Gefahren des e-Voting: Warum die Demokratie gefährdet ist

E-Voting wird als zusätzliche Wahlmöglichkeit etabliert – so hat es der Bundesrat entschieden. Doch wie sicher sind unsere Abstimmungen? Die Bundeskanzlei glaubt, dass sie mit der individuellen Verifizierbarkeit beim E-Voting CH das gröbste Sicherheitsproblem gelöst hat. Doch dabei hat sie den Menschen als Hauptschwachstelle vergessen, schreibt unser Gastautor René Droz.

Abstract.

Dass Cybermächte und auch -kriminelle in der Lage sind, unsere Computer via Internet zu Hunderttausenden unter Kontrolle zu bringen und so Applikationen abzuändern, kann heute nicht mehr ernsthaft bezweifelt werden. E-Voting CH setzt auf die Kompetenz der Bürgerinnen und Bürger, die die Theorie der Codeüberprüfungen kennen sollten und nicht gutgläubig den möglicherweise manipulierten Anweisungen auf dem Bildschirm folgen. Dies ist jedoch keine realistische Annahme. Das Stimmvolk hat Anspruch darauf, vom Staat geschützt zu werden, auch vor all den anderen Bürgerinnen und Bürgern, die ihre Stimme aus Unachtsamkeit einer kriminellen oder ausländischen Organisation überlassen. Ausserdem gibt es weitere nachhaltige Insider-Risiken, die nicht einmal annähernd kalkulierbar sind, so lange nicht absolute Transparenz aller Vorgänge herrscht, die zur Auszählung führen. Manipulationen wären zwar theoretisch detektierbar, wenn alle Vorgaben für diesen Zweck wirklich umgesetzt wären. Dies zu prüfen ist eine kaum handhabbare Herausforderung, zumal einmal gemachte Voraussetzungen jederzeit ändern können. Ein Restrisiko bleibt, dass die Manipulationen nicht aufgedeckt werden. Im wahrscheinlichsten Fall eines Angriffes auf den ungeschützten Heimcomputer ist das Ausmass aus Ressourcengründen nie so akkurat festzustellen, dass man das Gesamt-Ergebnisses mit Sicherheit als rechtens beweisen oder widerlegen könnte. Willkür tritt zudem dann auf, wenn aufgrund von Meldungen oder einzelnen Untersuchungen offiziell der Schluss gezogen würde, dass die Wahl wiederholt werden müsse, bzw. dass für eine Manipulation des Endergebnisses zu wenige Beweise vorlägen. Sollte das mehrmals vorkommen, so wird die Demokratie zur Farce. Willkür und auch schon geringste Zweifel an der Korrektheit der Abstimmungsergebnisse werden das Vertrauen der Bürgerinnen und Bürger in unseren Staat tief erschüttern. Wer will das in unserem Land?

Urvertrauen in die staatlichen Organe gefährdet

Die Gefährdung der Demokratie ist grundlegend von der Tatsache abhängig, ob wir einem Abstimmungsergebnis zutrauen können, dass es authentisch ist. Es gibt technische Risiken, die dazu führen können, dass es das nicht ist. Es gibt ein gesellschaftliches Risiko, dass wir aufgrund der technischen Risiken – vielleicht schon bevor sie eintreten - nicht mehr an die Funktionsfähigkeit der Demokratie glauben. Das Urvertrauen in die Institutionen unseres Staates stellt aber einen unverzichtbaren Wert dar. Die Verwaltung könnte jetzt nämlich versucht sein, einen allfälligen Schaden durch Manipulationsversuche an der Abstimmung bzw. Wahl kleinzureden, weil sie nicht in der Lage ist, genaue Fakten zu liefern. Willkürliche Entscheidungen, ob eine Wahl wiederholt werden muss, führen zu berechtigtem Unmut bei Volk und Politik. Man könnte sogar Manipulationen

glaubhaft vortäuschen, um Abstimmungswiederholungen zu erreichen. Aufgrund unklarer Fakten werden politische Gruppierungen alles behaupten können. Es steht nichts weniger als der Frieden im Land auf dem Spiel.

Das technische Risiko für eine Manipulation 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, die die Cyberbedrohung zu ihrem militärisch-strategischen Potential rechnen und auch 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.

Folgenden Risikokatalog der technischen Risiken einer Manipulation kann man zusammenstellen:

1. Cybercrime Outsider benutzerseitig: Angriff auf die Station des Abstimmenden
2. Cybercrime Outsider Zentrale: Angriff auf die Ballot-Auszählungsprozedur, die Ergebnisanzeige und die Prüfprozeduren durch eine Cyberattacke via Internet.
3. Manipulation Insider Zentrale: Gleichartiger Angriff durch einen Insider via Administrator Zugang. Einspeisung eines Fremdprogrammes und Löschung aller Spuren dafür.
4. Diebstahl der Voting Codes[1] durch Insider oder Outsider via Internet, via Druckzentrale oder elektronisch am Netz der Code erstellenden Computer
5. Abfluss des Stimmgeheimnisses durch Eingriffe in den Heimcomputer des Abstimmenden

Bei den besten Outsidern weiss man, dass ihre Fähigkeiten sich nicht nur auf bekannte Schwachstellen und deren Exploits[2] 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 geheimen Informationen von Herstellern und Geheimdiensten bereits kennen. Solche Angriffe gab es selbst in der Bundesverwaltung, und sie wurden erst nach Jahren zufällig entdeckt. Auch der deutsche Bundestag und das amerikanische Verteidigungsdepartement waren schon betroffen.

