Sicherheit und Vertrauenswürdigkeit von Wahlen und Abstimmungen im digitalen Umfeld

Bericht der Regierung vom 20. Januar 2026

Inhaltsverzeichnis

Zusammenfassung

Die öffentliche Hand steht vor der Herausforderung, die Sicherheit und Vertrauenswürdigkeit von Wahlen und Abstimmungen in einem digitalen Umfeld zu gewährleisten. Dies geht weit über die elektronische Stimmabgabe (E-Voting) hinaus. So basieren heute wesentliche Teile der Vorbereitung und Durchführung von Wahlen und Abstimmungen im Kanton St.Gallen auf dem Einsatz von Computern und digitalen Services.

Mit der Gutheissung des Postulats 43.19.09 «Sicherheit und Vertrauenswürdigkeit von Wahlen und Abstimmungen im digitalen Umfeld» hat der Kantonsrat die Regierung in der Septembersession 2019 eingeladen, Bericht zu erstatten über die Risiken für die Sicherheit und Vertrauenswürdigkeit von Wahlen und Abstimmungen durch den Einsatz von digitalen Services (E-Services), wie namentlich E-Voting, E-Counting und elektronische Ergebnisermittlung, und darin die bestehenden sowie weitere mögliche Sicherheitsmassnahmen darzulegen. Mit dem vorliegenden Bericht, in dem der Themenkomplex der Sicherheit und Vertrauenswürdigkeit von Wahlen und Abstimmungen aus unterschiedlichen Perspektiven beleuchtet wird, liegt nun eine umfassende Auslegeordnung vor.

Der erste Hauptabschnitt orientiert sich am chronologischen Ablauf von Wahlen und Abstimmungen, wobei jede Phase der Vorbereitung und Durchführung von IT-Sicherheitsexperten des Instituts für Informatik der Universität Zürich (UZH) einzeln auf potenzielle Bedrohungen hin analysiert wurde. Zur Eindämmung der identifizierten Bedrohungen werden anschliessend mögliche Gegenmassnahmen aufgezeigt, wobei unterschieden wird zwischen Massnahmen, die bereits umgesetzt sind, und möglichen weiterführenden Massnahmen.

Der Fokus im zweiten Hauptabschnitt liegt auf den Erkenntnissen und Erfahrungen, die der Kanton St.Gallen im Rahmen der Pilotversuche mit E-Voting gesammelt hat, sowie auf deren Übertragbarkeit auf andere digitale Services im Bereich der politischen Rechte. So haben die Kantone St.Gallen und Thurgau aufgrund ihrer Erfahrungen mit der elektronischen Stimmabgabe (Stichwort: «Sicherheit durch Transparenz») beispielsweise gemeinsam entschieden, den Quellcode ihres neuen Ergebnisermittlungssystems für Wahlen und Abstimmungen offenzulegen und dieses einem unbefristeten Bug-Bounty-Programm zu unterstellen.

Im dritten Hauptabschnitt werden schliesslich organisatorische Herausforderungen thematisiert, welche die Vorbereitung und Durchführung von Wahlen und Abstimmungen mit sich bringen kann und die – wie etwa die Wahlfälschung bei den Thurgauer Grossratswahlen im März 2020 («Fall Frauenfeld») gezeigt hat – ebenfalls das Potenzial haben, das Vertrauen in den Wahl- und Abstimmungsprozess zu schädigen. Der Fokus geht dabei bewusst über Bedrohungen, die sich aus dem Einsatz von Computern und digitalen Services ergeben können, hinaus und berücksichtigt auch zentrale Aspekte wie die sichere Lagerung von Stimmmaterial vor und nach einem Urnengang oder den Umgang mit Reservematerial.

Zusammenfassend lässt sich festhalten, dass nicht nur eine ganze Reihe an potenziellen Bedrohungen identifiziert werden konnte, die das Potenzial haben, die ordnungsgemässe Durchführung einer Wahl oder Abstimmung zu beeinträchtigen, es wird auch aufgezeigt, dass zur Eindämmung vieler dieser Bedrohungen bereits wirkungsvolle Gegenmassnahmen bestehen. Darüber hinaus konnten insbesondere im Zuge der Entwicklung und Einführung des neuen Ergebnisermittlungssystems für Wahlen und Abstimmungen zahlreiche Empfehlungen aus der Bedrohungsanalyse der Universität Zürich ebenso wie «best practices» aus den Erfahrungen mit der elektronischen Stimmabgabe direkt umgesetzt werden. Insgesamt sind die Sicherheit und die Vertrauenswürdigkeit der Wahlen und Abstimmungen im Kanton St.Gallen aus Sicht der Regierung bereits auf einem sehr guten Stand.

Allerdings gibt es keine hundertprozentige Sicherheit, weder mit Blick auf den Einsatz von digitalen Services noch im Fall der papierbasierten Verfahrensschritte und organisatorischen Prozesse im Rahmen der Vorbereitung und Durchführung von Wahlen und Abstimmungen. Deshalb werden im Fazit des vorliegenden Berichts verschiedene mögliche Massnahmen in Aussicht genommen, mit denen die Sicherheit und die Vertrauenswürdigkeit weiter gestärkt werden könnten. Diese betreffen insbesondere die beiden Bereiche, die aus einer risikobasierten Perspektive betrachtet als besonders sensitiv gelten müssen: die Manipulationssicherheit der Stimmrechtsausweise (da ohne diese keine gültigen Stimmen abgegeben werden können) sowie die sichere Lagerung des Stimmmaterials, namentlich bei den Gemeinden.

Herr Präsident
Sehr geehrte Damen und Herren

Wir erstatten Ihnen mit dieser Vorlage Bericht zum Postulat 43.19.09 «Sicherheit und Vertrauenswürdigkeit von Wahlen und Abstimmungen im digitalen Umfeld».

1 Ausgangslage

1.1 Auftrag des Kantonsrates

In der Aprilsession 2019 des Kantonsrates reichten die FDP-Fraktion und die damalige CVP-GLP-Fraktion das Postulat 43.19.09 «Sicherheit und Vertrauenswürdigkeit von Wahlen und Abstimmungen im digitalen Umfeld» ein. Die Regierung stellte am 14. Mai 2019 einen Antrag auf Gutheissung des Postulats. In der Septembersession 2019 hiess der Kantonsrat das Postulat mit 109 Ja- zu einer Nein-Stimme bei einer Enthaltung und 9 Abwesenheiten gut.

