E-Voting CH: Das Ende der Demokratie?

Wissen die Politiker, worauf wir uns hier einlassen? Ist sich der Bundesrat der Risiken und Folgen wirklich bewusst?

René Droz, Dipl. El.-Ing. ETH, ehemaliger Leiter des militärischen Computer Emergency Response Team, Führungsunterstützung, VBS, Worb
rdroz@sunrise.ch

Das Projekt E-Voting CH der Bundeskanzlei versucht die Quadratur des Kreises: günstig, sicher und bequem. Der Mensch wurde aber übersehen.

Bei E-Voting winken sofortige Resultaterkennung, Einsparungen bei den Auszählungsprozessen, Vergrösserung der Abstimmungsbeteiligung durch die «Generation Handy», durch handicapierte Personen und auch aufseiten der Auslandschweizer, die oft Mühe haben mit Lieferfristen per Post. Einfach und bequem soll es für den Stimmbürger sein, denn die Bemühungen, die richtige politische Antwort auf eine Abstimmungsfrage geben zu können, sind schon gross genug. Und selbstverständlich muss es auch sicher sein, denn niemand ist gewillt, sich in der politischen Willensbildung manipulieren zu lassen. Und zudem soll es auch nicht mehr kosten, als was jeder sowieso schon für seine IT-Infrastruktur ausgibt.

Die federführende Bundeskanzlei hat all dies umzusetzen versucht. Grosse wissenschaftliche Leistungen, insbesondere in der FH Bern, sind zweifellos erbracht worden. Bei der Kritik, die dennoch an der mangelnden ganzheitlich gesehenen IT-Sicherheit geübt wird, wird dann rasch der Vergleich mit anderen wichtigen Einrichtungen gemacht, die ebenfalls von der Cyberkriminalität bedroht werden, und die uns ebenso am Herzen liegen wie die Sicherheit der demokratischen Willensbildung. Aber sind diese Vergleiche angemessen?

Was ist speziell an E-Voting im Vergleich mit E-Banking?

Für einen solchen Vergleich wird meist E-Banking herangezogen: Jeder macht es, manchmal gibt's zwar Probleme, aber insgesamt gesehen funktioniert alles meist recht gut. Es gibt Ähnlichkeit im Vergleich der Architekturen punkto IT-Sicherheit: Man hat ein relativ teures, sicheres, gut überwachtes Zentralsystem und günstige, unsichere Usersysteme. Warum kann man das mit der Situation beim E-Voting zwar vergleichen, aber niemals gleichsetzen?

Es gibt entscheidende Unterschiede bei der Prävention, also den Sicherheitsmassnahmen (Tabelle 1), Unterschiede bei der Kontrolle der Transaktionen und beim Feststellen des Betru-

Crime Cases	E-Banking	E-Voting
Initialbedingungen	Die Bank kennt ein «normales» Verhalten und kann allenfalls Abweichungen erkennen, hinterfragen und/oder verhindern.	Es gibt kein normales oder erwartetes Verhalten, da meine Stimme mir gar nicht zugeordnet werden kann (Anonymitätsanspruch).
Missbrauch von Dritten bei Diebstahl der Account Credentials[1]	Authentizität der Benutzer wird meist gesichert durch Zusatzcode via Zweitkomponente (Handy) über Handy-Netz.	Sicherung durch Zweitkomponente: Printout mit Voting Codes werden über Postweg zugestellt (gleiches Risiko wie bei Briefpost-Voting).
Bei Verlust der Kontrolle über Computer durch Cyberattacke	Keine präventive Sicherung. Die gleiche Schadensart passiert nach der Feststellung aber nur einmal. Die Bank übernimmt Massnahmen zur Verhinderung des gleichen Angriffsmusters.	Keine präventive Sicherung. Die Erkennung ist nicht garantiert. Wenn erkannt, einzige sichere Massnahme zur Korrektur für das nächste Mal ist die Neuinstallation des PC.

