die datenschleuder.

das wissenschaftliche fachblatt für datenreisende
ein organ des chaos computer club

Preprint Auszug für Ausgabe 100: E-Voting in der Schweiz

Inhalt

Auszug aus „Die Datenschleuder Nr. 100“ (Beta Version, Stand 6. Mai 2019)

Herausgeber
(Abos, Adressen, Verwaltungstechnisches etc.)

Chaos Computer Club e. V.
Zeiseweg 9, 22765 Hamburg, <office@ccc.de>
PGP: 7845 0E35 3C70 05BA E2E7
CDDA 5E71 40C3 0426 8556

Kontaktadresse
(Artikel, Leserbriefe, Inhaltliches)

Redaktion Datenschleuder, Chaos Computer Club e. V.
Zeiseweg 9, 22765 Hamburg, <ds@ccc.de>
PGP: 2A75 2EB3 D0A0 5FA9 2726
2B8A A917 2CC7 B794 A17A
https://ds.ccc.de/

V. i. S. d. P.

Hanno „Rince“ Wagner

ISSN der Datenschleuder: 0930-1054 • 2019

$\frac{250}{100}$ €

#100

Zum „Schweizer“ Cybervoting: das Vertrauensproblem bleibt ungelöst

von Claudio Luck und Hernâni Marques
Vorstände und Pressesprecher CCC Schweiz <vorstand@ccc-ch.ch>

Das Projekt mit offiziellem Namen „Vote électronique“ (auch E-Voting oder weniger positiv konnotiert Cybervoting) läuft seit dem Jahr 2000. Es handelt sich dabei um ein Projekt der Bundeskanzlei – eine Stabsstelle der Schweizer Landesregierung (bekannt als Bundesrat), ganz ähnlich wie in Deutschland das Bundeskanzleramt. [1] Das primär vorgegebene Ziel ist es, das elektronische Abstimmen und Wählen der Zeit anzupassen – eine besondere Not dafür ist nicht angezeigt; insbesondere da das Abstimmen und Wählen in der Schweiz als Urnen- und Briefwahl akzeptiert ist. Hochrechnungen liegen an Abstimmungssonntagen unmittelbar nach Urnenschluss um 12 Uhr vor und Endergebnisse sind schon nach wenigen Stunden bekannt: einzelne Kantone oder Städte benötigen immer wieder länger oder haben auch einmal Probleme, doch an den Endergebnissen insgesamt ändert das nichts. Die aktuellen Verfahren genießen Vertrauen. Daran rütteln nun der Bundesrat und die Regierungen der Kantone (wie in Deutschland Bundesländer) verstärkt.

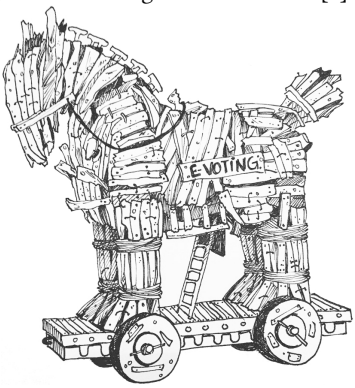
Ähnlich wie bei Wahlcomputern oder Wahlstiften [2] in Deutschland sehen wir uns in der Schweiz damit konfrontiert, dass Computerwahlen immer stärker verbreitet werden. Dabei handelt es sich bei der Form von E-Voting, die wir in der Schweiz haben, zusätzlich noch um wesentlich komplexeres E-Voting. Es wird über das Internet durchgeführt und ist somit – wie treffend im Logbuch:Netzpolitik Ausgabe 286 gesagt wurde [3] – tatsächliches Cybervoting, welches zudem „zeitsouverän“ ist, weil grundsätzlich von überall her abgestimmt werden kann. In den ersten Jahren hat die Bundeskanzlei zusammen mit interessierten Kantonen Grundlagen erarbeitet und seit 2004 finden praktische Versuche mit Cybervoting statt. Die daraus resultierenden Stimmabgaben fließen summarisch in die Endergebnisse ein. Von den ursprünglich 22 137 zugelassenen Cybervotern alleine im Kanton Genf (September 2004), waren für die Abstimmungen vom 10. Februar 2019 bereits 226 635 Credentials auf zehn Kantone verteilt, um Stimmen vollelektronisch ohne jeden Papertrail einzuspeisen.

