Instrument, das verbleibt, ist eine *Wahlwiederholung*: Dies ist bei bundesweiten Abstimmungskämpfen oder gar Parlamentswahlen nicht nur mit hohen Kosten für die BefürworterInnen und GegnerInnen einer Vorlage verbunden, sondern bedeutet auch einen Vertrauensverlust in das politische System. Es ist nicht damit zu rechnen, dass sich die Häufung solcher Vorgänge in einer Erhöhung der Abstimmungs- und Wahlbeteiligung niederschlägt.

Art. 7: Stimmabgabe an der Urne

Es ist zu begrüssen, dass gesetzlich vorgeschrieben wird, zu garantieren, dass die Urnenwahl weiterhin und schweizweit existieren muss.

Sicherlich ungelöst bleibt das Problem für AuslandschweizerInnen: Ohne E-Voting oder mit E-Voting unter *DDoS*-Angriffsbedingungen zum Schluss einer Abstimmung oder Wahl ist es unrealistisch und ökologisch unsinnig davon auszugehen, dass diese das Stimmrecht via Urnenwahl wahrnehmen. Mit den Kantonen sollten Lösungen ausgearbeitet werden, die Präsenzwahl bei Botschaften oder Konsulaten zu ermöglichen. Dies gelingt offensichtlich auch anderen Ländern, namentlich der Europäischen Union – z. B. gerade mit Hinblick auf die Europawahl Ende Mai 2019. Finanzielle Erwägungen sollten – da es um demokratische Mitbestimmung geht – eine nur untergeordnete Rolle spielen,

falls das Ziel von Landesregierung und Kantonen tatsächlich ist, die fünfte Schweiz umfassend an den Schweizer Entscheiden zu beteiligen.

Art. 8 Abs. 1 und 1^{bis}: (Briefliche Stimmabgabe)

Im Erläuternden Bericht ist auf S.12 festgehalten:

> Selbstverständlich haben die *Gemeinden auch bei diesem Verfahren Massnahmen und Vorkehrungen zu treffen, damit den einschlägigen Bestimmungen über die unverfälschte Stimmabgabe Nachachtung verschafft wird.*

Es wird damit auf **Art. 6 Abs. 1** Bezug genommen; nicht garantiert ercheint uns, dass diese Prozesse öffentlich dokumentiert werden, damit (einzelne) Gemeinden oder Kantone konkret für ihre Praxen kritisiert werden können. Dies würde es in der Folge auch ermöglichen, das Vertrauen in die Papierwahl weiter zu festigen.

Art. 8a: Elektronische Stimmabgabe

Diesen Artikel gilt es restlos zu streichen.

Den Sinn bundesrätlicher Bewilligungen gemäss **Abs. 2** kann grundsätzlich in Frage gestellt werden: Jüngst wurde bekannt, dass das *Scytl*-System, für das die Schweizerische Post sich als Wiederverkäuferin für vier Kantone in Stellung gebracht hat, seit dem Jahr 2016 *illegal* – entsprechend der eigenen Verordnungen – im Einsatz ist.

Der Grund dafür ist, dass eine internationale ForscherInnengruppe um Sarah Jamie Lewis[10] gezeigt hat, dass die sogenannte *individuelle Verifizierbarkeit* kryptografisch gebrochen ist.[11] Es bestehen Hinweise, dass die Schweizerische Post – nicht ganz freiwillig – das aus dem Ausland stammende E-Voting-System bis auf weiteres und für die vier angeschlossenen Kantone BS, FR, NE und TG abgeschaltet hat.

[10] Vgl. Profil auf openprivacy.ca: `https://openprivacy.ca/people/sarah-jamie-lewis/` (Abruf: 30.4.2019)

[11] Vgl. Medienmitteilung CCC-CH, 25.3.2019: `https://www.ccc-ch.ch/2019-03-25_evoting_postdemokratie_stimme_unerwuenscht.html` (Abruf: 30.4.2019)

Nicht minder kritisch erscheint, dass der Kanton Neuchâtel schon zuvor viele Jahre ein (Vorgänger-)System von *Scytl* im Einsatz hatte – bevor er die Kontrolle an die Schweizerische Post übergab: Es besteht kein Grund zur Annahme, dass die Kryptografie bei diesem System tadellos war. Nicht weniger kann ausgeschlossen werden, dass es zu entsprechenden Manipulationen bereits kam.