Ohne genaueste Überprüfungen der technisch-betrieblichen Sicherheits-Bedingungen lässt sich bei Insidern 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.

Beim **Risiko 1, bei dem** die Station des Abstimmenden angegriffen wird, kann man jetzt schon die Wahrscheinlichkeit attestieren, dass es sicher passieren wird. Die Frage ist nur: wann? Der Gegner wird sich erst formieren, wenn es attraktiv und erfolgversprechend genug ist, er wird dann keine mehrjährige Testphase brauchen. Auf dem Handy lädt man z.B. eines Tages eine neue E-Voting App, mit der man ein Foto der Codes machen muss, um die mühsame Code-Eingabe zu ersparen. Die App kann dann gleich auch selbst abstimmen und einem vorgaukeln, sie hätte das abgestimmt, was *man*

[1] Alle benötigten Codes
[2] Ausnutzungsprozedur

eingegeben habe. Der verwendete Trojaner im Computer wird vielleicht nicht die Abstimmungscodes simulieren können, aber er kann z.B. verhindern, dass auf dem User-PC die Verifikation oder die Bestätigung der Verifikations-Kontrolle durchgeführt werden kann, und das abhängig davon, was man abstimmen wollte. Einige Stimmberechtigte werden das merken, die meisten aber 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 Potential an entweder manipulierten oder verhinderten Stimmen. Sie können nicht erfasst werden, denn sie werden sich nicht alle melden und sich als vermeintliche „Digital-Idioten" outen.

Risiko 2 und 3 – also Angriffen auf die Ballot-Auszählungsprozedur, die Ergebnisanzeige und die Prüfprozeduren durch eine Cyberattacke via Internet bzw. die Manipulation Insider Zentrale - sind Varianten des Angriffs auf die Auswertezentrale. Aufgrund der Tatsache, dass nur ganz wenige Leute die Prozeduren genau kennen, die für die Ergebnisermittlung relevant sind, ergeben sich folgende Probleme:

1. Wie kann ein Angriff überhaupt erkannt werden, wenn dieser auf die Überprüfungshilfsmittel erfolgt, auf die sich der Betreiber verlässt?

2. Wie kann ein Angriff verhindert werden, der vom (vielleicht einzigen) Fachmann aus selbst erfolgt?

Natürlich könnte man mit aufwendigen organisatorischen Prozessen alle diese Fälle abzufangen versuchen. Es darf aber aufgrund gemachter Erfahrungen in realen IT-Umfeldern bezweifelt werden, dass bei Kantonsverwaltungen überall genügend Know-How zur richtigen Zeit an der richtigen Stelle ist. Der dafür nötige Ressourcenaufwand würde wohl nicht geleistet werden (können).

Beim **Risiko 4, dem** Diebstahl der Voting-Codes[3] durch Insider oder Outsider via Internet, können Unberechtigte eine Stimme abgeben, klugerweise in den letzten möglichen Augenblicken der Abstimmung, denn nur dann bleibt es erfolgreich und unbemerkt, falls der Originalbesitzer des Voting-Codes zu den Nichtwählern gehört. Auch das gibt ein beachtliches Potential an gefälschten Nichtwählerstimmen. Eine daraufhin festgestellte „erhöhte Stimmbeteiligung" könnte sogar als Rechtfertigung für E-Voting interpretiert werden. Es ist aufgrund des Abstimmgeheimnisses unmöglich, diese Stimmen zu zählen. Der Verlust der Codes könnte zwar eines Tages bekannt werden, das muss aber nicht zwingend sein.

Risiko 5, der Abfluss des Stimmgeheimnisses durch Eingriffe in den Heimcomputer des Abstimmenden wurde soeben von einem Studenten in der Praxis nachvollzogen[4]. Nicht der Staat muss verdächtigt werden, Abstimmungsdaten für andere Zwecke als die Auszählung zu missbrauchen. Aber alle andern hätten mit ein wenig krimineller Energie und etwas Know-How die Möglichkeit, dies zu tun. Was sie damit anfangen würden, bleibt Objekt der Spekulation.

[3] Alle benötigten Codes

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

Zum Autor:

Dipl. El.-Ing. ETH René Droz, 65, leitete 10 Jahre lang das militärische Computer Emergency Response Team in der Führungsunterstützung im VBS. Er verfügt über 28 weitere Jahre Berufserfahrung in Industrie und Verwaltung in den Bereichen Netzwerktechnik und IT Sicherheit.
Er ist heute pensioniert und setzt sich ehrenamtlich für politische Anliegen, die sein Fachgebiet betreffen, ein.

21.06.2018/dr