Tabelle 1: Prävention: Sicherheitsmassnahmen

E-Banking	E-Voting
Ich stelle meinen Schaden bei jeder Transaktion immer und präzis fest und kann zusammen mit der Bank Massnahmen gegen den erlittenen Schaden ergreifen.	Der Einzelne könnte zwar einen Betrug bei sich feststellen und evtl. noch brieflich abstimmen. Er tut es aber nicht zwingend. Das Ausmass des gesamten Schadens kann nicht nachgemessen werden (Wie viele Infizierte, die nicht oder falsch abgestimmt haben?). Deshalb keine Massnahmen zur Korrektur möglich.

Tabelle 2: Kontrolle und Detektion des Betruges sowie nachträgliche Reaktion

E-Banking	E-Voting
Mein manipuliertes Konto schadet (höchstens) mir, allenfalls der Bank. Ich habe die Kontrolle darüber. Die Bank hilft beim Kalkulieren und Optimieren der Risiken und trägt allenfalls den Schaden mit.	Meine verfälschte Stimme schadet dem gesamten Stimmvolk. Dieses kann – als Ganzes – nichts tun. Die Bundeskanzlei hat die zentrale nationale Kontrolle. Sie trägt aber den Schaden nicht.

Tabelle 3: Das Opfer und die Hoheit über die Reaktion

ges (Tabelle 2) sowie Unterschiede beim Opfer und der Hoheit über seine Reaktionsmöglichkeiten (Tabelle 3).

Wie gut ist das E-Voting System CH und was sind die Risiken?

Hier sind drei Fragen zu beantworten: Wie günstig, benutzerfreundlich und wie sicher ist das E-Voting CH?

Kostengünstigkeit

Die Kostengünstigkeit kann zurzeit weder bestritten noch belegt werden. Es kostet den Anwender offenbar (vorläufig) nichts. Allerdings fehlen auch noch die Kostentransparenz und das Finanzierungskonzept. Es dürften seit 2000 schon sehr viele Millionen geflossen sein und noch viele weitere fliessen. Aber solange sie nicht in Gänze aufgezeigt werden, kann man auch keine Kosten/Nutzen-Rechnung anstellen.

Benutzerfreundlichkeit

Die Benutzerfreundlichkeit lässt sich an der Anleitung ableiten, die von den Kantonsverwaltungen herausgegeben wird. Es sind diverse, ellenlange Codes einzutippen und auf der Empfangsseite zu überprüfen, bevor man jeweils den nächsten Schritt machen kann. Verglichen mit der Briefwahl kann man bei bestem Willen nicht von einer Vereinfachung der Abstimmungsprozedur reden, denn das Einzige, was die Stimmenden damit nicht mehr tun müssen, ist, den Brief zuzukleben und zum nächsten Briefkasten zu bringen.

Sicherheit

Die Sicherheit der Lösung trägt viele Aspekte: Die IT-Architektur ist mit E-Banking vergleichbar, mit den oben erwähnten Unterschieden bei Prävention, Kontrolle und Verantwortung. Es werden für die Kantone zwei Applikationslösungen angeboten zur Vermeidung eines absoluten Hersteller-Klumpenrisikos. Im

Der Mensch bildet somit wieder einmal die grösste Schwachstelle im E-Voting, bei dem man sich grosse technische Mühe zur Herstellung von Sicherheit gegeben hat.

