Motion betreffend Stoppen des Projekts "Ausdehnung von E-Voting" | 18.5416.01

Der Grosse Rat des Kantons Basel-Stadt hat am 18. Oktober 2017 dem Ratschlag betreffend Ausdehnung E-Voting auf Stimmberechtigte mit Wohnsitz im Kanton Basel-Stadt zugestimmt und Mittel in der Höhe von Fr. 5'900'000 bewilligt. Gemäss Ratschlag sollen ab 2019 alle drei Stimmkanäle (elektronische, briefliche und persönliche Stimmabgabe) 100% der im Kanton Basel-Stadt Stimmberechtigten zur Verfügung stehen. Der Kanton hat sich für das System der Schweizerischen Post AG entschieden.

In der Debatte im Grossen Rat haben zahlreiche Votantinnen und Votanten auf die Risiken von E-Voting hingewiesen. Bereits ein Jahr nachdem der Grosse Rat die Einführung beschlossen hat, zeigte der Chaos Computer Club Schweiz (CCC) Anfang November 2018, dass E-Voting unsicher ist. Es wurde am Beispiel des Genfer E-Voting-System demonstriert, wie einfach Stimm- und Wahlberechtigte auf eine gefälschte E-Voting-Website umgeleitet werden können. (Eine verständliche Zusammenfassung hier: https://www.srf.ch/news/schweiz/elektronische-abstimmungen-hacker-findenschwachstelle-im-groessten-schweizer-e-voting-system und https://timogrossenbacher.ch/2018/11/ist-e-voting-in-der-schweiz-sicher/).

Bereits einen Monat später (Ende November 2018) gab der Kanton Genf bekannt, sein E-Voting System im Februar 2020 einzustellen. Begründet wird es mit den hohen Kosten und der Komplexität.

Dass das Projekt eingestellt wird, ist verständlich, denn die vom CCC genutzte Schwachstelle kann nicht so leicht behoben werden. Die Schwachstelle - der konkrete Angriff "DNS Cache Poisoning" - ist systeminhärent und seit längerem bekannt (auch den Betreibern anderer E-Voting-Systeme). Bei DNS-Cache-Poisoning handelt es sich, ähnlich wie bei Phishing, um einen Angriff, der die Gutgläubigkeit, Naivität und technische Ignoranz von Menschen ausnützt. Solches "social engineering" gehört seit Jahrzehnten zu den günstigsten und einfachsten Angriffsmethoden von Hackern.

Befürworter von E-Voting argumentieren, dass der CCC die Attacke nicht zu Ende geführt habe und damit keine Stimmmanipulationen demonstriert habe. Dem Angreifer ist es jedoch gelungen "man in the middle" zu sein und damit hat er so etwas wie einen Generalschlüssel gefunden. Danach braucht es noch das Unwissen des Stimmbürgers und je grösser dieses Unwissen, oder diese Gutgläubigkeit, desto grösser der potenzielle Schaden. Oft werden Prüfcodes als Gegenmassnahme gegen Manipulation genannt. Doch wenn der Angreifer "man in the middle" ist, dann ist auch deren Nutzen beschränkt. Denn der Angreifer kann den Nutzer zu fast allem bewegen, wenn er es geschickt anstellt.

Auch wenn dies nur ein Angriffsszenario war, es hat gezeigt, dass E-Voting nicht sicher ist und dass dadurch das Vertrauen in die direkte Demokratie untergraben wird. Die elektronische Stimmabgabe kann nicht als sicherer und vertrauenswürdiger Stimmkanal ausgebaut werden, denn wenn ein seit Jahrzehnten bekannter Angriff wie DNS-Spoofing nicht verhindert werden kann, so kann E-Voting nicht als sicher gelten.

Die Motionäre fordern den Regierungsrat auf, das Projekt "Ausdehnung E-Voting auf Stimmberechtigte mit Wohnsitz im Kanton Basel-Stadt" baldmöglichst jedoch spätestens innerhalb von 6 Monaten zu stoppen.

Michael Wüthrich, Thomas Grossenbacher, Alexander Gröflin, Aeneas Wanner, Joël Thüring, Sibylle Benz, Olivier Battaglia, Luca Urgese, Tim Cuénod, Erich Bucher