Widerstand nötiger denn je

Der Erfakreis Zürich (CCCZH) hat sich 2013 erstmals öffentlich gegen Cybervoting geäußert – mit einem offenen Brief an das Zürcher Kantonsparlament, um den Kanal „elektronische Stimmabgabe“ aus dem Wahlgesetz streichen und Cybervoting somit verbieten zu lassen. [4] Der Antrag aus linken und rechten Kreisen scheiterte. Vordringlich wird die Lage seit April 2017 – da verkündet der Bundesrat per Medienmitteilung „[…] nächste Schritte zur Ausbreitung der elektronischen Stimmabgabe“ beschlossen zu haben. Ziel ist es, bis zu den Parlamentswahlen 2019 zwei Drittel der Kantone (Gesamtzahl Kantone: 26) mit dem Cybervoting zu beglücken [5]. Dieses Ziel konnten wir torpedieren [6].

Beginnend mit 2018 haben wir, nach längeren Mailthreads mit der Bundeskanzlei und einem Gespräch vor Ort, nicht nur die medialen Interventionen massiv verschärft [sie-

he 7], sondern auch angefangen demonstrative Hacks durchzuführen, um auf die grundsätzlichen Probleme des Cybervotings in Web-Voting-Form hinzuweisen: Danilo Bargen vom Coredump Rapperswil [8], ein Hackerspace des CCC-CH, hat beispielsweise gezeigt, wie auf den Endgeräten durch ein malignes Add-On das Stimmgeheimnis aufgehoben werden kann: abgesehen davon ist der Angriff geeignet, um Abstimmende an der Ausübung des Stimmrechts zu hindern – sollte beispielsweise die „falsche“ Wahl getroffen werden. [9]



Míka Eríksdóttir

Im November 2018 haben Volker Birk und andere Aktivisten des CCCZH [10] schließlich einen DNS-Spoofing-Angriff auf das Genfer System demonstriert, was durch den Umstand begünstigt wurde, dass weder HSTS-Preloading von Google noch DNSSEC der IETF aktiviert war [11]. Die Betreiber haben den Missstand, bekannte Angriffe dieser Art zu verteuern, auch in der Folge nicht behoben, wohingegen das System der Schweizer Post unter evoting.ch beide Technologien im Einsatz hat – DNSSEC seit Februar 2019; wenn auch die Unterstützung auf Ebene der Resolver für DNSSEC auch in der Schweiz mager (bei rund 10 %) bleibt.

Wichtiger ist aber die politische Ebene: Aktivisten des CCC-CH ist es zusammen mit ExponentInnen praktisch des gesamten Parteienspektrums gelungen, ein Initiativkomitee auf die Beine zu stellen, das ein fünfjähriges Moratorium für das Cybervoting fordert [12]. Die Diversität des Komitees, das von ganz links bis ganz rechts über das demokratische Spektrum reicht, ist auch für Schweizer Verhältnisse, wo es immer wieder parteiübergreifend *sachpolitisch* zu temporären Seilschaften kommt (vgl. beispielsweise den Kampf gegen das Überwachungsgesetz BÜPF [13]) erstaunlich. Andererseits wird damit klargemacht, dass es kein typisch parteipolitisches Thema mit Links-Rechts-Schema ist, sondern eines, wo es um alles geht: das Vertrauen in das politische System der Schweiz. Und: weil es offenkundig ist, dass die Bundeskanzlei zusammen mit einigen kantonalen Regierungen das Cybervoting verbreiten möchten, ist es unabdingbar, dass der politische Druck *schweizweit* erhöht wird, um dies zu verhindern. Die effektive Unterschriftensammlung, um eine Volksabstimmung über das Thema Cybervoting zu erzwingen, hat schließlich am Samstag, 16. März begonnen.

Nun haben wir zusammen mit den parteipolitischen und anderen Akteuren 18 Monate Zeit, um 100 000 gültige Unterschriften zu sammeln und (ironischerweise) bei der Bundeskanzlei einzureichen, die das Zustandekommen der Volksinitiative prüfen muss. Genauso ironisch ist, dass der Initiativtext von der Bundeskanzlei geprüft wurde – allerdings muss betont werden, dass es innerhalb der höchsten Stabsstelle auf Bundesebene diverse Abteilungen gibt. Das Cybervoting ist eine eigene Abteilung. Im Wesentlichen fordert die Initiative, dass Abstimmungen und Wahlen nicht nur ohne besondere Sachkenntnisse nachvollziehbar sind – ähnlich wie beim Urteil des Deutschen

Bundesverfassungsgerichts gegen Wahlcomputer, sondern auch, dass die Möglichkeit von Manipulationen nicht höher als bei Papierwahlen sein darf. Außerdem wird die Möglichkeit echter Nachzählungen gefordert – insgesamt Anforderungen, die mit heutigen uns bekannten ICT-Grundlagen äußerst schwierig zu erfüllen sein dürften, falls dies überhaupt je möglich sein sollte. Schließlich nimmt die Komplexität von ICT-Systemen tendenziell immer weiter zu und nicht etwa ab, wie dies nötig wäre, um IT-Sicherheit beherrschbar(er) zu machen.