Art. 8b: Nachvollziehbarkeit der elektronischen Stimmabgabe und der korrekten Ermittlung des Ergebnisses der elektronisch abgegebenen Stimmen

Alleine schon mangels der Möglichkeit für StimmbürgerInnen zu kontrollieren, welche konkrete Software im Einsatz ist[12] und weil mangels Handschriftlichkeit und wegen dem Stimmgeheimnis es nicht möglich ist, *Stichproben* über die approximative Richtigkeit der Abstimmung oder Wahl durchzuführen, kann von einer "korrekten Ermittlung des Ergebnisses" keine Rede sein.

Schwerer als bei der Briefwahl wiegen diese Eigenschaften beim E-Voting deshalb, weil – wie in der Kritik zu **Art 6.** angeführt – die Skalierbarkeit stark unterschiedlich ist (vgl. S.8). Zudem konnte bei der bisher grössten, bekannt gewordenen Wahlfälschung in Missbrauch der Briefwahl der Walliser Täter auf Grund des Schriftbilds ermittelt werden.[13] Eine Fornensik derart erscheint beim E-Voting aussichtslos (vgl. S.9).

Art. 8c: Öffentlichkeit der Informationen zum System und dessen Betrieb

Dieser Artikel ist restlos zu streichen.

Im Übrigen verweisen wir auf unsere Kritik an **Art. 8b** auf S.13.

---

[12] Vgl. CCC-CH im Tages-Anzeiger, 2.3.2018: `https://www.tagesanzeiger.ch/schweiz/standard/evoting-waere-das-ende-fuer-die-demokratie/story/16044404` (Abruf: 30.4.2019)

[13] Vgl. Aussagen CCC-CH im megafon, April 2019: `https://vecirex.net/docs/201904--megafon-evoting-burn-it-with-fire.pdf` (Abruf: 30.4.2019)

Art. 8d: Bewilligung der elektronischen Stimmabgabe

Dieser Artikel ist restlos zu streichen.

Im Übrigen verweisen wir auf unsere Kritik an **Art. 8b** auf S.13.

Zudem sei mit Blick auf **Abs. 3** speziell darauf hingewiesen, dass bisherigen Zertifizierungsübungen von Bund und SystembetreiberInnen von wenig Erfolg gekrönt waren – u. a. ist es enstsprechenden Prüfgesellschaften wie der *KPMG* nicht gelungen, eklatante Fehler in der Kryptografie des Systems der Schweizerischen Post aufzudecken. Dieselbe ForscherInnengruppe um Sarah Jamie Lewis, die nur wenige Wochen später auch die *individuelle Verifizierbarkeit* des Systems der Schweizerischen Post gebrochen hat (vgl. S.12), gelang es die vollmundigen Versprechen von Bund und Post hin zu einem System der *universellen Verifizierbarkeit* in Luft aufzulösen – das System hat sich vielmehr als System zur *universellen Wahlfälschung* entpuppt.[14]

Solche Verhältnisse sind deswegen als besonders kritisch zu beurteilen, weil ohne diese ForscherInnen die Gefahr da war, dass dieses System bei tatsächlichen Abstimmungen und Wahlen (weiter) zum Einsatz gekommen wäre – mit sowohl gebrochener *individueller* als auch *universeller Verifizierbarkeit*.