Kurz&bündig

Dass Cyberkriminelle in der Lage sind, unsere Computer im Internet zu Hunderttausenden unter Kontrolle zu bringen und Applikationen abzuändern, kann heute nicht mehr ernsthaft bezweifelt werden. E-Voting CH setzt darum auf die Bürger, die die Theorie der Codeüberprüfungen kennen müssen und nicht einfach blind der Applikation folgen. Dies ist nicht realistisch. Wir als Stimmbürger sollten aber darauf Anspruch haben, vom Staat geschützt zu werden, auch vor all den anderen Bürgern, die ihre Stimme aus Unachtsamkeit einer kriminellen oder ausländischen Organisation überlassen. Ausserdem gibt es noch weitere nachhaltige Insider-Risiken, die nicht einmal annähernd kalkulierbar sind. Zweifel an der Korrektheit der Abstimmungsergebnisse werden das Vertrauen der Bürger in unseren Staat tief erschüttern. Manipulationsvorwürfe sind in ihrem Ausmass aus Ressourcengründen nie zu beweisen oder zu widerlegen. Und wofür ein solches staatspolitisches Fiasko riskieren? Verglichen mit der erprobten Briefwahl ist einzig bei Auslandschweizern überhaupt ein nennenswerter Nutzen ersichtlich. Aber gerade sie sind die wahrscheinlichsten Opfer bei einer Manipulation.

Vergleich zu der Verteilung der Verantwortung auf 26 Kantonsverwaltungen stellt das aber immer noch ein relativ grosses Klumpenrisiko dar.

Den Systemanforderungen an die Applikation darf unterstellt werden, dass sie der kryptologischen Sicherheit genügend Rechnung tragen. Ob die beiden Umsetzungen davon dies ebenso tun, dürfte wohl keine demokratisch legitimierte Instanz kaum je prüfen und bestätigen bzw. widerlegen können. Dennoch würde die Fachwelt die grössten Risiken nicht zuerst da suchen, es gibt genügend offensichtlichere Risiken, die prioritäre Aufmerksamkeit einfordern und wohl den grösseren Risikobeitrag ausmachen.

Das Ziel der Anonymität der Stimmabgabe wurde bei der inzwischen verbotenen Lösung des Kantons Zürich offenbar verfehlt, bei den verbleibenden zwei Lösungen CHVote und Scytl wurde die Erfüllung dieser Anforderung glaubhaft gemacht. Allerdings gilt die Aussage nur *ohne* Berücksichtigung der hackbaren, völlig ungesicherten IT-Architektur des User-PC. Man darf daraus schliessen, dass der Staat zwar daran gehindert wird, mit E-Voting Gesinnungsschnüffelei zu vollziehen, dass aber Cyber-Kriminelle durchaus in der Lage wären, Abstimmungsdaten zu ermitteln. Was die damit machen würden, darüber kann spekuliert werden. Diese Konstellation finden wir flächendeckend in der IT-Landschaft, und sie zeigt, dass der Staat generell nicht bzw. nur in speziellen Fallkategorien in der Lage ist, die Bürger vor dem Cybercrime zu schützen. Die Frage stellt sich, ob man so einen Anspruch überhaupt stellen sollte und welche Konsequenzen man daraus ziehen sollte, wenn man es nicht kann.

Ohne genaueste Kenntnisse der technisch-betrieblichen Sicherheitsbedingungen lässt sich bei Insidern nur eines sicher sagen: Das Risiko kann nicht wirklich kalkuliert werden.

Das applikatorische Ziel der Sicherung gegen Stimmverfälschungen wurde insofern erreicht, als glaubhaft gemacht wird, dass die Kryptologie (d.h. die Erstellung der zu überprüfenden Codes) von Aussenstehenden nicht gefälscht werden kann. Es bedingt aber, dass der Stimmbürger das komplizierte Verfahren der Codeüberprüfungen beim Abstimmungsverfahren genau kennt und insbesondere merkt, wenn sein Computer etwas anderes zu wollen scheint, als die Originalapplikation und die Anleitung der Kantonsverwaltung vorgeben. Selbst dann kann der Benutzer aber im besten Fall nichts anderes machen als eine Briefwahl oder einen Gang an die Urne, wobei die Behörden dann in jedem einzelnen Fall manuell nachprüfen müssen, ob die Stimme nicht zweimal abgegeben wurde[2]. Bereits heute ist klar, dass in so einem Fall Auslandschweizer Stimmbürger meist *nicht* genügend Zeit haben werden für die Briefwahl, denn diese ist nur 24 Stunden länger offen als die E-Vote-Wahl.

