Post sortieren bei der Parlamentswahl 1951: Ein Bild aus der Vergangenheit. Keystone

Warum E-Voting zum Stresstest für die Demokratie werden könnte

In drei Kantonen können Wahlberechtigte wieder online abstimmen. Doch der Zeitpunkt ist schlecht. Das Vertrauen in die staatliche Digitalkompetenz ist angeschlagen.

Von Adrienne Fichter, 10.10.2023

Es ist eine zwanzigjährige Leidensgeschichte. Die Schweiz, das Land mit den weltweit meisten Abstimmungen, versucht seit zwei Dekaden krampfhaft, einen digitalen Stimmkanal einzuführen.

Nun wird seit langem erstmals wieder E-Voting für eine eidgenössische Wahl zugelassen. Die Kantone Basel-Stadt, St. Gallen und Thurgau dürfen bis 2025 mit dem digitalen Stimmkanal experimentieren. Doch die Begeisterung dafür hält sich stark in Grenzen. Der abtretende Bundeskanzler Walter Thurnherr, der das Dossier jahrelang vorangetrieben hatte, erwähnte das Thema in einem kürzlich erschienenen Interview mit keinem einzigen Wort.

Das hat seine Gründe: Denn die Geschichte ist begleitet von Pleiten, Pech und Pannen – und ihr Happy End ist ebenso vorläufig wie trügerisch.

Die bisherige Geschichte geht so: Die Bundeskanzlei – zuständig für Abstimmungen und Wahlen – liess 2003 das Bundesgesetz über die politischen Rechte revidieren. Damit wollte sie E-Voting-Experimente ermöglichen. Der Impuls für das Wählen via Internet ging (und geht bis heute) stark von den Auslandschweizerinnen aus, aber auch von den Behindertenverbänden.

2005 startete der Kanton Neuenburg erste Tests mit dem E-Voting-System der Post, deren Softwarelieferant die umstrittene spanische Firma Scytl war. Und auch ein Konsortium von acht Kantonen – darunter Aargau und Graubünden – experimentierte mit E-Voting, allerdings mit einem anderen System der Firma Unisys.

2015 folgte der erste Rückschlag: Die Bundeskanzlei liess das System des Konsortiums durchfallen. Grund: Es hatte Lücken, aufgrund deren das Stimmgeheimnis nicht gewährleistet werden konnte.

Die Probleme des Monopolisten

Bundeskanzler Walter Thurnherr, der zum E-Voting-Turbo avanciert war, zog danach die Zügel bezüglich IT-Sicherheit an. Weil er wusste, dass anders kaum gegen den Widerstand der digitalen Zivilgesellschaft und von IT-kompetenten Politikern anzukommen ist. Denn: E-Voting birgt massive konzeptionelle und technische Risiken.

– Die konzeptionellen Risiken: Nur wenige Personen sind imstande, die komplexen E-Voting-Systeme zu verstehen und Manipulationen aufzudecken. Die Bürgerin muss darauf vertrauen, dass ihre digitale Stimme nicht manipuliert wird, etwa von einer Mitarbeiterin des Kantons.
– Die technischen Risiken: Die Stimmabgabe erfolgt beim digitalen Wählen und Abstimmen in einem Browser, der mit dem offenen Internet verbunden und damit angreifbar ist. Ein Hack des E-Voting-Systems betrifft nicht nur eine einzige Wahlstimme, sondern potenziell Hunderttausende. Aufgrund des fehlenden Papiers kann keine Nach- oder Neuauszählung der Stimmen stattfinden.

Die Bundeskanzlei verpflichtete deshalb die Anbieter – neben der Offenlegung des Quellcodes – zur Durchführung von sogenannten Bug-Bounty-Programmen (Programme, bei denen jede Meldung von Softwarefehlern und Sicherheitslücken belohnt wird) und Penetrationstests (legale Versuche, ein System von aussen zu hacken).

2019 nahm sich ein weiterer Anbieter aus Kostengründen aus dem Rennen: der Kanton Genf mit seinem selbst entwickelten Open-Source-System.

Es verblieb nur noch die Post, die von da an ein E-Voting-Monopol hatte. Doch auch die von ihr eingesetzte Software war nicht sicher, wie Recherchen der Republik zeigten. Der australische Bundesstaat New South Wales hatte 2015 dieselbe Software wie die Post eingesetzt – und Security-Forscher hatten eine gravierende Lücke im System entdeckt: Die Verschlüsselungen im Browser funktionierten nicht korrekt.

Auch in der Schweiz scheiterte Scytl, der Technologiepartner der Post, 2019 am Realitycheck: Die kanadische Security-Forscherin Sarah Jamie Lewis und ihr Team fanden während der Testphase zwei empfindliche Sicherheitslücken. Ihr Verdikt war vernichtend: «Die Protokolle sind meiner Meinung nach mit fehlendem Verständnis der Kryptografie implementiert worden, kombiniert mit schlampiger Programmierung.»

Die Post zog darauf ihr System zurück.