Die lange Zeitspanne zwischen Gutheissung des Postulats und Zuleitung des vorliegenden Berichts ist auf unterschiedliche Gründe zurückzuführen. Insbesondere galt es, die Offenlegung des Quellcodes des neuen Ergebnisermittlungssystems für Wahlen und Abstimmungen im Rahmen eines Bug-Bounty-Programms sowie den Wahlzyklus 2023/2024 abzuwarten. Zudem wurde aufgrund des ebenfalls hängigen parlamentarischen Auftrags das Projekt zur Einführung E-Collecting priorisiert. Die Regierung erläuterte dies jeweils in den Berichten zum Stand der Bearbeitung der gutgeheissenen parlamentarischen Vorstösse. In diesem Zusammenhang verlängerte der Kantonsrat die Frist für die Zuleitung des Berichts bis Januar 2026 (32.25.01A).

Mit der nun erfolgten Berücksichtigung der jüngsten Entwicklungen kann dem Kantonsrat eine umfassende Auslegeordnung zu den Risiken für die Sicherheit und Vertrauenswürdigkeit von Wahlen und Abstimmungen, die sich durch den Einsatz von digitalen Services (E-Services) ergeben, vorgelegt werden. Dabei wird aufgezeigt, mit welchen Sicherheitsmassnahmen diese Risiken bereits heute reduziert werden oder in Zukunft weiter gemindert werden könnten.

1.2 Wahlen und Abstimmungen in einem digitalen Umfeld

Die öffentliche Hand steht vor der Herausforderung, die Sicherheit und Vertrauenswürdigkeit von Wahlen und Abstimmungen in einem digitalen Umfeld zu gewährleisten, das weit über die elektronische Stimmabgabe (E-Voting) hinaus geht. So basieren heute wesentliche Teil der Vorbereitung und Durchführung von Wahlen und Abstimmungen auf dem Einsatz von Computern und digitalen Services, angefangen bei den Stimmregistern über die Aufbereitung und den Druck des Stimmmaterials bis hin zur Auszählung der Stimmen in den Gemeinden, der Zusammenführung des Ergebnisses auf kantonaler Ebene und dessen Übermittlung an den Bund.

Die Sicherheit und Vertrauenswürdigkeit von Wahlen und Abstimmungen in einem digitalen Umfeld setzt deshalb in Bezug auf jeden der eingesetzten Services angemessene Sicherheitsmassnahmen voraus.

2 Herangehensweise und Aufbau des Berichts

Der vorliegende Bericht ist in drei Hauptabschnitte gegliedert, in denen der Themenkomplex der Sicherheit und Vertrauenswürdigkeit von Wahlen und Abstimmungen aus unterschiedlichen Perspektiven beleuchtet wird. Die Ausführungen in Abschnitt 3 orientieren sich am chronologischen Ablauf von Wahlen und Abstimmungen im Kanton St.Gallen. Der Fokus liegt dabei schwergewichtig auf möglichen Bedrohungen, die sich aus dem Einsatz von Computern und digitalen Services ergeben können und die das Potenzial haben, die ordnungsgemässe Vorbereitung und Durchführung ebendieser Wahlen oder Abstimmungen zu beeinträchtigen.

Als Grundlage für die Ausführungen in Abschnitt 3 dient eine umfassende Bedrohungsanalyse des gesamten Prozesses der Vorbereitung und Durchführung von Wahlen und Abstimmungen, die das Institut für Informatik der Universität Zürich (UZH) zwischen Oktober 2021 und Juli 2022

im Auftrag der Staatskanzlei erstellt hat.[1] Darin wird jede Phase der Vorbereitung und Durchführung (für einen Überblick siehe Abschnitt 3.1) einzeln auf potenzielle Bedrohungen hin analysiert. Anschliessend werden mögliche Gegenmassnahmen zur Mässigung oder Eindämmung der identifizierten Bedrohungen aufgezeigt, wobei unterschieden wird zwischen Massnahmen, die bereits umgesetzt sind, und möglichen weiterführenden Massnahmen.

Da im Kanton St.Gallen verschiedene digitale Services im Bereich der politischen Rechte im gleichen Zeitraum geplant und umgesetzt wurden, in dem die UZH ihre Bedrohungsanalyse durchführte – namentlich das neue Ergebnisermittlungssystem für Wahlen und Abstimmungen, das im Rahmen der Ersatzwahl eines st.gallischen Mitglieds des Ständerates am 12. März 2023 erstmals produktiv zum Einsatz kam –, sind diverse Erkenntnisse aus der Analyse der UZH (diese findet sich im Anhang ganz am Ende dieses Berichts) direkt in die Entwicklung der betreffenden Services miteingeflossen.

In den Abschnitten 4 und 5 wird anschliessend auf zwei Aspekte, die in den Ausführungen in Abschnitt 3 bereits kurz angeschnitten, aber nicht vertieft behandelt wurden, gesondert eingegangen. Der Fokus in Abschnitt 4 liegt dabei auf den Erkenntnissen und Erfahrungen, die der Kanton St.Gallen im Rahmen der Pilotversuche mit der elektronischen Stimmabgabe (E-Voting) gesammelt hat sowie auf deren Übertragbarkeit auf andere digitale Services im Bereich der politischen Rechte.

Bereits seit dem Jahr 2009 bietet der Kanton St.Gallen einem Teil seiner Stimmberechtigten die Möglichkeit, ihre Stimmen elektronisch abzugeben. Im Zusammenspiel mit den anderen E-Voting-Kantonen (Basel-Stadt, Thurgau sowie seit 2024 auch Graubünden), der Bundeskanzlei, der Wissenschaft sowie der Schweizerischen Post als Anbieterin des aktuell einzigen E-Voting-Systems in der Schweiz haben sich über die Jahre verschiedene Erkenntnisse und «best practices» herauskristallisiert. Wie in Abschnitt 4.6 aufgezeigt wird, ist es sinnvoll, diese – zumindest bis zu einem gewissen Grad – auch auf andere digitale Services im Bereich der politischen Rechte anzuwenden (Stichwort: *Sicherheit durch Transparenz*). So haben die Kantone St.Gallen und Thurgau etwa gemeinsam entschieden, den Quellcode ihres neuen Ergebnisermittlungssystems für Wahlen und Abstimmungen offenzulegen und dieses einem unbefristeten Bug-Bounty-Programm zu unterstellen.

