KANTON LUZERN

Kantonsrat

A 388

Anfrage Estermann Rahel und Mit. über die Sicherheitsstandards von Software im Bereich Wahlen und Abstimmungen

eröffnet am 26. Oktober 2020

Kaum ein Land führt so viele Urnengänge durch wie die Schweiz. Mindestens vier Mal pro Jahr finden hierzulande kommunale, kantonale oder nationale Wahlen und/oder Abstimmungen statt. Sie sind wichtige Momente der direktdemokratischen Mitbestimmung. Das Vertrauen in die Richtigkeit der Wahl- und Abstimmungsergebnisse ist hoch. Gleichzeitig müssen die Wahl- und Abstimmungsprozesse höchsten Anforderungen an die Sicherheit und Vertraulichkeit genügen, damit dieses Vertrauen gewahrt bleibt. Würde dieses Vertrauen erodieren, zögen Interessengruppen und Parteien die Resultate in Zweifel, was Gift für das direktdemokratische Schweizer System bedeutete.

Das Auszählen von Wahl- und Abstimmungsergebnissen umfasst zwar immer noch viel Handarbeit, gleichzeitig kommt in den Urnenbüros auch Software zum Einsatz: einerseits für die Erfassung und Auszählung von Abstimmungszetteln («E-Counting»), andererseits für die Übermittlung, die Zusammenfassung und die Errechnung von Ergebnissen. Während Ersteres in der «Verordnung über die elektronische Erfassung und Auszählung von Stimmzetteln bei Abstimmungen» geregelt ist, gibt es zu Letzterem wenig Vorgaben. Der zweite Bereich – die Übermittlung, die Zusammenfassung und die Errechnung von Ergebnissen sowie die dafür eingesetzte Software – ist Gegenstand dieser Anfrage.

Die Verantwortung für diese Software tragen die Kantone. Zwei Forschungsgruppen der ETH Zürich beziehungsweise der Universität Zürich haben voneinander unabhängig die von den Kantonen eingesetzte Software für die Übermittlung, die Zusammenfassung und die Errechnung von Wahl- und Abstimmungsergebnissen untersucht. Dabei kamen in den meisten Softwares Sicherheitslücken zum Vorschein[1] – auch in derjenigen, die im Kanton Luzern (und in weiteren Kantonen) im Einsatz ist: der Software Sesam Wahlen[2] der Sesam AG. Die gefundenen Sicherheitslücken sind:

- «Insiderattacken»: Wer sich bereits innerhalb des Verwaltungsnetzes befindet oder sich Zugang verschafft, hat umfassende Administrationsbefugnisse und könnte nach Belieben Ergebnisse verändern.
- Der Zugriff auf die Datenbank, in der die Wahl- und Abstimmungsresultate durch die Gemeinden eingetragen werden, verläuft über ein einziges Login mit einem Standardpasswort. Dieses ist öffentlich verfügbar und müsste von der Administration aktiv geändert werden – was aber niemand kontrolliert.
- Zudem ist der Quellcode der Software nicht öffentlich einsehbar und folgt damit nicht dem Open-Source-Prinzip. Die Offenlegung des Quellcodes von Software (Open Source) wäre eine einfache und in Fachkreisen anerkannte Möglichkeit, um für mehr Sicherheit und Transparenz – und somit Vertrauen – in eine Software zu sorgen.[3]

[1] https://www.republik.ch/2020/09/25/passwort-wahlen
[2] https://www.sesam-ag.ch/wahlen/
[3] Zwei Beispiele: 1. So konnten Fachspezialist*innen durch die Offenlegung des Quellcodes der E-Voting-Software Fehler und Sicherheitslücken aufdecken. 2. Das Open-Source-Prinzip war eine der tragenden Säulen, um ein hohes Vertrauen in die Schweizer Corona-App sicherzustellen.

Insgesamt existieren in den Urnenbüro-Prozessen genügend manuelle Überprüfungsmechanismen, so dass nicht davon ausgegangen werden muss, dass in Luzern bisher Manipulationen vorgekommen sind. Trotzdem ist es wichtig, sich um höchste Sicherheits- und Transparenzstandards zu bemühen, damit das Vertrauen in die direktdemokratischen Prozesse erhalten bleibt.

Wir bitten Sie um Antworten auf die folgenden Fragen:

1. Waren dem Kanton Luzern die von den Forschenden gefundenen Sicherheitslücken bewusst? Falls ja, seit wann, und was hat er dagegen unternommen?
2. Sind dem Kanton Luzern Fälle bekannt, in denen es aufgrund der Sicherheitslücken zu Fehleingaben kam oder die Lücken ausgenutzt wurden?
3. Wie instruiert der Kanton die kommunalen Wahlbehörden für die Anwendung der Software und sensibilisiert sie für Sicherheit und Datenschutz? Ist die kantonale Dienststelle Informatik, der IT-Sicherheitsbeauftragte sowie die Datenschutzstelle einbezogen?
4. Hält es der Kanton für nötig, entsprechende Sicherheits- und Anwendungsstandards in einer Verordnung basierend auf dem Stimmrechtsgesetz festzuschreiben? Was würde sie beinhalten?
5. Jeder Softwareeinsatz bringt Sicherheitsrisiken mit sich, denen mit Schutzzielen begegnet werden muss. Wurden für den Einsatz der Software die Schutzziele definiert und die Informationen gemäss Informatiksicherheitsverordnung (SRL Nr. 26b) klassifiziert? Existiert ein Massnahmenplan zur Erreichung der Schutzziele?
6. Werden geeignete Schutzmassnahmen ergriffen, um unbefugten Zugriff, Missbrauch und Verfälschung der Informationen während des Datenaustausches über Organisationsgrenzen hinweg zu verhindern?
7. Arbeitet der Kanton in der Verbesserung und Weiterentwicklung von elektronischen Prozessen im Bereich Wahlen und Abstimmungen mit anderen Kantonen zusammen, welche die gleiche Software nutzen? Wie sieht diese Zusammenarbeit aus?
8. Nach welchen Kriterien wählt und überprüft der Kanton Luzern die Software für die Ermittlung von Wahl- und Abstimmungsergebnissen, insbesondere hinsichtlich Sicherheit?
9. Wird der Kanton bei zukünftigen Ausschreibungen für die Wahl- und Abstimmungssoftware die Offenlegung des Software-Quellcodes einfordern?

Estermann Rahel
Meyer Jörg
Bucher Philipp
Thalmann-Bieri Vroni
Meier Anja
Stutz Hans
Budmiger Marcel
Engler Pia
Schnider-Schnider Gabriela
Schuler Josef
Zeier Maurus
Koch Hannes
Heeb Jonas
Cozzio Mario
Wimmer-Lötscher Marianne
Arnold Valentin
Bucher Noëlle
Fässler Peter
Ledergerber Michael
Candan Hasan