Und die Politik drückte den Reset-Knopf.

2020 nahm das Parlament einen zweiten Anlauf und arbeitete neue Rechtsgrundlagen für einen weiteren E-Voting-Versuchsbetrieb aus. Nur noch unabhängig geprüfte und vollständig verifizierbare Systeme sollen zugelassen werden. Das bedeutet: Sowohl die wählenden Bürger als auch die vom Kanton mandatierten Prüferinnen müssen feststellen können, ob die im Internet abgegebene Stimme korrekt in der digitalen Urne eingetroffen ist. E-Voting ist ausserdem nur für maximal 30 Prozent der Stimmberechtigten zugelassen. Die Kantone schielen dabei vor allem auf die Auslandschweizer.

Die Post hat in der Zwischenzeit ihre Hausaufgaben gemacht. Sie kaufte den Quellcode ihres Lieferanten Scytl, entwickelte ihn weiter und bestand bisher alle Sicherheitstests. Die Post verfügt nun über ein permanentes Bug-Bounty-Programm, 2022 nahmen 3400 Personen daran teil. Die Bundeskanzlei war zufrieden: «Ein Eindringen in die Infrastruktur oder in die elektronische Urne ist nicht gelungen.» Im Juni 2023 haben 4239 Stimmberechtigte in Basel-Stadt, St. Gallen und Thurgau elektronisch abgestimmt. Die Post scheint den grossen Check des Bundes bestanden zu haben.

Das aktuelle E-Voting-System erweist sich also vorerst als robust. Nun können 65'000 Stimmberechtigte (1,2 Prozent des Elektorats) bis 2025 via Internet wählen und abstimmen. Ende gut, alles gut?

So einfach ist es leider nicht.

Verantwortung an Bürger abgeschoben

Die Bundeskanzlei sowie die Kantone legten im Sommer 2023 umfassende Risikobeurteilungen vor, die von den Medien kaum beachtet wurden.

Der Techjournalismus-Blog «dnip.ch» aber analysierte die Berichte – und kam zum Schluss: Trotz aller technischer Fortschritte existiert immer noch eine Vielzahl von Risiken. Sie werden von Bund und Kantonen einfach entweder mit Massnahmen bewältigt (mehr Transparenz, mehr Dokumentation) – oder kleingeredet. Ein mögliches Risiko könnte zum Beispiel eine Situation darstellen, in der die Resultate der Papierstimmen massiv von denen der digitalen Stimmen abweichen. Denn das könnte das Vertrauen in den elektronischen Stimmkanal mindern. Die Kantone scheinen dieses Szenario als unwahrscheinlich einzuschätzen. Denn: Bisher sei dieses Phänomen noch nie aufgetreten.

Aber wird etwas auch in Zukunft nicht passieren, nur weil es noch nie eingetreten ist?

Die Bundeskanzlei wälzt den Grossteil der Verantwortung für korrektes digitales Abstimmen auf die Bürgerinnen ab. Diese müssen nicht nur anhand der Codes genau überprüfen, ob ihre Stimme korrekt übermittelt wurde, sondern darüber hinaus einige IT-Skills mitbringen: Wähler müssen anhand von Webserver-Zertifikaten erkennen, ob sie mit dem richtigen E-Voting-Server verbunden sind, über virenfreie digitale Endgeräte verfügen und neue Software-Updates laden (wie einfach ein Angriff hierbei passieren kann, demonstrierte soeben der Informatiker Andreas Kuster). Und sie dürfen auf keine Desinformationskampagnen von ausländischen Hackerinnen reinfallen, niemals verdächtige Browser-Erweiterungen installieren und schon gar nicht auf dubiose Links klicken. Und sollte ein Bürger selber Unstimmigkeiten bemerken, muss er von sich aus aktiv werden und sich bei der zuständigen Stelle des Kantons melden.

Liest man all die Anforderungen durch, kommt man zum Schluss: Am besten würde der Staat die Schweizer Stimmbevölkerung einen einwöchigen Cyberkurs absolvieren lassen.

Die beste Sicherheitsmassnahme ist daher die bereits angesprochene verbindliche Vorgabe der Verordnung, dass nur ein beschränkter Teil der Wählerschaft für E-Voting zugelassen werden darf. Salopp gesagt: Sollte bei der Post etwas schiefgehen, kommt es auf die verlorenen Stimmen nicht allzu sehr an.

Doch auch das ist zu kurz gedacht: Zuweilen können wenige hundert Stimmen den Ausschlag geben. Der Blog «dnip.ch» nennt sinngemäss unter anderem folgende zentrale Fragen, die für politischen Sprengstoff sorgen könnten: Wie gross ist die Hürde bei einer Manipulation elektronisch abgegebener Stimmen, um eine Abstimmung zu wiederholen? Und was machen die Behörden, wenn die Verlierer die Resultate wegen des E-Votings anzweifeln?