In Abschnitt 5 wird zudem vertiefter auf *organisatorische* Herausforderungen eingegangen, welche die Vorbereitung und Durchführung von Wahlen und Abstimmungen mit sich bringen können und die – wie beispielsweise die Wahlfälschung bei den Thurgauer Grossratswahlen im März 2020 («Fall Frauenfeld») oder die Panne bei der Auszählung der Wahl des St.Galler Stadtparlamentes am 22. September 2024 gezeigt haben – ebenfalls das Potenzial haben, das Vertrauen in den Wahl- und Abstimmungsprozess bzw. in dessen korrekte Durchführung, zu schädigen. Der Fokus von Abschnitt 5 geht damit bewusst über Bedrohungen, die sich aus dem Einsatz von Computern und digitalen Services ergeben können, hinaus und berücksichtigt auch zentrale Aspekte wie beispielsweise die sichere Lagerung von Stimmmaterial vor und nach einem Urnengang.

Nicht vertieft eingegangen wird im Rahmen des vorliegenden Berichts hingegen auf allgemeine «Gefahren», die der Einsatz von Computern mit sich bringt (siehe zu diesem Punkt auch Abschnitt 3.1). Ebenfalls nicht Bestandteil des Berichts ist das Sammeln von elektronischen Unterschriften zur Unterstützung von Volksinitiativen oder Referendumsbegehren (E-Collecting). Letzteres findet sowohl zeitlich als auch thematisch ausserhalb der hier beschriebenen Prozesse statt und hat mit Wahlen und Abstimmungen nur am Rande zu tun – dann nämlich, wenn

[1] Da die Prozesse bei eidgenössischen, kantonalen und kommunalen Wahlen und Abstimmungen weitgehend identisch sind, beziehen sich die Ausführungen im vorliegenden Bericht grundsätzlich auf alle drei föderalen Ebenen. Auf Besonderheiten einzelner Prozesse wird soweit nötig hingewiesen.

nach Abschluss der parlamentarischen Behandlung an der Urne über ein zustande gekommenes Volksbegehren abgestimmt werden muss.

In Abschnitt 6 werden die Erkenntnisse und Empfehlungen aus den Abschnitten 3 bis 5 zusammengeführt und es werden die weiterführenden Massnahmen definiert, welche die Regierung konkret umzusetzen oder zu prüfen beabsichtigt und mit denen die Sicherheit und die Vertrauenswürdigkeit der Wahlen und Abstimmungen im Kanton St.Gallen weiter gestärkt werden können.

3 Chronologischer Ablauf von Wahlen und Abstimmungen: Bedrohungen und Gegenmassnahmen

3.1 Prozessübersicht

Zum Zweck der Übersichtlichkeit sowie der besseren Nachvollziehbarkeit wird der Prozess der Vorbereitung und Durchführung von Wahlen und Abstimmungen im Kanton St.Gallen in sieben aufeinanderfolgende Phasen unterteilt.[2] Innerhalb jeder dieser Phasen gibt es verschiedene Arbeitsschritte, die von unterschiedlichen Beteiligten in Auftrag gegeben und ausgeführt werden (siehe Abbildung 1 und dazugehörige Legende). Die beteiligten Personen stellen gleichzeitig auch die Sicherheit und Vertrauenswürdigkeit des jeweiligen Prozessschritts sicher.

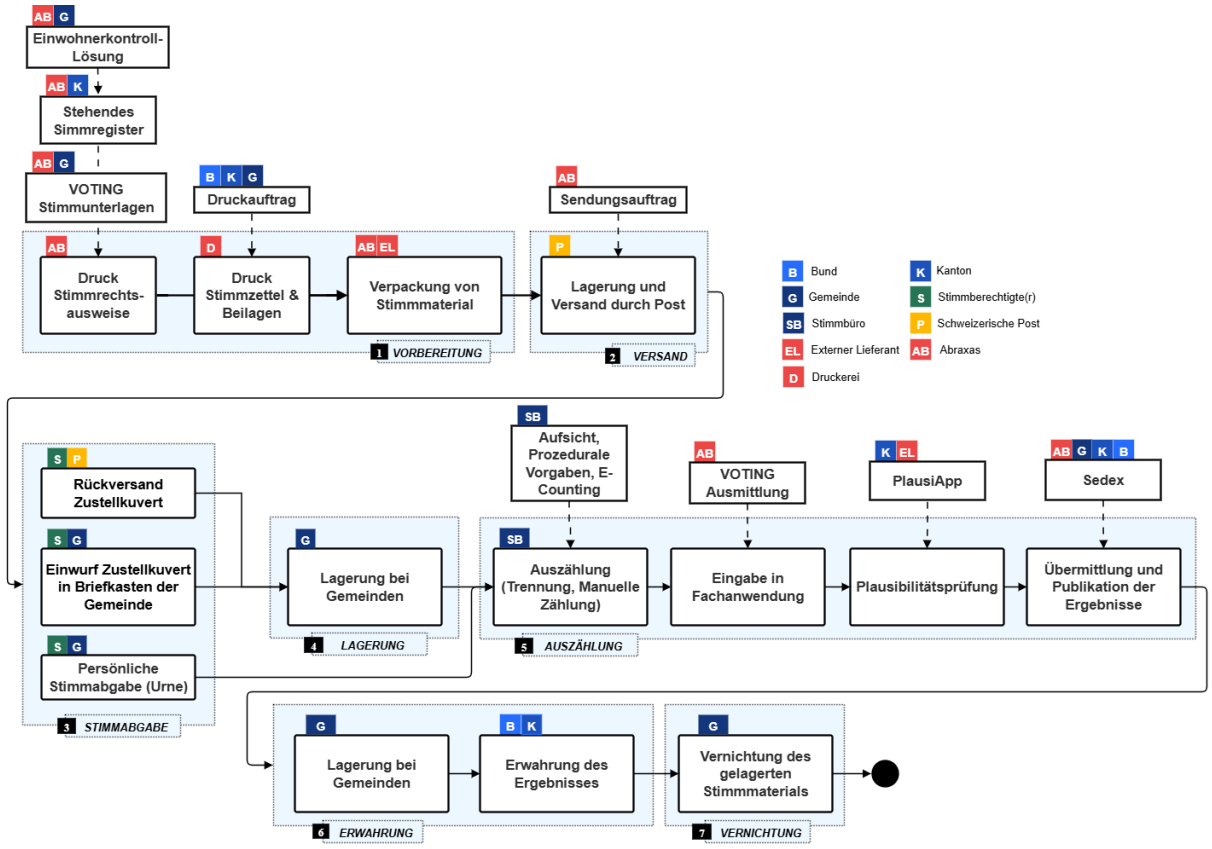

Abbildung 1: Phasen der Vorbereitung und Durchführung von Wahlen und Abstimmungen (Quelle: UZH)

[2] Diese Einteilung geht zurück auf den im Jahr 2019 veröffentlichten Artikel «The Swiss Postal Voting Process and its System and Security Analysis» von Christian Killer und Burkhard Stiller (abrufbar unter www.researchgate.net/publication/335997715_The_Swiss_Postal_Voting_Process_and_Its_System_and_Security_Analysis). Beide sind Mitverfasser der in Abschnitt 3 diskutierten Bedrohungsanalyse der UZH.

