Ctrl-Alt-R

10 neue Erkenntnisse zum E-Voting der Post

Von Patrick Recher, 01.03.2019

E-Voting geht in eine nächste Runde. Nach der Veröffentlichung des Quellcodes kann das System der Post seit Montag legal gehackt werden. Ausserdem haben Post und Bundeskanzlei an einer Medienkonferenz Fragen beantwortet. Hier die 10 wichtigsten Erkenntnisse der Woche:

1. Der veröffentlichte Source Code ist unvollständig: Ein Bestandteil sowie die Anleitung zum Starten fehlen

Auf Nachfrage der Republik hat die Post klargestellt, dass nicht der gesamte Source Code veröffentlicht wurde:

> Nicht Bestandteil des publizierten Materials sind die Konfiguration des Urnengangs, ein User Interface (UI) für die Abstimmung und weitere Konfigurationsteile. Diese Elemente wären nötig, um einen End-2-End-Urnengang abwickeln zu können.

E-Mail von Post-Mediensprecher Oliver Flüeler, 16. Februar 2019.

Zudem fehlt die Anleitung, wie das System gestartet werden kann. Das erschwert die Prüfung des Systems. Die Situation ist vergleichbar mit einem Autohersteller, der sein neustes Modell in Einzelteile zerlegt, ohne Bauanleitung auf den Prüfstand schickt und behauptet, Experten könnten damit die Sicherheit des fertigen Fahrzeugs beurteilen. Das System erfüllt aufgrund dieser zwei Mängel den Artikel 7b der Verordnung der Bundeskanzlei über die elektronische Stimmabgabe nicht.

2. Die Bundeskanzlei hat noch nicht entschieden, ob die Post sämtliche Auflagen erfüllt

Die Bundeskanzlei wird das System der Post erst beurteilen, wenn der erste Kanton den Antrag stellt, die elektronische Stimmabgabe mit diesem System für alle zu ermöglichen. Die Post und die spanische Firma Scytl, welche die Technologie liefert, haben also noch die Chance nachzubessern.*

3. Das Modell «Open Code» bröckelt: Scytl und Post lassen Kopien löschen, ein Leak gab es trotzdem nicht

> Die Post kann nicht nachvollziehen, warum man einen Quellcode, der frei und legal zugänglich ist, als Raubkopie verbreitet.

E-Voting-Blog der Post.

Von einem Leak zu sprechen, suggeriert fälschlicherweise, dass der Code vorzeitig** an die Öffentlichkeit gelangt ist. Das ist falsch. Es wurden Kopien des von der Post veröffentlichten Source Code auf anderen Websites verbreitet. Gemäss der Lizenz ist dies verboten.

> Distributing or publishing the access tools, granting access to third parties and sharing the source code are not permitted.

Lizenz E-Voting-Solution.

Der veröffentlichte Code gehört Post und Scytl. Die Veröffentlichung soll die staatlichen Auflagen erfüllen – mehr nicht. Der Begriff Open Code ist eine Erfindung der Post. Anders als bei Open Source Code wird die Community nicht zur Mitarbeit eingeladen. Dies ist bei so wichtiger Infrastruktur wie der Abstimmungssoftware bedauerlich.

4. Nach dem 24. März sind keine legalen Tests mehr möglich

Bis Donnerstag haben sich mehr als 2900 Personen aus über 18 Ländern für den öffentlichen Intrusionstest angemeldet. Dieser wurde von Bund und Kantonen gefordert, um die Sicherheit des Systems zu prüfen. Alle Beteiligten sind sich einig, dass dies lediglich eine weitere Massnahme ist und sich die Sicherheit deshalb nicht abschliessend beurteilen lässt.

Derzeit gibt es keinen Plan, nach dem Ablauf des Intrusionstests am 24. März einen rechtlichen Rahmen für das legale Hacking des Systems zu schaffen. Die Bundeskanzlei zeigt sich offen dafür, dass «gutgesinnten Leuten» immer ein Kanal offenstehen werde. Doch Hackerinnen, die den Verdacht haben, Sicherheitslücken entdeckt zu haben, fehlen dann das Testsystem und die rechtliche Absicherung. Im Vergleich zur Post haben alle grossen Technologiefirmen (Github, Facebook, Tesla, Amazon) ein fortlaufendes sogenanntes Bug-Bounty-Programm.

5. Geheimdienst und weitere Bundesbehörden sind in die Sicherheitsvorkehrungen involviert

Die Bundeskanzlei informierte an der Medienkonferenz diese Woche erstmals darüber, «dass kompetente Stellen innerhalb der Bundesverwaltung und externe Experten in den Intrusionstest eingebunden wurden und eine längerfristige Zusammenarbeit mit ihnen angestrebt wird». Namentlich sind dies auf Nachfrage der Republik die Melde- und Analysestelle Informationssicherung (Melani), der Nachrichtendienst des Bundes und das Verteidigungsdepartement.