Müdigkeitserscheinungen bei kritischen Geistern

Die Wiederzulassung des E-Votings könnte zum Stresstest der Demokratie werden. Denn das Timing ist schlecht:

Erstens gibt es seit der Corona-Pandemie eine laute politikverdrossene und staatsskeptische Minderheit, die sich eine digitale Öffentlichkeit auf Messenger-Apps wie Telegram aufgebaut hat. Sie könnte E-Voting-Ergebnisse systematisch anzweifeln und damit – sollte einmal ein schwerer Fehler gefunden werden – eine Demokratie-Krise auslösen.

Zweitens wird die Schweiz zurzeit von einer Cyberattacke nach der anderen eingeholt. Fairerweise muss man sagen, dass es sich bei vielen der staatlichen IT-Desaster um Altlasten aus den 2000er- und frühen 2010er-Jahren handelt, etwa beim Beschaffungsskandal rund um die Firma Xplain oder beim mittlerweile vom Netz genommenen elektronischen Impfbüchlein Meineimpfungen.ch. Trotzdem mindert jede negative Schlagzeile das Vertrauen in staatliche Digitalprojekte.

Drittens birgt auch das Versagen privater Systeme Gefahren fürs E-Voting: So sind die Postadressen von 425'000 Auslandschweizerinnen im Darknet auffindbar, weil eine Druckerei des Medienkonzerns CH Media von der Ransomware-Gruppe Play gehackt worden war. Es wäre für Hackergruppen ein Leichtes, diese Adressen herunterzuladen, anzuschreiben und sie damit auf eine manipulierte E-Voting-Seite ihres Kantons zu locken.

Und viertens lässt die Wachsamkeit nach. Nach zwanzig Jahren Debatte lassen sich Ermüdungserscheinungen in der hiesigen Informatikerinnen-Szene beobachten. Das «Swiss IT Magazine» kritisierte zu Recht, dass sich Schweizer IT-Verbände bei der Vernehmlassung zur Revision der E-Voting-Verordnung kaum mit den technischen Anhängen auseinandergesetzt hatten. Inputs zu Schwachstellen kamen stattdessen von ethischen Hackern aus der ganzen Welt. Die Begleitung von E-Voting braucht jedoch permanente Aufmerksamkeit, denn die Gefahrenlage im Netz verändert sich stets.

Ein Grundsatzentscheid sollte her

Die lange Geschichte des E-Votings hat aber auch ihr Gutes. In all den Jahren ist ein neues politisches Bewusstsein rund um Softwareentwicklungen der öffentlichen Hand entstanden. Öffentliche Sicherheitsprüfungen und Transparenz beim Quellcode werden beim Bund immer mehr zum State of the Art. Und zum Vorbild für weitere Projekte wie die Swiss-Covid-App.

Es wäre wünschenswert, würden diese Standards auf alle IT-relevanten Bereiche des Wählens ausgeweitet, etwa auch auf Systeme zur Ermittlung von Wahlresultaten (die die Zuteilung der Sitze an die Parteien berechnen). Doch Wahlen sind Sache der Kantone. Und diese haben die Hoheit über ihre IT-Systeme. 2020 deckte die Republik Sicherheitslücken in Software zur Ermittlung von Wahlergebnissen auf, die in der Folge behoben wurden. Die Kantone verlangen jedoch keine öffentlichen Sicherheitstests wie beim E-Voting, was insbesondere die Piratenpartei kritisiert.

Die Prioritätenliste der Schweizer Bundespolitik in Sachen Digitalisierung ist für langjährige Beobachter schwer nachvollziehbar. Weshalb wird mit E-Voting ausgerechnet die risikoreichste Form der Digitalisierung forciert, von der namhafte Cybersecurity-Expertinnen aus aller Welt immer wieder abraten? Die Schweiz hätte die vergangenen zwanzig Jahre dazu nutzen können, Demokratie-Innovationen zu fördern, mit denen Städte, Kantone und Zivilgesellschaft bereits Pilotprojekte durchführen: für ein partizipatives Budget (Luzern, Lausanne), digitale Unterschriftensammlungen (Schaffhausen) oder ein digitales Vernehmlassungstool («Demokratis») etwa.

Es wäre gut, könnte die Schweizer Stimmbevölkerung bald einen Grundsatzentscheid zum E-Voting fällen. Bisher haben Befürworter die Legitimität von E-Voting mit Umfragewerten begründet. Eine breite Allianz hatte 2020 einen erfolglosen Versuch unternommen, mit einer Volksinitiative ein Moratorium von E-Voting zu erreichen. Dennoch würde ein neuer Versuch Klarheit über den Volkswillen schaffen. Und damit endlich auch eine landesweite Debatte über alle Aspekte wie Sicherheit und politische Teilhabe ermöglichen, wie sie vor zwei Jahren bei der E-ID-Abstimmung geführt wurde.

Transparenzhinweis: Die Autorin ist Mit-Herausgeberin von dnip.ch.

Sie wollen mehr Informationen zu den Wahlen?

In unserem Dossier finden Sie Analysen, Porträts und Interviews, die Ihnen Argumente für Ihre Wahlentscheidung liefern können.