– **Phase Vorbereitung:** Die erste Phase umfasst den Druck des Stimmmaterials (also der Stimmrechtsausweise, der Stimmzettel sowie weiterer Beilagen), der in der Regel zwei bis drei Monate vor dem Urnengang erfolgt.

– **Phase Versand:** Während der zweiten Phase wird das Stimmmaterial verpackt und der Post übergeben. Diese stellt die sichere Zwischenlagerung bis zum Beginn des gesetzlich reglementierten Zeitfensters sicher, während dem das Stimmmaterial ausgeliefert werden darf, und stellt es anschliessend den Stimmberechtigten zu.

– **Phase Stimmabgabe:** Nachdem sie das Stimmmaterial erhalten haben, geben die Stimmberechtigten in der dritten Phase ihre Stimmen ab. Dabei ist es ihnen freigestellt, ob sie dies an der Urne tun, auf dem postalischen Weg oder mittels E-Voting (in den Gemeinden, in denen dies bereits möglich ist)[3].

– **Phase Lagerung:** Nach dem Eingang der brieflichen Stimmabgaben werden die Zustellkuverts in der jeweiligen Gemeinde bis zum Abstimmungswochenende sicher und verschlossen aufbewahrt (vierte Phase).

– **Phase Auszählung:** Die fünfte Phase beginnt am Wahl- oder Abstimmungswochenende mit der Öffnung der Zustellkuverts. Zuerst werden die Stimmrechtsausweise durch die Mitglieder des Stimmbüros geprüft, anschliessend werden die Stimmzettelkuverts geöffnet und die Stimmzettel ausgezählt. Die ermittelten Werte – also das Teilergebnis der betreffenden Gemeinde – werden anschliessend im Ergebnisermittlungssystem elektronisch erfasst und von der Staatskanzlei plausibilisiert. Letztere trägt die Teilergebnisse aller Gemeinden dann zusammen und veröffentlicht anschliessend das kantonale Endergebnis.

– **Phase Erwahrung:** Nach der Publikation der Ergebnisse werden Stimmzettel und Stimmrechtsausweise vom Stimmbüro verpackt und versiegelt. Das Stimmmaterial wird anschliessend von der jeweiligen Gemeinde bis zur Erwahrung durch den Bundesrat (bei eidgenössischen Abstimmungen) oder den neu gewählten Nationalrat (bei den Nationalratswahlen) bzw. durch die Regierung des Kantons St.Gallen (bei kantonalen Wahlen und Abstimmungen) sicher aufbewahrt (sechste Phase). Im Fall der Nationalratswahlen wird zudem der Abschluss der Bereinigungsarbeiten im Bundesamt für Statistik (BFS) abgewartet.

– **Phase Vernichtung:** In der siebten und letzten Phase erfolgt die Vernichtung des Stimmmaterials, nachdem das Ergebnis der betreffenden Wahl oder Abstimmung rechtmässig erwahrt wurde. Im Fall von kantonalen Vorlagen findet die Erwahrung in der Regel einen Monat nach dem Urnengang statt. Im Fall von eidgenössischen Abstimmungen kann es mehrere Monate dauern, bis der Bundesrat die Ergebnisse erwahren kann.

In den nachfolgenden Abschnitten 3.2 bis 3.8 werden die aktuell erkennbaren, potenziellen Bedrohungen für den Wahl- und Abstimmungsprozess im Kanton St.Gallen beschrieben. Wie eingangs erwähnt, stützen sich die Ausführungen auf die Bedrohungsanalyse, welche die UZH zwischen Oktober 2021 und Juli 2022 im Auftrag der Staatskanzlei durchgeführt hat. Die Beschreibungen der identifizierten Bedrohungen und namentlich auch der Gegenmassnahmen zu deren Eindämmung wurden bei der Erarbeitung dieses Berichts teilweise gekürzt und an verschiedenen Stellen aktualisiert. Letzteres wurde notwendig, da ein Teil der elektronischen Systeme, deren Einsatz von der UZH analysiert wurde, unterdessen durch modernere Services abgelöst wurden. Dabei sind verschiedene Erkenntnisse aus der Bedrohungsanalyse wie ebenfalls bereits erwähnt in die Entwicklung dieser Services eingeflossen. Die im Folgenden präsentierte Systemlandschaft entspricht somit dem aktuellen Stand im Winter 2025/2026.

[3] Sofern nicht ausdrücklich anders bezeichnet, sind mit «Gemeinden» nachfolgend jeweils die politischen Gemeinden gemeint.

Die nachfolgend beschriebenen Bedrohungen sind anhand der oben skizzierten sieben Phasen strukturiert und bewusst *nicht* allgemeiner Natur.[4] Vielmehr wurden sie von den Experten der UZH für die spezifischen Arbeitsschritte während der jeweiligen Phase als relevant eingestuft. Dies ist wichtig, damit auch spezifische Gegenmassnahmen formuliert werden können, welche die betreffenden Prozesse bzw. deren Schwächen explizit adressieren. Für die Beschreibung der identifizierten Bedrohungen wird so weit als möglich auf Begriffe aus der sicherheitstechnischen Fachsprache verzichtet. Die beiden zentralen Begriffe der «Bedrohung» und der «Skalierbarkeit» werden in der Analyse der UZH wie folgt definiert (S. 3; Zitat leicht gekürzt):

> *Eine Bedrohung ergibt sich durch die (realistische) Möglichkeit, durch böswilliges Einwirken Schaden auf Schutzziele wie die Vertrauenswürdigkeit, die Integrität oder die Verfügbarkeit eines digitalen Informationssystems oder einen durch Menschen behandelten Prozess zu erreichen. In diesem Kontext muss ein Angreifer einen spezifischen Angriffspfad auswählen. Unter der Skalierbarkeit eines Angriffs wird dann eine Einschätzung des benötigten Aufwands aus Sicht des Angreifers verstanden.*

3.2 Phase Vorbereitung

3.2.1 Einführung und Übersicht über Arbeitsschritte

Die Phase Vorbereitung steht ganz am Anfang des Wahl- und Abstimmungsprozesses und umfasst drei Arbeitsschritte: die Aufbereitung und den Druck der Stimmrechtsausweise, den Druck der Stimmzettel und weiterer Beilagen sowie die Verpackung des Stimmmaterials. Anschliessend wird das Stimmmaterial zum Versand an die Stimmberechtigten an die Post übergeben.