Wie funktioniert das „Schweizer“ Cybervoting grundsätzlich?

Das Cybervoting der Schweiz soll flächendeckend als Web-Voting eingeführt werden. Abgestimmt wird mit beliebigen browserfähigen Geräten auf zentralen Webseiten der Schweizer Post oder der Genfer Staatskanzlei, wobei das Genfer System voraussichtlich zum letzten Mal im Februar 2020 zum Einsatz kommen wird.

Genf wirft – aufgrund der Notwendigkeit 2,3 Millionen Schweizer Franken zu investieren – schlichtweg das Handtuch. Und das, obwohl Genf seit mehr als zehn Jahre lang an ihrem Cybervoting-System gefeilt hat [14].

Die Schweizer Post baut unterdessen ihr System im Kern nicht selber, sondern hat dafür eine Kooperation mit der spanischen Firma Syctl, deren Motto „We Power Democracy“ lautet. Die Firma bietet elektronische Abstimmungslösungen (auch in Form von Wahlcomputern) in 42 (!) Ländern an: die Firmengeschichte ist, wie eine umfassende Recherche des Schweizer Online-Magazins Republik enthüllt hat, äußerst fragwürdig und schafft wenig Vertrauen [15]. Es ist ebenso wenig hilfreich, dass die Schweizer Post, zusätzlich zu ihrer Firmengeschichte als (Quasi-)Monopolist, in jüngerer Zeit mit Korruption aufgefallen ist: konkret wurde die Buchhaltung des Teilbetriebs PostAuto systematisch frisiert [16].

Die vorgeschlagene Spezifikation für ein „sicheres“ Cybervoting stammt von der Berner Fachhochschule (BFH), welche eng mit der Bundeskanzlei zusammenarbeitet: Es kommen Zero-Knowledge-Proofs, homomorphe Verschlüsselung und als zweiter Faktor ein Papierversand mit den Credentials (und Vergleichs- sowie Bestätigungscodes) zum Einsatz. Das Cybervoting der Schweiz kommt somit zur Zeit auch nicht ohne Papier aus [17]. Allerdings wurden bei anderen Systemen, wie in Estland, wo die Authentifikation mittels Personalausweis erfolgt, bereits erhebliche Sicherheitsprobleme durch Alex J. Halderman (akademisch spezialisiert auf Cybervoting) aufgezeigt [18, 19]. Trotzdem gehört die teilweise oder gar vollständige „Dematerialisierung“ zu den Zielen des Bundesrates, wie das aus dem Bericht der „Expertengruppe Vote électronique“ (EXVE) hervorgeht. [20]

Alleine der Umstand, dass für die elektronische Stimmabgabe weder besonders gesicherte Geräte noch ein persönlicher privater Schlüssel (z. B. im Personalausweis) zum Einsatz kommt, macht deutlich, dass skalierende Manipulationen, bei denen massenhaft Impersonation geübt wird, eine reale Gefahr sind: dies wird auch von den BFH-Forschenden nicht totgeschwiegen (vgl. S.134 der Spezifikation). Das „kryptografische Monster“ – wie das Republik-Magazin in einem weiteren Artikel treffend schreibt [21] – hängt sklavisch davon ab, dass die Credentials nicht abfließen bzw. in Kopie verkauft oder erhackt werden. Angesichts der Tatsache, dass es sich bei den Druckzentren für den Druck der Credentials um kantonale Betriebe ohne besondere elektronische Abschirmung oder erhöhten Sicher-

heitsvorkehrungen handeln dürfte, sind das kühne Annahmen. Zumal hier quasi hundertprozentige Sicherheit unabdingbar ist. Korruption ist ebenfalls ein Problem, das nicht ausgeschlossen werden kann – schließlich kann durch das gewählte Verfahren auch massenweise für Nichtwählende abgestimmt werden (vgl. zu den grundsätzlichen Sicherheitsproblemen einschließlich der Einschätzungen einiger namhafter internationaler KryptoexpertInnen wie [22] und [23]).