Der Mensch bildet somit wieder einmal die grösste Schwachstelle im E-Voting, bei dem man sich grosse technische Mühe zur Herstellung von Sicherheit gegeben hat. Nicht nur der Mensch als Stimmbürger, sondern auch der Mensch als Betreiber oder Hersteller der Auszählungsanwendungen könnte natürlich bei entsprechender krimineller Energie Manipulationen einspeisen, die kaum überprüfbar sind. Eine kleine Gruppe von Insidern könnte eine riesige Wirkung bei der Resultatausgabe auslösen, genau so wie Stalin gesagt hat: «Nicht die Abstimmenden bestimmen das Resultat, sondern die Auszähler.» Welche Massnahmen hier zur Verhinderung solcher Möglichkeiten vorgesehen oder nicht vorgesehen sind, unterliegt keiner Kontrolle einer demokratisch legitimierten Instanz. Man müsste eine Art ENSI[3] für Cybergefahren erfinden, die sich damit befassen müsste. Aber selbst dann wissen wir, dass auch damit nicht alle Risiken ausgeschlossen sind.

Folgenden Risikokatalog der technischen Risiken kann man zusammenstellen:

- Risiko 1: Cybercrime Outsider benutzerseitig;
- Risiko 2: Cybercrime Outsider Zentrale;
- Risiko 3: Manipulation Insider Zentrale;
- Risiko 4: Diebstahl der Voting Codes[4];
- Risiko 5: Abfluss des Stimmgeheimnisses.

Das Risiko wird bestimmt durch den Anreiz eines Gegners, entsprechenden Schaden zufügen zu *wollen* (bzw. Nutzen daraus zu ziehen), sowie aufgrund seiner Fähigkeiten, es tun zu *können.* Die Schweiz in ihren politischen Entscheidungen zu beeinflussen, dürfte einen sehr grossen Anreiz auslösen. Wir müssen deshalb damit rechnen, es mit den besten Gegnern zu tun zu bekommen: Geheimdienste von ausländischen Mächten, kriminelle Organisationen mit entsprechenden Netzwerken und finanzkräftigen Kunden irgendwelcher Art. Alles, was möglich ist, wird via Darknet und Bitcoin in der Anonymität und im quasi rechtsfreien Raum gemacht werden. Die Fähigkeiten wiederum sind auch abhängig vom Schwierigkeitsgrad des Manipulationsvorganges.

Für Insider- und Outsider-Risiken sind komplett unterschiedliche Ansätze zu kalkulieren. Ohne genaueste Kenntnisse der technisch-betrieblichen Sicherheitsbedingungen lässt sich bei *Insidern* nämlich nur eines sicher sagen: Das Risiko kann nicht wirklich kalkuliert werden, vor allem nicht, wenn man die dynamischen Umgebungsparameter eines Informatik-Centers mit ins Kalkül zieht, wie Software-Migrationen und -Updates, Hardwarewechsel, Zutritts- und Notfallregelungen, Personalüberprüfungen, personelle Wechsel bei Verantwortlichen, Betreibern, Lieferanten, Reinigungspersonal etc. Bei den besten *Outsidern* weiss man, dass ihre Fähigkeiten sich nicht nur auf *bekannte* Schwachstellen und deren Exploits[5] in den Betriebssystemen und Browsern stützen, die gerade noch nicht behoben sind, sondern dass es zudem einige *unbekannte* Schwachstellen in den Systemen gibt, welche (vorerst) nur Eingeweihte mit Zugang zu Geheiminfos von Herstellern und anderen Geheimdiensten bereits kennen. Solche Angriffe gab es selbst in der Bundesverwaltung und sie waren erst nach Jahren zu entdecken. Auch der deutsche Bundestag und das amerikanische Verteidigungsdepartement waren schon betroffen.