Im Rahmen der Aufbereitung der Stimmrechtsausweise kommen verschiedene Systeme und Services zum Einsatz (siehe auch Abbildung 2). Aus der jeweiligen Einwohnerkontroll-Lösung der Gemeinde werden jede Nacht automatisch die für die Stimmrechtsausweise benötigten Daten der Stimmberechtigten an das stehende Stimmregister der Staatskanzlei übermittelt. Dieses ist mit dem Service *VOTING Stimmunterlagen* verbunden, über den die Gemeinden ihre Bestellung des eidgenössischen und kantonalen Stimmmaterials erfassen, allfälliges kommunales Stimmmaterial für die Verpackung anmelden und mit Hilfe von standardisierten Templates die Druckdateien für ihre Stimmrechtsausweise generieren. Diese Druckdateien werden anschliessend über den verschlüsselten kantonalen Datentransfer *(CONNECT SG)* an das Druck- und Verpackungszentrum der Abraxas (DVZ) oder – falls eine Gemeinde ihre Stimmrechtsausweise bei einem anderen Anbieter drucken lassen will – an ein von der Gemeinde bezeichnetes und an *CONNECT SG* angebundenes Datenverzeichnis übermittelt.

Da für die Aufbereitung der E-Voting-Stimmrechtsausweise besondere Sicherheitsvorgaben gelten (siehe Abschnitt 4.4.2), wurde für deren Übermittlung ein komplexerer Prozess definiert, der asymmetrische Verschlüsselung und Offline-Geräte kombiniert. Für die Übermittlung der Druckdaten ans DVZ wird ebenfalls *CONNECT SG* verwendet, im DVZ kommt für die E-Voting-Stimmrechtsausweise jedoch eine gesonderte Druckstrasse zum Einsatz. Da diese vollständig offline betrieben werden muss, werden die Druckdaten mit Hilfe eines separaten USB-Sticks eingelesen.[5]

---

[4] Auf allgemeine Bedrohungen für Informationssysteme wie Phishing, Ransomware- oder DDoS-Angriffe wird in diesem Bericht nicht vertiefter eingegangen. Ein summarischer Überblick findet sich in Abschnitt 4 der Analyse der UZH im Anhang.

[5] Der sichere Umgang mit USB-Sticks ist unter Ziff. 13.3 im Anhang zur Verordnung der Bundeskanzlei über die elektronische Stimmabgabe (SR 161.116; abgekürzt VEleS) verbindlich geregelt. Die Bundeskanzlei überwacht die korrekte Umsetzung durch den Kanton mittels unabhängiger Prüfungen (siehe Abschnitt 4.3.2).

Der Druck der Stimmzettel sowie der Abstimmungsbroschüren wird je nach der föderalen Ebene, auf der eine Wahl oder Abstimmung stattfindet, durch die Bundeskanzlei, die Staatskanzlei oder die jeweilige Gemeinde in Auftrag gegeben. Externe Druckereien führen diese Druckaufträge aus und liefern die gedruckten Stimmzettel und Beilagen für die Verpackung an die Firma Abraxas. Im Fall von Gemeinden, die ihr Stimmmaterial von einem anderen Anbieter verpacken lassen, leitet Abraxas das eidgenössische und kantonale Stimmmaterial direkt an diesen weiter.

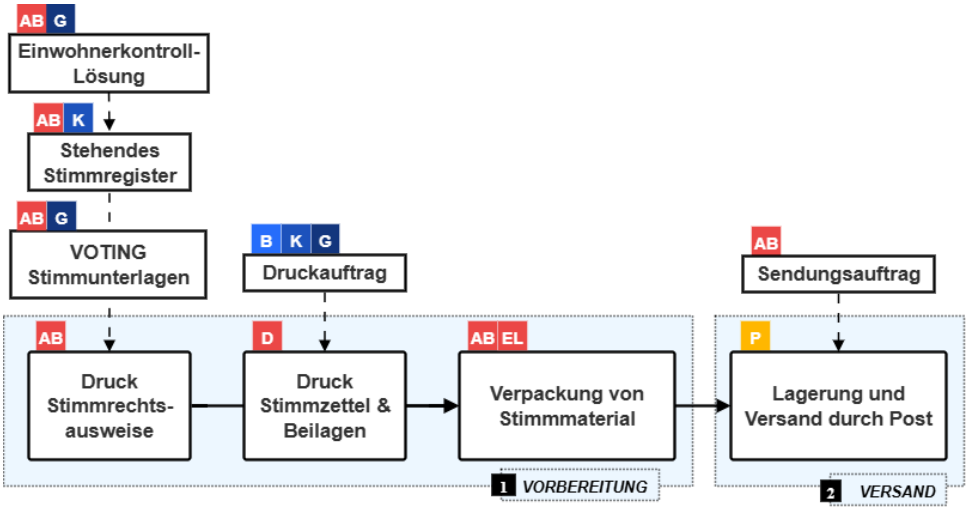

Abbildung 2: Vorbereitung und Versand des Stimmmaterials (Quelle: UZH)

Im Zuge des Arbeitsschritts Verpackung werden die Stimmrechtsausweise, die Stimmzettel sowie die weiteren Beilagen zusammengeführt und das Zustellkuvert wird anschliessend zum Versand an die Stimmberechtigten an die Post übergeben.