6. Von den Prüfberichten wurden nur die Deckblätter veröffentlicht

Die Zertifizierung des Wirtschaftsprüfers KPMG soll die Sicherheit des E-Voting-Systems belegen. Geprüft wurden die Funktionalität, die Infrastruktur und der Betrieb und die Sicherheit gegen Angriffe. Die erste Prüfung hatte fünf Mängel zutage gefördert, die dann von der Post korrigiert wurden, um zertifiziert zu werden. Welche Mängel beanstandet wurden, wird nicht bekannt gegeben.

Der Bundeskanzlei liegen lediglich die Deckblätter der Zertifikate vor. Diese konnten dank des Öffentlichkeitsgesetzes publik gemacht werden. Die Post sagte an der Medienkonferenz auf Nachfrage, dass die vollumfänglichen Dokumente nur den Kantonen zur Verfügung stehen, weil ein Vertrag mit KPMG und Details in den Dokumenten die Veröffentlichung verhindern. Damit sich die Öffentlichkeit ein Bild über die Sicherheit des Gesamtsystems machen kann, wäre eine Veröffentlichung aller Berichte zwingend.

7. Die Wählerinnen sind für die Sicherheit ihres Computers selber verantwortlich

> Natürlich trägt auch der Abstimmende eine Teilverantwortung, dass sein Gerät möglichst vertrauenswürdig ist, etwa in dem er keine Software zweifelhafter Herkunft installiert, regelmässige Updates durchführt etc.

Schriftliche Antwort der Post auf Anfrage der Republik.

Aufgrund der ausgeklügelten Kryptografie ist es praktisch ausgeschlossen, dass Stimmen manipuliert werden können, ohne dass dies pflichtbewussten Wählern, die ihre erhaltenen Kontrollcodes prüfen, auffallen würde. Wenn ein Computer oder ein Smartphone mit schädlicher Software (Viren, Trojaner oder Ähnliches) infiziert ist, kann das Stimmgeheimnis jedoch aufgehoben werden. Philipp Egger von der St. Galler Staatskanzlei sagt, dass sich die Kantone bewusst sind, hier noch Aufklärungsarbeit leisten zu müssen.

8. Auch E-Voting beginnt mit einem Brief – und die elektronischen Urnen schliessen vor den Wahllokalen

Um elektronisch wählen zu können, muss zuerst ein Brief mit Codes in Empfang genommen werden. Jederzeit und überall abstimmen zu können, wird damit nicht möglich. Zudem werden die elektronischen Urnen 24-Stunden vor den Wahllokalen geschlossen – eine Sicherheitsmassnahme, sollte das System im letzten Moment ausfallen oder manipuliert werden. So könnten Wählerinnen immer noch zur Urne eilen. Damit ist das Argument, E-Voting sei einfacher und bequemer, nur eingeschränkt gültig.

Die Expertengruppe Vote électronique umreisst in ihrem Schlussbericht vom 27. Juni die Pläne, E-Voting in Zukunft zu «dematerialisieren», also den Stimmausweis elektronisch zuzustellen.

9. Im Gegensatz zur Papierwahl ist die Verantwortung bei E-Voting auf nur wenige Personen verteilt

Bis anhin konnten Wählerinnen darauf vertrauen, dass die korrekte Durchführung von Wahlen und Abstimmungen von Wahlbehörden und auszählenden Bürgern gewährleistet wird. Beim E-Voting wird die Verantwortung auf weniger Personen aufgeteilt. Die Bevölkerung und die Mitarbeiter der Kantone müssen den Softwareentwicklern von Scytl und den Systemadministratoren der Post vertrauen. Die Öffentlichkeit kann nicht überprüfen, ob der veröffentlichte Code jener ist, der auf den Servern läuft. Open Source Code und Blockchain-Technologie hätten das Potenzial, die Öffentlichkeit besser einzubinden.

10. Das komplizierte System wird nicht in absehbarer Zeit für die Mehrheit der Bevölkerung verständlich sein

Das zentrale Element der Demokratie – Wahlen und Abstimmungen – wird zu einem kryptografischen Monster, das grosse Teile der Bevölkerung nicht durchschauen werden. Enorme Anstrengungen müssen unternommen werden, um das System sicher zu machen und Manipulationen zu erkennen. Geht bei Wahlen etwas schief, wird das Vertrauen in den demokratischen Prozess nachhaltig geschwächt. E-Voting hat das Potenzial, Wahlen sicherer zu machen. Es ist grundsätzlich wünschenswert, aber das vorliegende System ist noch nicht so weit.

** In Abschnitt 2 haben wir fälschlicherweise behauptet, dass die Kantone und der Bundesrat angestrebt hätten, E-Voting noch 2019 für alle Stimmenden zuzulassen. Bund und Kantone streben lediglich an, dass zwei Drittel der Kantone E-Voting einsetzen. Wir entschuldigen uns für den Fehler.*
*** In einer früheren Version dieses Artikels hiess es, der Code sei unerlaubt an die Öffentlichkeit gelangt.*

Veranstaltung

Heute Abend findet im Rothaus eine Debatte über das E-Voting-System der Post statt. Eingeladen sind Gäste aus der Praxis, Experten, Republik-Journalistinnen – und Sie. Es hat noch Plätze frei.