Beim Risiko 1 (Cybercrime Outsider benutzerseitig) kann man darum jetzt schon die Wahrscheinlichkeit attestieren, dass es passieren wird. Der Gegner wird sich aber erst formieren, wenn es attraktiv und erfolgversprechend genug ist, er wird keine mehrjährige Testphase brauchen. Der verwendete Trojaner wird vielleicht nicht die Abstimmungscodes simulieren können, aber er kann z.B. verhindern, dass auf dem User-PC die Verifikation oder die Bestätigung der Verifikationskontrolle durchgeführt werden kann, und das abhängig davon, was abgestimmt wurde. Einige Stimmenden werden das merken, andere nicht. Einige werden die Hotline anfragen. Die Antwort dort wird immer die gleiche sein: «Die Briefwahl ist für Sie noch offen.» Aber selbst bei diesen Leuten wird es einige geben, die die Zeit, die Lust oder die Möglichkeit nicht mehr haben, die Stimme mit dem Brief oder an der Wahlurne abzugeben, und das sind z.B. insbesondere die Auslandschweizer. So entsteht ein *nicht vernachlässigbares Potenzial an entweder manipulierten oder verhinderten Stimmen.*

Wo sind die Überlegungsfehler im Projekt bei der Bundeskanzlei?

Man stellt sich die Frage, ob denn die federführende Bundeskanzlei nicht um diese Gefahren der Cyberkriminalität weiss? Die Antwort ist ganz einfach: Doch, sie weiss es. Ihr Standpunkt ist: «Unsere Anweisungen zu einer sicheren Stimmabgabe sind klar. Sie müssen sich einfach genau an diese Anweisungen halten, und wenn Sie einen Fehler in Ihrem Computer bemerken, können Sie noch brieflich abstimmen. Dazu müssen Sie einfach früh genug mit E-Voting anfangen.» Daraus ist zu schliessen, dass der Stimmbürger offenbar selbst schuld ist, wenn er das System nicht richtig versteht und nur den Anweisungen des Computers folgt, währenddessen die Bundeskanzlei ihre Arbeit richtig gemacht hat.

Sollte die Demokratie nicht eher das Vertrauen der Bürger zum Staat und seinen Institutionen optimieren als nur die Effizienz der Verwaltungsvorgänge?

In der Verwaltung geht man davon aus, dass die Bürger alles korrekt ausführen, und wenn nicht, trifft es sie selbst und sie müssen es auch selbst auslöffeln. Der Anspruch des Stimmbürgers, vom Staat geschützt zu werden, vor all den anderen Bürgern, die ihre Stimme aus Unachtsamkeit einer kriminellen oder ausländischen Organisation überlassen, scheint kein Thema zu sein. Statt der Verifikation wird nur eine Verifizierbarkeit angeboten. Sollte die Demokratie denn im Übrigen nicht eher das Vertrauen der Bürger zum Staat und seinen Institutionen optimieren als nur die Effizienz der Verwaltungsvorgänge?

Gemäss Auskunft aus der Bundeskanzlei ist vorgesehen, dass man dort, wenn während einer Abstimmung «genügend Meldungen über Unregelmässigkeiten» aufträten, das E-Voting suspendieren könne und wolle. Leider hat man aber offenbar keine Ahnung, mit welcher Dunkelziffer man rechnen müsste. Meldet so einen Vorfall jeder Fünfte oder jeder Fünftausendste? Kommen diese Meldungen bei der Hotline an, sind sie qualitativ brauchbar, werden sie verdichtet und analysiert, und wenn ja, von wem? Und wer würde dann den «Halt»-Knopf drücken, in welchem Augenblick und bei welchem Anlass? Und was geschieht mit bereits gefälscht eingegebenen und bestätigten Stim-

Fussnoten

1 User-ID/-Passwort bzw. Voting Card Data. Sie könnten gestohlen (kopiert) werden.
2 Aufgerubbelter Bestätigungscode auf dem Stimmausweis.
3 Eidgenössisches Nuklearsicherheitsinspektorat ENSI.
4 Alle benötigten Codes.
5 Ausnutzungsprozedur, die dank der Schwachstelle Zugang verschafft.
6 <http://www.noevoting.ch>.