3.2.2 Potenzielle Bedrohungen

Mit Blick auf die drei Arbeitsschritte in der Phase Vorbereitung wurden von den Experten der UZH fünf potenzielle Bedrohungen identifiziert. Diese wurden anhand ihres zu erwartenden Schadensausmasses kategorisiert.[6]

ID	Beschreibung	Schadensausmass
B1	Diebstahl und Missbrauch von Stimmmaterial, insbesondere der Stimmrechtsausweise	HOCH
B2	Fälschung von Stimmrechtsausweisen	HOCH
B3	Manipulation des Stimmregisters (Hinzufügen, Löschen, Ändern)	MITTEL
B4	Inkonsistenzen im Stimmregister (z.B. infolge Umzugs von Stimmberechtigten)	NIEDRIG
B5	Verzögerung des Drucks von Stimmmaterial	NIEDRIG

[6] Das Schadensausmass wird mit Blick auf die primären Schutzziele – die integre und erfolgreiche Durchführung einer Abstimmung oder Wahl sowie die Wahrung des Stimmgeheimnisses – in drei Stufen («hoch», «mittel» und «niedrig») unterteilt, wobei diese sich an der Anzahl der Stimmen orientieren, die durch einen potenziellen Angriff gefälscht werden könnten. Während im Fall eines erfolgreichen Angriffs bei einem niedrigen Schadensausmass «lediglich» einzelne Stimmen gefälscht werden könnten, beschreibt ein hohes Schadensausmass ein Szenario, in dem der Angriff auf einen substanziellen Anteil der Wählerbasis ausgeweitet werden könnte (Analyse UZH, Abschnitt 2.1).

Unter der **Bedrohung B1** wird eine Reihe an möglichen Bedrohungen subsumiert, die sich aus der physischen Lagerung, Verpackung und Zustellung von Stimmmaterial ergeben. Der sicherheitsrelevante Fokus liegt dabei klar auf dem Stimmrechtsausweis, da ohne gültige Stimmrechtsausweise keine Stimmabgaben möglich sind. Die Gültigkeit der Stimmrechtsausweise wird von den Mitgliedern des Stimmbüros überprüft, was sowohl das Schadensausmass eines allfälligen Angriffs reduziert als auch ein gewisses Manipulations- und Fehlerpotenzial mit sich bringt (zu diesem Punkt siehe auch B17). Um den Aufwand eines Angriffs mittels eines Diebstahls von Stimmmaterial einzuschätzen, muss zudem berücksichtigt werden, dass ein solcher zu verschiedenen Zeitpunkten während des Prozesses möglich ist. Zunächst wird das Stimmmaterial in der Druckerei hergestellt und zwischengelagert. Obschon dies an einem zentralen Ort geschieht, erschweren vorhandene Prozesskontrollen einen Angriff. So werden beispielsweise die Druckdaten für E-Voting-Stimmrechtsausweise verschlüsselt übertragen und erst in der Druckerei entschlüsselt, wobei sie nur im Vieraugenprinzip abgerufen werden können. Es kann aber auch anderes Stimmmaterial gestohlen (oder kopiert) werden, beispielsweise die Stimmzettel. Da Letztere jedoch nicht an eine bestimmte Person gebunden sind, sind sie grundsätzlich zugänglich und eine Vervielfältigung ist nicht per se problematisch. Zudem ist eine Stimmabgabe nur in Kombination mit einem gültigen Stimmrechtsausweis möglich. Die Abgabe mehrerer Stimmzettel durch die gleiche Person hätte zudem keine Auswirkungen, da überzählige Stimmzettel im Rahmen der Überprüfung durch das Stimmbüro ausgesondert werden (siehe auch B10). Daher ist wie eingangs erwähnt primär der Stimmrechtsausweis sicherheitsrelevant.

Die **Bedrohung B2** beinhaltet die Fälschung oder Vervielfältigung von Stimmrechtsausweisen. Mit zusätzlichen Stimmrechtsausweisen liessen sich Stimmen fälschen – also zusätzliche Stimmen abgeben – und damit das Ergebnis einer Wahl oder Abstimmung beeinflussen. Die Erkennung (und Eindämmung) eines derartigen Angriffs ist jedoch schwierig. Zunächst sind mögliche Diskrepanzen nur anhand offensichtlicher Mehrfachstimmabgaben oder physischer Unregelmässigkeiten der Stimmrechtsausweises zu erkennen. Erschwerend kommt hinzu, dass einmal bemerkte Unregelmässigkeiten nicht mehr «bereinigt» werden können, wenn zu diesem Zeitpunkt die Stimmrechtsausweise bereits von den Stimmzettelkuverts getrennt sind (zum Ablauf der Prüfung der Gültigkeit der Stimmabgaben und der Auszählung siehe Abschnitte 3.5 und 3.6), da dann nicht mehr eruiert werden kann, welche Stimmzettel nicht in die Auszählung einfliessen dürften.

Die **Bedrohung B3** umfasst mögliche Manipulationen des Stimmregisters. So ist es denkbar, dass Stimmberechtigte entfernt, hinzugefügt oder deren Daten (z.B. die Wohnadresse) verändert werden könnten. Auf diese Weise könnten Stimmberechtigte von einer Wahl oder Abstimmung ausgeschlossen oder als fiktive Stimmberechtigte zu dieser zugelassen werden. Die Verwaltung der Stimmberechtigten erfolgt dezentral in den Einwohnerkontroll-Lösungen der Gemeinden. Bislang kamen im Kanton St.Gallen vier unterschiedliche Einwohnerkontroll-Lösungen zum Einsatz, wobei die allermeisten Gemeinden mit *Loganto* ein System benutzten, das von der Firma Abraxas mandantenfähig betrieben wird. Im Frühjahr 2022 haben der Kanton und die St.Galler Gemeinden gemeinsam eine neue Lösung ausgeschrieben und anschliessend eingeführt. Seit Ende November 2025 arbeiten sämtliche Gemeinden mit dem neuen *Datenmanagement für Einwohnende (DME)*, das auf der bereits etablierten Lösung *Innosolv City* basiert und ebenfalls auf der Infrastruktur von Abraxas betrieben wird. Auch das stehende Stimmregister der Staatskanzlei wird von Abraxas betrieben. In diesem werden die Stimmregisterdaten der Gemeinden tagesaktuell zusammengeführt, wobei im Sinn der Datensparsamkeit nur diejenigen Daten übertragen werden, die für die Aufgabenerfüllung der Staatskanzlei ge-

mäss der am 11. November 2025 durch die Regierung erlassenen Verordnung über das stehende Stimmregister unabdingbar sind. Mutationen an den importierten Daten sind im stehenden Stimmregister nicht möglich.[7]