Zu guter Letzt ist es mit der blossen Zertifizierung einer E-Voting-Software, selbst wenn erfolgreich(er) möglich, nicht getan, denn: E-Voting-Systeme sind im Kontext eines Gesamtsystems von Endgeräten von StimmbürgerInnen, der Serverinfrastruktur und der vermittelnden Netzwerkinfrastrukturen (bei den bisherigen Systemen über das offene Web im Internet) in ihrer Sicherheit und Vertrauenswürdigkeit zu beurteilen. Das *NIST*, die US-Standardisierungs- und Regulierungsbehörde, kam schon 2011 nach einem Forschungsaufwand von USD 100 Millionen zum Schluss, dass *Online-Voting* (wie in der Schweiz) unmöglich abzusichern sei.[15] Wie es möglich ist, dass Bundesrat, Bundeskanzlei und Kantone hier zu abweichenden Ergebnissen kommen, bleibt ein Geheimins. Schliesslich macht die US-Behörde klar, dass es nicht möglich ist, sogenannte *Commodity-Hardware*, wie sie auch beim "Schweizer" E-Voting auf allen Seiten des *Online-Voting*

[14] Vgl. Medienmitteilung CCC-CH, 12.3.2019: `https://www.ccc-ch.ch/2019-03-12_evoting_totalschaden_universelle_wahlfaelschung.html` (Abruf: 30.4.2019)

[15] CSO Online, 2. Mai 2018: `https://www.csoonline.com/article/3269297/online-voting-is-impossible-to-secure-so-why-are-some-governments-using-it.html?page=2` (Abruf: 30.4.2019)

zum Einsatz kommt, erfolgreich als sicher zu zertifizieren.

Art. 8e: Anmeldung für die elektronische Stimmabgabe

Dieser Artikel ist restlos streichen.

Im Übrigen verweisen wir auf unsere Kritik an **Art. 7** auf S.11.

Art. 38 Abs. 1 Bst. c und Abs. 4 und 5: (Ungültige Wahlzettel und Kandidatenstimmen)

Diese Absätze sind restlos zu streichen.

Art. 47 Abs. 1^{ter}: (Verfahren)

Dieser Absatz ist zu streichen.

Art. 49 Abs. 1 Bst. c und Abs. 2 und 3: (Ungültige Wahlzettel)

Diese Absätze sind restlos zu streichen.

Art. 84 Abs. 2 und 3: Verwendung technischer Hilfsmittel)

Die Regelung von **Abs. 1** ist zu begrüssen, sofern sie die Kanäle der Papierwahl be-

trifft (auf E-Voting ist zu verzichten). Allerdings sollte sie nicht nur im Konjunktiv stehen, sondern zwingend erfolgen. Insbesondere sollten nur technische Hilfsmittel bewilligt werden, die im Quellcode und mit entsprechender Dokumentation vorliegen, damit ihre Funktionsweise nachvollzogen werden kann.

Die statistische Plausibilisierung in **Abs. 2** – insbesondere für Verfahren der automatischen Auszählung von Stimm- und Wahlzetteln – ist zu begrüssen. Sie deckt sich mit unseren Forderungen.[16]

Zu beachten ist ferner, dass ein konservativer Schwellenwert zu definieren ist, ob welchem automatisch eine komplette Nachzählung der Stimm- und Wahlzettel angezeigt ist, um rasch das Vertrauen in Abstimmungs- und Wahlergebnisse bei Abweichungen wieder herzustellen.

Es ist weiterhin bekannt, dass die aktuellen *E-Counting*-Systeme eine intransparente Funktionsweise aufweisen. Insbesondere ist der Quellcode dieser Systeme nicht bekannt: Bundesrat und Bundeskanzlei sind hier gefordert, *E-Counting*-Systeme zu fördern, die unter Freie-Software- bzw. Open-Source-Lizenzen verfügbar sind. Dies nämlich würde es der Öffentlichkeit erlauben, die Erkennungsraten dieser Systeme verbessern zu helfen und somit die Anzahl benötigter manueller Nachzählungen aller Stimm- und Wahlzettel zu minimieren.

Chaotische Grüsse

Für den CCC-CH: Hernâni Marques u. a. Mitglieder

[16] Vgl. Medienmitteilung CCC-CH, 2.3.2018: `https://www.ccc-ch.ch/ccc-ch-ruft-zum-boykott-vom-e-voting-stimmkanal-auf-und-fordert-statistisch-kontrolliertes-e-counting.html` (Abruf: 30.4.2019)