	Risiko-kategorie	Beschreibung	Detektion	Mögliche reaktive Gegenmassnahme	Risikobeurteilung
1	Cybercrime Outsider benutzerseitig	Einspeisen von Schadcodes in die Applikation: – verleiten den User, Codes einzuspeisen – verleiten den User, Codes nicht zu überprüfen – behindern die Abstimmung alles in Funktion der Abstimmungsabsicht	Möglich, aber mit grosser Dunkelziffer	Wenn detektiert, Briefwahl im Einzelfall Nachzählung ist nicht möglich	Wahrscheinlich, trifft Gesellschaft
2	Cybercrime Outsider Zentrale	Einspeisen von Schadcodes in die zentralen Vorgänge zur Manipulation der Auszählung	Möglich	Wenn detektiert: Wahlwiederholung Nachzählung ist nicht möglich	Möglich, nicht kalkulierbar, trifft Gesellschaft
3	Cybercrime Insider Zentrale	Manipulieren der Auszählung	Kaum	Keine	Möglich, nicht kalkulierbar, trifft Gesellschaft
4	Diebstahl der Voting Codes	Abstimmungsrecht geht an nicht autorisierte Personen	Ja, aber nicht garantiert	Nur auf Antrag der Betroffenen kann korrigiert werden	Möglich, nicht kalkulierbar, trifft Gesellschaft
5	Abfluss des Stimmgeheimnisses	Die Stimme von z.B. prominenten Bürger(-inne)n wird zwecks Erpressung oder Herabsetzung veröffentlicht	Ja	Justiz	Möglich, nicht kalkulierbar, trifft Einzelnen

Tabelle 4: Risikokatalog

men, wer zählt die verhinderten Stimmen und avisiert die Betroffenen, die es nicht gemerkt haben? Diese sind nie alle zu erfassen.

Was sind die Folgen von breiter Einführung E-Voting CH?

Wie auch immer die oben gestellten Fragen beantwortet werden, es muss klar daran erinnert werden, dass es neben diesen bekannten «akuten» Risiken noch die «chronischen», erwähnten nichtkalkulierbaren IT-Risiken gibt. Diese können u.U. nicht einmal detektiert werden, wenn sie eintreffen (Tabelle 4: Risiko-Katalog).

Unterlegene politische Gruppierungen werden somit alles behaupten können und keiner der Verantwortlichen kann etwas sicher bestätigen oder widerlegen.

Wenn das Erstere noch nicht dazu gereichen sollte, führt zumindest diese Tatsache garantiert zu einer Verunsicherung in der Bevölkerung. Es könnte aber auch umgekehrt zu einer Vortäuschung von Cybercrimes kommen, da diese ebenso schwierig zu evaluieren sind, wie die echten Cybercrimes selbst. Unterlegene politische Gruppierungen werden somit alles behaupten können und keiner der Verantwortlichen kann etwas sicher bestätigen oder widerlegen. Feststellungen verbleiben in vagen Vermutungen. Für genaue Überprüfungen bräuchte es gigantische Ressourcen. Das Zeitalter der «alternativen Fakten» wird dann auch hierzulande aufblühen.

Das Vertrauen in Politik und Staat wird massiv gestört, die gesellschaftlichen Folgen wären verheerend: Das Urgestein unseres nationalen Zusammenhaltes zerbröselt.

Das Parlament ist jetzt gefragt. Die Gesetzgebung zu E-Voting kommt wohl erst in zwei bis drei Jahren. Bis dann läuft das Ganze als Testbetrieb ohne gesetzliche Grundlage munter weiter. Man könnte sich z.B. auch an den Erkenntnissen anderer Länder orientieren: Sie haben E-Voting abgesagt (Norwegen, Frankreich, Deutschland). Wer will das in drei Jahren noch stoppen, wenn bis dann noch keine offensichtlichen Skandale – hervorgebracht durch Medien – vorliegen? Wenn das Parlament nicht in der Lage ist, E-Voting zu stoppen, so kann nur noch das Volk mit einer Initiative[6] helfen. ■