Die **Bedrohung B4** betrifft ebenfalls die Stimmregister der Gemeinden bzw. die darin gehaltenen Daten. So können Inkonsistenzen auch als Folge von Mutationen – also durch den Zu- oder Wegzug von Stimmberechtigten – nach dem Versand des Stimmmaterials für eine Wahl oder Abstimmung entstehen. In einer solchen Konstellation ist es möglich, dass eine Person einmalig zwei Sets an Stimmmaterial erhält (eines von der alten Wohnsitzgemeinde und eines von der neuen) oder gar keines. Allerdings gestaltet sich die Skalierbarkeit eines Angriffs diesbezüglich eher schwierig. Zum einen, weil grosse Differenzen im Stimmregister auffallen würden, zum anderen, weil gesetzlich geregelt ist, dass Neuzuzügerinnen und Neuzuzügern nur im Austausch gegen den von der bisherigen Wohnsitzgemeinde bereits erhaltenen Stimmrechtsausweis neues Stimmmaterial ausgehändigt werden darf. Somit sind Angriffe, die eine kleine Differenz im Endergebnis zur Folge haben, zwar denkbar, eine Manipulation des Ergebnisses mit einer grossen Zahl an manipulierten Stimmen erscheint jedoch sehr unwahrscheinlich.

Die **Bedrohung B5** beinhaltet mögliche Verzögerungen im Druckprozess, die sowohl die Produktion der Stimmrechtsausweise als auch jene von Stimmzetteln oder anderen Beilagen betreffen können. Durch eine (länger anhaltende) Verzögerung kann theoretisch die gesamte Vorbereitung einer Wahl oder Abstimmung behindert werden, wenn das nötige Stimmmaterial nicht rechtzeitig für die Verpackung und den Versand bereit ist. Im schlimmsten Fall könnte die gesetzlich vorgeschriebene Frist für die Zustellung des Stimmmaterials an die Stimmberechtigten nicht eingehalten werden.

3.2.3 Bereits umgesetzte und mögliche zusätzliche Gegenmassnahmen

Mit der Inbetriebnahme von *VOTING Stimmunterlagen* 2023 haben die St.Galler Gemeinden sowie die Staatskanzlei und die von ihr beauftragte Verpackungsdienstleisterin (Abraxas) einen digitalen Service erhalten, der sie während des ganzen Prozesses der Bestellung, Produktion und Verpackung von Stimmmaterial unterstützt (M1). So ist es heute möglich, für jede Gemeinde die Zahl der stimmberechtigten Personen mit der Anzahl an bestellten, produzierten und verpackten Stimmunterlagen abzugleichen und auf diese Weise Fehlern ebenso sowie unbewussten oder bewussten Manipulationen durch beteiligte Personen vorzubeugen (B1 und B3). Zudem wird durch die Möglichkeit des Abgleichs die Wahrscheinlichkeit minimiert, dass gefälschte Stimmrechtsausweise unbemerkt in den Prozess eingeschleust oder echte Stimmrechtsausweise aus diesem entfernt werden können – etwa indem sie vor der Verpackung gestohlen werden (B2). Die Problematik von (geringfügigen) Inkonsistenzen aufgrund von Zu- oder Wegzügen nach dem Versand des Stimmmaterials (B4) wird dadurch allerdings nicht gelöst.

Eine denkbare zusätzliche Gegenmassnahme zur Verhinderung der Fälschung und des Missbrauchs von Stimmrechtsausweisen (B1 und B2) sowie möglicher Mehrfachstimmabgaben als Folge von Inkonsistenzen im Stimmregister (B4) wäre der Aufdruck eines weiteren Sicherheitsmerkmals (z.B. eines Datamatrix-Codes) auf den Stimmrechtsausweisen, anhand dessen ein Abgleich mit dem stehenden Stimmregister möglich wäre (M2). Auf diese Weise könnten – im Idealfall direkt am Wahl- oder Abstimmungssonntag – die Echtheit und Validität des Stimmrechtsausweises geprüft und Mehrfachstimmabgaben oder gefälschte Stimmen verunmöglicht

[7] Die einzige Ausnahme ist das Hinzufügen des so genannten «E-Voter-Flags», das anzeigt, ob sich eine stimmberechtigte Person in ihrer Gemeinde für die elektronische Stimmabgabe angemeldet hat. Diese Information muss auf kantonaler Ebene geführt werden, um sicherzustellen, dass die Vorgabe des Bundes, wonach höchstens 30 Prozent des kantonalen Elektorats zur elektronischen Stimmabgabe zugelassen werden dürfen, eingehalten wird (siehe auch Abschnitt 4.3.1).

werden (weiterführende Überlegungen zu diesem Punkt folgen im Abschnitt 3.4.3 im Rahmen der Diskussion von B10).

Für eine Manipulation des Stimmregisters einer Gemeinde (B3) durch eine externe Person wäre ein direkter Angriff auf Abraxas nötig, da sowohl *Loganto* als auch die Nachfolgelösung *DME* auf der Infrastruktur der Firma betrieben werden. Um einer derartigen Bedrohung entgegenzuwirken, steht daher die Informationssicherheit von Abraxas im Vordergrund. Das Unternehmen Abraxas ist ISO 27001 zertifiziert (M3), was bedeutet, dass organisatorische Risiken regelmässig überprüft und mit entsprechenden Kontrollen gesichert werden.[8] Die Einhaltung dieses Sicherheitsmanagements auf Seiten von Abraxas wird in einem unabhängigen Audit geprüft. Darüber hinaus wird 2026 der Quellcode der neuen Lösung *DME* im Rahmen eines Bug-Bounty-Programms offengelegt werden, was es einem internationalen Kreis von Sicherheitsexperten möglich macht, die Lösung auf mögliche Schwachstellen hin zu prüfen (M4; detaillierte Ausführungen zum Bug-Bounty-Programm folgen in Abschnitt 4.6).

Schwieriger ist es, eine Manipulation durch eine beteiligte Person (z.B. eine Mitarbeiterin oder ein Mitarbeiter des Einwohneramtes der Gemeinde) zu verhindern. Allerdings kann davon ausgegangen werden, dass eine stimmberechtigte Person, die (in diesem Fall zu Unrecht) kein Stimmmaterial erhält, selbiges bei der Gemeinde einfordern wird. Die Manipulation bliebe also nicht unbemerkt. Dasselbe gilt für das Hinzufügen einer grösseren Zahl an fiktiven Stimmberechtigten. Die dadurch entstehende Differenz zur Anzahl der Stimmberechtigten bei vorangegangenen Wahlen oder Abstimmungen würde im Rahmen der Bestellung des Stimmmaterials, spätestens jedoch bei der Plausibilitätsprüfung des Gemeindeergebnisses (M5; siehe Ausführungen zu B18 in Abschnitt 3.6.3) auffallen.