Míka Eríksdóttir

Zum eigentlichen Kern: Vertrauensprobleme ohne Ende

Des Pudels Problemkern beim Cybervoting ist aber nicht Sicherheit, sondern Vertrauen. Eine demokratische Abstimmung und Wahl muss dazu geeignet sein, nicht nur die Gewinnerseite, sondern auch eine Verliererpartei zufrieden zu stellen: in der Schweiz kommt es häufiger zu emotionsgeladenen Abstimmungskämpfen. Beispiele hierfür sind die Selbstbestimmungsinitiative oder die Masseneinwanderungsinitiative der SVP. Letztere wurde im Februar 2014 nur sehr knapp angenommen. Obwohl es spontan zu Protestkundgebungen linker Gruppierungen kam, hat niemand die Endergebnisse in globo angezweifelt. Solche Szenarien sind bei stärker verbreitetem Cybervoting, wie das geplant ist, sehr viel wahrscheinlicher, weil nur noch sehr wenige Akteure im Gesamtprozess involviert sind. Eine Auszählung bzw. ernstzunehmende Wahlbeobachtung wie bei der Papierwahl entfällt. Brisant ist, dass schon bei der heutigen Cybervoting-Verbreitung enge Abstimmungen und Wahlen knapp gekippt werden können. Eine wirkliche Gewissheit, dass dies nicht geschehen ist, gibt es nicht: man ist dem Prinzip Hoffnung ausgeliefert.

Beim Cybervoting besteht das grundsätzliche Problem, das die gesamte Kette im Ergebnis für einen normalen Bürger, aber auch für eine Kryptoexpertin nicht nachvollziehbar ist. Beispielsweise ist die Schweizer Post gezwungen, den Quellcode frei verfügbar zu machen, will sie ihr in Spanien eingekauftes Cybervotingsystem für 100 % des Elektorats eines Kantons zum Einsatz bringen. Dabei handelt es sich um rund 250 000 Codezeilen in der Programmiersprache Java, die von sehr hoher Komplexität geprägt sind [24]. Welcher Programmierer, welcher Kryptoexperte kann den gesamten Quellcode prüfen? Wie kann eine Bürgerin prüfen, ob dieser Code komplett unverändert läuft? Wie kann eine Bürgerin prüfen, ob die Toolchain, mit deren Hilfe der Quellcode in Bytecode übersetzt wurde, unverändert war? Wie kann ausgeschlossen werden, dass im letzten Schritt eine Hintertür eingeführt wird (Problem von „Reflections on Trusting Trust“ [25])? Baut die Schweizer Post den Quellcode überhaupt selber oder kommt das

Kompilat direkt aus Barcelona, wo Scytl den Hauptsitz hat?

Der Chaos Computer Club Schweiz (CCC-CH) ist der Ansicht, dass solcher Raum für Misstrauen und Spekulationen bei einem Abstimmungs- und Wahlsystem Gift für die Demokratie ist: Wir lehnen damit die Einführung von Cybervoting in der Schweiz resolut ab [26]. Wir machen hiermit auch klar, dass wir dezidiert sind, die Einführung von Cybervoting auf allen Ebenen zu bekämpfen und freuen uns hierbei auch um jede Unterstützung aus den CCC-Dezentralen in Deutschland und Österreich, denn: wird flächendeckendes Cybervoting in der Schweiz salonfähig, besteht akut die Gefahr, dass das auch in anderen Ländern Fuß fasst. Schließlich hat die Schweiz den Ruf einer stabilen und funktionierenden Demokratie mit umfassenden Mitbestimmungsrechten. Das Signal einer Schweiz, die Cybervoting einführt, ist für uns fatal. Wir möchten das verhindern und möchten erreichen, dass die Bundeskanzlei das Projekt nach fast 20 Jahren einstellt.

Happy Hacking!

