Ctrl-Alt-R

E-Voting der Post – hat jemand den Code geprüft?

Von Andreas Moor, 29.03.2019, Update: 13.45 Uhr

Übung abgebrochen: «Post setzt ihr E-Voting-System befristet aus», verkündet die Post in einer aktuellen Pressemitteilung. Während des Intrusionstests seien kritische Fehler entdeckt worden, deshalb werde die Post «den Quellcode korrigieren und von unabhängigen Experten erneut überprüfen lassen». Das Unternehmen betont, dass es während des Intrusionstests nicht zu einer Manipulation der Abstimmungsresultate kam.

Bei der aktuellen Diskussion über das E-Voting-System der Post spielt die universelle Verifizierbarkeit von Abstimmungsresultaten eine zentrale Rolle. Dabei handelt es sich um einen kryptografischen Mechanismus der Software, der sicherstellt, dass die Bürgerin sich weder auf *die Korrektheit der Übermittlung* noch auf *die Ehrlichkeit des Betreibers* verlassen muss.

Der Wähler muss lediglich die auf den Abstimmungsunterlagen aufgedruckten Codes mit denen auf dem Bildschirm vergleichen – eine Kette ausgeklügelter Verschlüsselungskomponenten stellt sicher, dass eine Manipulation der Abstimmung ausgeschlossen ist und dass das Abstimmungsgeheimnis gewahrt wird. Diese Funktion ist auch eine zwingende Anforderung in Artikel 5.1 der Verordnung über die elektronische Stimmabgabe (VEleS), bevor das System für mehr als die Hälfte der Abstimmenden zugelassen wird.

Am 24. März haben Sarah Jamie Lewis und ihr Team in dem für die universelle Verifizierbarkeit zuständigen Quelltext erneut einen schwerwiegenden Mangel entdeckt. Er ermöglicht es einem Angreifer, elektronisch abgegebene Stimmen so zu verändern, dass sie ungültig gewertet und deshalb nicht gezählt werden – ohne dass dies bei der formalen Verifizierung bemerkt würde. Wie beim letzten Mal hat die Post reagiert und erneut mitgeteilt, dass es schwierig sei, «die Schwachstelle auszunutzen, weil ein Angreifer zahlreiche Schutzmassnahmen ausser Kraft setzen müsste».

Gegenüber der Republik erklärt Sarah Jamie Lewis: «Ohne universelle Verifizierbarkeit muss sich die Öffentlichkeit darauf verlassen, dass die Post (oder eine andere Wahlbehörde) mit dem Abstimmungsergebnis ehrlich umgeht – diese Bedingung ist unhaltbar in einer demokratischen Gesellschaft.» Ihr Team habe zwar nur einen kleinen Teil des Quellcodes untersucht, doch es habe gezeigt, dass «das System für den beabsichtigten Zweck nicht geeignet» sei.

Da stellt sich natürlich die Frage: Wer legt für die Qualität des Programmcodes die Hand ins Feuer?

Theorie und Praxis

Früher oder später gelangt man so zu Abschnitt 5.4 des Anhangs «Technische und administrative Anforderungen an die elektronische Stimmabgabe» der VEleS, in dem ausgeführt wird, wie die Überprüfung der Verifizierbarkeit im Rahmen der Zulassung durch die Bundeskanzlei vonstattenzugehen hat. Für die Vertrauenswürdigkeit massgebliche Funktionen, heisst es dort, «sind anhand des Quellcodes und des kryptografischen Protokolls eingehend zu prüfen».

Im Fundus von Prüfzertifikaten der Post allerdings *fehlt der Nachweis, dass diese Untersuchung des Quellcodes stattgefunden hat*. Weder Post noch KPMG beantworten die Fragen der Republik zur Zertifizierung des Quellcodes. Die Firma Contego, gegründet von zwei ETH-Professoren für Informationssicherheit, bescheinigt dem Unternehmen zwar, dass die Protokolle und theoretischen Grundlagen des Systems grundsätzlich valide sind, vollzieht allerdings keine Beurteilung der Implementierung.

Sprecher René Lenzin von der Bundeskanzlei meint dazu lapidar, «dass der Offenlegung des Quellcodes eine Überprüfung nach Ziffer 5.4 VEleS Anhang vorausgehen muss». Ob diese Voraussetzung erfüllt sei, prüfe die Bundeskanzlei «im Rahmen eines allfälligen Bewilligungsverfahrens». Sprich: Der Bund wartet auf die erste Anfrage eines Kantons, bevor er überhaupt etwas prüft.

Kryptografie ist theoretisch, die Entwicklung von E-Voting-Systemen ist praktisches Ingenieurshandwerk. Das von Contego erstellte Gutachten befasst sich mit der Theorie; eine Beurteilung der Umsetzung im Quellcode ist nirgends zu finden. Hat ihn jemand untersucht und steht er oder sie für die Codequalität gerade? Wenn ja, wer? Wenn nein, was dann?

Wenn man sich in der Diskussion um die Sicherheit des elektronischen Abstimmens anstatt auf Transparenz auf das Renommee von Organisationen mit wohlklingenden Namen wie KPMG und ETH stützt, muss man das Versprechen von Solidität auch einlösen. Es genügt nicht, sich hinter einer Mauer des Schweigens zu verschanzen und zu hoffen, dass der Sturm bald vorüberzieht.