Referenzen

[1] https://www.bk.admin.ch/bk/de/home/politische-rechte/e-voting.html

[2] Website Kampagne gegen Wahlcomputer, https://wahlcomputer.ccc.de/

[3] Tim Pritlove (14.02.2019): „LNP286 Zeitsouveränes Cybervoting“, https://logbuch-netzpolitik.de/lnp286-zeitsouveraenes-cybervoting

[4] Fabian Vogt (11.11.2013): „E-Voting in Zürich soll verboten werden“ https://www.computerworld.ch/business/digitalisierung/e-voting-in-zuerich-verboten-1332552.html

[5] Mitteilung des Bundesrates über nächste Schritte zum E-Voting, https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen/bundesrat.msg-id-66273.html

[6] https://www.watson.ch/

[7] Medienspiegel des CCC-CH https://www.ccc-ch.ch/category_pressreview.html

[8] https://www.coredump.ch/

[9] https://www.coredump.ch/2018/06/17/verletzung-stimmgeheimnis-e-voting-st-gallen/

[10] https://www.ccczh.ch/

[11] https://www.srf.ch/news/schweiz/elektronische-abstimmungen-hacker-finden-schwachstelle-im-groessten-schweizer-e-voting-system

[12] https://e-voting-moratorium.ch/

[13] https://stopbuepf.ch/

[14] https://www.nzz.ch/schweiz/e-voting-genf-will-eigenes-system-nicht-weiterfuehren-ld.1440276

[15] https://www.republik.ch/2019/01/31/das-heikle-geschaeft-mit-der-demokratie

[16] https://www.srf.ch/news/schweiz/postauto-skandal-so-lief-der-offerten-schwindel

[17] „Cryptology ePrint Archive: Report 2017/325“, https://eprint.iacr.org/2017/325

[18] https://estoniaevoting.org/

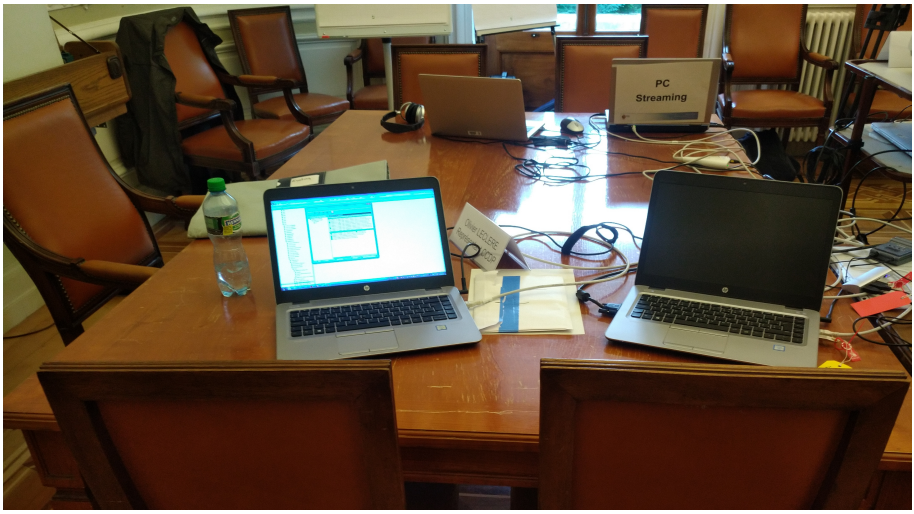
[19] https://media.ccc.de/v/31c3_-_6344_-_en_-_saal_1_-_201412281400_-_security_analysis_of_estonia_s_internet_voting_system_-_j_alex_halderman

[20] https://www.bk.admin.ch/bk/de/home/politische-rechte/e-voting/berichte-und-studien.html

[21] https://www.republik.ch/2019/03/01/10-neue-erkenntnisse-zum-e-voting-der-post

[22] https://www.nau.ch/politik/bundeshaus/e-voting-der-post-lasst-sich-

nicht-schutzen-sagt-chaos-computer-club-65486021
[23] https://www.heise.de/newsticker/meldung/Die-Schweiz-kurz-vor-dem-Haertetest-ihres-E-Voting-Systems-4316841.html
[24] https://ppzs.ch/2019/03/piratenpartei-zentralschweiz-republiziert-den-source-code-des-e-voting/
[25] „Reflections on trusting trust“ https://dl.acm.org/citation.cfm?id=358210
[26] https://www.ccc-ch.ch/ccc-ch-ruft-zum-boykott-vom-e-voting-stimmkanal-auf-und-fordert-statistisch-kontrolliertes-e-counting.html



Vertrauensverlust nach Cybervoting-Wahlbeobachtung

von Claudio Luck und Hernâni Marques
Vorstände und Pressesprecher CCC Schweiz <vorstand@ccc-ch.ch>

Die Schweizer Cybervoting-Systeme (auch E-Voting-Systeme) bauen stark auf Kryptographie auf. Die Wahlkommission – bestehend aus gewählten Politiker und Beamten – soll die Sicherheitselemente initialisieren und handhaben. Die Sicherheitsannahme der ganzen Abstimmung oder Wahl hängt vom vorsichtigen Umgang damit ab. Das verunsicherte zwei Hacker vom CCC Schweiz, die sich darauf als Wahlbeobachter beim „Genfer System“ empfahlen. Ein Erlebnisbericht.

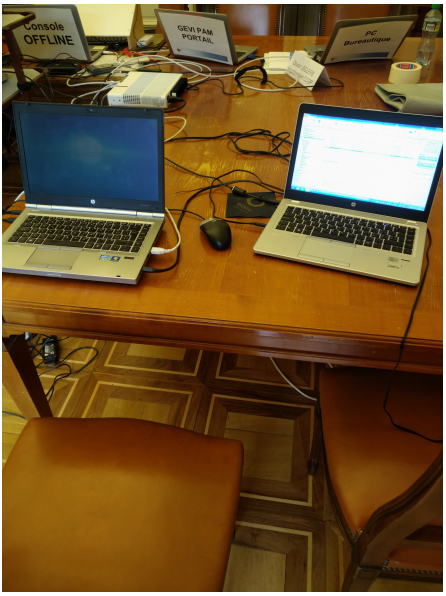
Während unserer Wahlbeobachtung am 23. September 2018 setzten sechs (von 26) Kantone auf das „Genfer System“: Aargau (AG), Basel-Stadt (BS), Bern (BE), Luzern (LU), St. Gallen (SG) und Genf (GE) selbst. Die Kantone lagern die gesamte Abwicklung des Cybervotings an die Staatskanzlei des Kantons GE aus. Sie behalten sich das Recht vor, eigene Leute zu entsenden. Jedoch macht kein Kanton mit Ausnahme vom Kanton SG davon Gebrauch. Die Kantone AG, BS, BE und LU übten im September selbst keinerlei für uns sichtbare Kontrolle aus.

Das offizielle Setting

Wir sind mit über 20 Leuten in einem Saal, die meisten haben eine offizielle Rolle inne.

Einige hingegen überwachen offenbar uns. Auch die Notizen, die wir auf Papier kritzeln, finden diskret zugeneigte LeserInnen.

Der Überblick ist von unserem Sitz aus hervorragend. Direkt vor uns ist eine Kamera aufgebaut. So sehen wir drumherum direkt auf den Kabelsalat. Ein Laptop zeigt eine E-Mail mit einem Passwort in großen roten Lettern. Sowieso sind die ganzen Laptops bereits aufgebaut, wenn die Wahlkommission eintrifft. Ob sie zwischenzeitlich manipuliert wurden, kann sie also nicht ausschließen. Auch wir als Wahlbeobachter sehen uns bei rechtzeitiger Ankunft mit dem fertigen Setup konfrontiert. Im weiteren Verlauf glaubt die Wahlkommission blind den Ergebnissen, die sie von diesen Laptops, via Projektor dargestellt, sieht.



Das rote Passwort weicht später einer TeamViewer-Session, womit sich die zwei Repräsentanten vom Kanton St. Gallen zuschalten, der einzige Kanton (außer Genf selbst), der sich um etwas (virtuelle) Kontrolle bemüht.

Wir erhalten noch eine Papierkopie des Sollprotokolls, der als „NON PUBLIQUE“ klassifiziert ist, und fragen uns, wer grad über TeamViewer alles mithört.

Auf den ersten Blick

Die ganze Wahlbeobachtung ist langweilig und repetitiv, weil man Systemadministratoren zuschaut, wie sie Dateien, die alle fast gleich heissen, schrittweise zwischen Remote-Desktops und lokale Speichermedien kopieren, sie dort vor- und nachbearbeiten sowie zwischendurch auf die Offline-Arbeitsstation transferieren. Währenddessen werden Prüfsummen der verschlüsselten und entschlüsselten elektronischen Wahlurnen vom Bildschirm ins Protokoll geschrieben und später verglichen. Genau genommen nur die ersten und letzten fünf Zeichen davon, was kryptografisch 40-bittiger Schwachsinn ist.

Etwas Hektik kommt im Saal auf, sobald die Kommissäre auf der Offline-Konsole die Passwörter zum geheimen Schlüssel preisgeben müssen. Auffallend demonstrativ laufen die Systemadministratoren, die sonst alle Systeme stellvertretend für die Wahlkommission bedienen, ans andere Ende des Saals. Ganz unauffällig hingegen lesen die Kommissäre bei der Eingabe der Passwörter von ihrem Handy ab. Dies ist angesichts der zu erwartenden Angriffe auf genau diese Geheimnisträger grobfahrlässig. Dass die sichere Offline-Verwahrung des geheimen Schlüssels durch den Handyeinsatz komplett dahinfällt, lässt die beobachtende Wahlkommission kalt. Alleine dies wäre ein plausibler Grund um die Fairness und auch die Integrität der Wahl auf der Stelle zu bezweifeln.

Die Wahlbeobachtung ist also doch elektrisierend, weil dem durchschnittlich aufmerksamen Hacker bei fast jedem Handgriff gewichtige Mängel im Sicherheitskonzept auffallen.

Schwierige Schlüsselsicherung

Die Sicherheit der elektronischen Urne beruht darauf, dass die geheimen Schlüssel absolut vom Internet fern gehalten werden („air-gapped“) und auch sonst nicht abfließen. Es ist aber anzunehmen, dass das „Offline“-Laptop, das mit Windows bestückt ist und aus dem normalen Beschaffungswesen des Kantons Genfs entstammt, durchaus irgendwie mit Updates aus dem Internet versorgt wird – ein Angriffspunkt, allen voran für staatliche Akteure. Auch das Gebäude ist elektronisch nicht abgeschirmt, so dass mit entsprechendenem Aufwand auch der Airgap keine wirkliche Hürde ist.

Die Passworthandhabe ist auch sonst eine Show. Dass die Kommissäre ihre Handys als Gedankenstütze einsetzen, ist bereits der GAU, wenn nicht sogar ein Super-GAU. Die Tastatur ist zwar verdeckt, aber trotzdem anfällig für „Schultersurfen“. Dafür besonders suspekt positioniert ist ein ungenutzter smarter TV-Flachbildschirm, der schräg hinten in der Ecke steht und alles spiegelt: wer weiß, ob der auch eine Webcam eingebaut hat. Im öffentlichen Bugtracker zur Genfer Cybervotingsoftware ist ein weiteres Problem dokumentiert: Die Software zeigt die Eingaben in das Passwort-Feld offenbar im Klartext an, statt – wie üblich – durch Punkte: Es gäbe dafür ein „Business Requirement“, da diese „political people“ nicht sehr geübt im Umgang mit Computern seien und es sonst wiederholt zu Eingabefehlern käme [1]. Es ist aber sowieso unklar, mit welcher Software hier wirklich gearbeitet wird und konkret die Endergebnisse erzeugt werden. Der veröffentlichte Quellcode des Genfer Systems ist weder vollständig noch auf dem neusten Stand.

Weiter in den Hash-Spielen

Da gleichzeitig Abstimmungen auf Bundesebene und eine freie Personenwahl im Kanton St. Gallen durchgeführt werden, wiederholen sich viele Schritte, die sich nur in Details unterscheiden. So fällt unter allgemeinem Gelächter plötzlich auf, dass der vorher notierte Hashcode des anderen Laufs verglichen wird – also wohl die falsche Seite des Protokolls abgearbeitet wurde.

Baustelle am Eingang zum Sitzungszimmer

Die Panne

Bei der Nachbearbeitung der ausgezählten Ergebnissen des Kanton St. Gallen wird eine erwartete Datei ohne Fehlermeldung einfach nicht generiert. Auch die Wiederholung der Schritte bringt keine Besserung, so dass die Sitzungsleitung beschließt, diesen Lauf zu unterbrechen und eine Pause einzuberufen.

Nach der angekündigten vorübergehenden Verweisung aus dem Saal (die Zwischenergebnisse sind zu dem Zeitpunkt noch Amtsgeheimnis) kommen wir rechtzeitig auf den Anfang der Pause zurück. Die Wahlkommission verweilt draußen bei Kaffee und Croissants, während die Techniker im Saal alleine detaillierte Debug-Logs studieren, von deren Existenz die Wahlkommission wohl keine Kenntnis hat. Keiner dieser Schritte ist im ausgehändigten Protokoll beschrieben.

Lockere Pause

Gegen Ende der langen Pause flanieren wir nochmals an der ganzen IT-Ausrüstung vorbei und versuchen nachzuvollziehen was mit welchem Kabel verbunden ist. Plötzlich fällt uns auf, dass wir ja ganz alleine im Saal stehen. In diesem Moment hätten wir beliebige Handlungen an allen Geräten vornehmen können – z. B. präparierte USB-Sticks einstecken, um nach Wiederaufnahme der Sitzung mittels autorun ein Chaos zu stiften. Es stellt sich beispielsweise die Frage, was eigentlich wäre, wenn plötzlich ein lächelnder Putin oder Trump projiziert würde. Wie würde das in Social-Media ankommen? Würde jemand den Ergebnissen der Kantone mit elektronischen Abstimmungen noch trauen? Wir realisieren, dass das Cybervoting in jedem Schritt an einem seidenen Faden hängt – und das kantonsübergreifend.

Außerplanmässige Lösung

Während der Pause kommt es mit der Staatskanzlei St. Gallen zur Absprache, dass man ohne die fehlende Datei auskomme. Der Plan ist also, weiterzumachen als ob nichts geschehen wäre. Unbegründeterweise wird angenommen, dass das Programm schlicht den Dienst verweigert hat, die Ergebnisse aber nicht verfälscht wurden.

Kopie zwecks Analyse

Zwecks weiteren Untersuchungen zur Panne wird aber noch eine Kopie eines der Speichermedien angefertigt und mit einer offiziellen Plombe (Kabelbinder) versehen. Auch das ist im Protokoll nicht vorgesehen. Es existiert nun also ein zusätzliches Speichermedium mit Daten über die Wahl.

Vertrauen entsteht nicht

Insgesamt fällt auf, dass es in der Praxis kein echtes Sicherheitskonzept gibt. Es mangelt bereits am Fundament für den Aufbau eines systematischen Information-Security-Management-Systems (ISMS). Ein Bewusstsein für die Risiken scheint wenig ausgeprägt. Es gibt keine systematische Integration von baulichen, organisatorischen, personellen und technischen Mittel. Würde man das ISMS systematisch aufbauen, würde man die Zielkonflikte erkennen, die das Cybervoting inne hat. Es verlagert und konzentriert die Absicherung der Wahlen hin zur Wahlkommission, die jedoch wie die Bevölkerung selbst keine besondere IT-Kenntnisse hat, und mit praktisch völlig ungesicherten Geräten hantiert. Die Staatskanzleien üben zudem keine effektive Kontrolle aus. Es liegt uns hierbei auch E-Mail-Korrespondenz mit am Genfer System beteiligten Kantone vor, die bestätigen, dass sie üblicherweise alles dem Kanton Genf und seiner Wahlkommission überlassen. Die Öffentlichkeit erfährt über abenteuerliche Operational-Security-Zustände und Pannen gar nichts. Offiziell zählt dieser Anlass nun offenbar zu den 200 und mehr „erfolgreichen Versuchen“ – wie die Bundeskanzlei gerne in den Medien betont und in einem „Faktenblatt – Vote électronique“ herausstreicht [2]. Wir haben bisher nur diese einzige Cybervoting-Wahlbeoachtung durchgeführt und sind schonmal entsetzt; wobei auch bei anderen Wahlbeobachtungen nicht

immer alles reibungslos abläuft, wie ein vorhergehender Erlebnisbericht vom Journalisten Christoph Lenz im Tages-Anzeiger zeigt [3]. Dort hat zumindest das Word von Microsoft gestreikt, eine proprietäre Software, die in einer derart sensiblen Umgebung, wo Endergebnisse vollelektronisch ohne Nachzählungsmöglichkeit erzeugt werden, gar nicht erst zum Einsatz kommen sollte.

Der Versuch auch den Eisatz des zweiten Cybervoting Systems zu beobachten (das der Post) wurde uns im Februar von diversen Kantonen verwehrt – u. a. vom Kanton Thurgau, der sich auf das Amtsgeheimnis (!) berufen hat. Dies trägt weiterhin nicht zu unserem Vertrauen in Teilergebnisse, die mit Cybervoting generiert werden, bei [vgl. 4, 5].

Referenzen

[1] https://github.com/republique-et-canton-de-geneve/chvote-1-0/issues/20

[2] https://www.bk.admin.ch/dam/bk/de/dokumente/pore/Faktenblatt%20E-Voting.pdf.download.pdf/Faktenblatt_DE.pdf

[3] https://www.tagesanzeiger.ch/schweiz/standard/Was-wenn-der-Tresorraum-der-Schweizer-Demokratie-geknackt-wird/story/29881888

[4] https://www.woz.ch/-958c

[5] https://www.tagblatt.ch/ostschweiz/frauenfeld/hacker-wenden-sich-wegen-e-voting-an-den-thurgauer-rechtsdienst-ld.1091346