Als bestehende Gegenmassnahme zur Verhinderung von Mehrfachstimmabgaben als Folge von Inkonsistenzen im Stimmregister (B4) dient die gesetzliche Vorgabe, dass im Kanton St.Gallen gemäss Art. 53 Abs. 1 des Gesetzes über Wahlen und Abstimmungen (sGS 125.3; abgekürzt WAG) Neuzuzügerinnen und Neuzuzüger das Stimmmaterial für eine Wahl oder Abstimmung nur gegen Abgabe des von der bisherigen Wohnsitzgemeinde erhaltenen Stimmrechtsausweises erhalten (M6). Seit der Inbetriebnahme des stehenden Stimmregisters Anfang 2024 besteht zudem die Möglichkeit von tagesaktuellen Abfragen, was es erlaubt, jederzeit Gewissheit über die Stimmberechtigung von Personen und deren Wohnsitz zu erlangen.

Aufgrund der eher «grosszügigen» Fristen, welche die einschlägigen Gesetze für die Zustellung des Stimmmaterials vorschreiben, sind mit Blick auf (mutwillig herbeigeführte) Verzögerungen im Druckprozess (B5) keine eigentlichen Gegenmassnahmen nötig. So besagt Art. 11 Abs. 3 des Bundesgesetzes über die politischen Rechte (SR 161.1; abgekürzt BPR), dass die Stimmberechtigten im Fall einer eidgenössischen Abstimmung die benötigten Unterlagen mindestens drei und frühestens vier Wochen vor dem Abstimmungstag erhalten müssen. Die gleiche Zustellfrist gilt auch bei Wahlen und Abstimmungen auf kantonaler Ebene (Art. 52 Abs. 1 WAG). Da die Produktionspläne, welche die Staatskanzlei gemeinsam mit Abraxas ausarbeitet – und die für alle Gemeinden verbindlich sind –, sich an diesen Fristen orientieren, wird den verantwortlichen Behörden auch im Fall einer Verzögerung im Druckprozess in der Regel genügend Zeit bleiben, um einen erneuten Druck und Versand von Stimmmaterial einzuleiten, falls dies nötig sein sollte.

Zusammenfassend hier der Überblick über die fünf Gegenmassnahmen, die zur Eindämmung der identifizierten Bedrohungen in der Phase Vorbereitung bereits umgesetzt werden oder welche die Regierung mit Blick auf eine zukünftige Umsetzung näher zu prüfen beabsichtigt:

---

8 Weitere Informationen zur ISO-Zertifizierung von Abraxas finden sich im Internet unter https://www.abraxas.ch/de/uber-uns/qualitaetsmanagement.

Massnahme	Eingedämmte Bedrohungen	Status
M1: Durchgängige digitale Unterstützung des Bestell-, Produktions- und Verpackungsprozesses mit ständiger Möglichkeit des Mengenabgleichs	B1: Diebstahl und Missbrauch von Stimmmaterial B2: Fälschung von Stimmrechtsausweisen B3: Manipulation des Stimmregisters	umgesetzt
M3: ISO-Zertifizierung des Informationssicherheits-Managements der Systemanbieterin	B3: Manipulation des Stimmregisters	umgesetzt
M4: Offenlegung des Quellcodes der neuen Stimmregister-Lösung der Gemeinden (*DME*) im Rahmen eines Bug-Bounty-Programms	B3: Manipulation des Stimmregisters	in Umsetzung
M5: Plausibilisierung der Gemeindeergebnisse durch die Staatskanzlei	B3: Manipulation des Stimmregisters (ebenso: B10: Abgabe von gefälschtem Stimmmaterial; B18: Manipulation der Auszählung durch Insiderinnen oder Insider)	umgesetzt
M6: Gesetzliche Vorgaben betreffend Umzug in andere Gemeinde (Stimmrechtsausweis darf in Zuzugsgemeinde nur gegen Abgabe desjenigen aus Wegzugsgemeinde ausgehändigt werden)	B4: Inkonsistenzen im Stimmregister	umgesetzt
M2: Zusätzlicher Datamatrix-Code auf Stimmrechtsausweis für Abgleich mit dem Stimmregister	B1: Diebstahl und Missbrauch von Stimmmaterial B2: Fälschung von Stimmrechtsausweisen B4: Inkonsistenzen im Stimmregister (ebenso B10: Abgabe von gefälschtem Stimmmaterial)	zu prüfen

3.3 Phase Versand

3.3.1 Einführung und Übersicht über Arbeitsschritte

Die zweite Phase des Wahl- und Abstimmungsprozesses umfasst die Lagerung des verpackten Stimmmaterials bei der Post sowie den anschliessenden Versand der Zustellkuverts an die Stimmberechtigten (siehe auch Abbildung 2).

Nach der Verpackung des Stimmmaterials durch Abraxas – oder durch einen anderen Verpackungsdienstleister, sollte eine Gemeinde dies wünschen – werden die Zustellkuverts der Post übergeben. Da der Zeitraum, in dem die Zustellung des Stimmmaterials zu erfolgen hat, gesetzlich geregelt ist, werden die Zustellkuverts bis zum Versand bei der Post sicher zwischengelagert. Wie in Abschnitt 3.2.3 bereits erwähnt, erfolgt die Zustellung an die Stimmberechtigten dann frühestens vier und bis spätestens drei Wochen vor dem Wahl- oder Abstimmungssonntag.[9]

3.3.2 Potenzielle Bedrohungen

Mit Blick auf die Lagerung bei der Post und den Versand des Stimmmaterials wurden von der UZH vier potenzielle Bedrohungen identifiziert.

[9] Hierfür wird im Vorfeld aller eidgenössischen Blanko-Abstimmungstermine die Spezialdienstleistung «Wahl- und Abstimmungssendung» der Schweizerischen Post verwendet (vgl. www.post.ch/de/briefe-versenden/dokumenten-und-urkunden/wahl-und-abstimmungssendung).

ID	Beschreibung	Schadensausmass
B6	Diebstahl von Stimmmaterial während der Lagerung bei der Post	MITTEL
B7	Diebstahl von Stimmmaterial nach Versand an die Stimmberechtigten (z.B. aus dem Briefkasten)	MITTEL
B8	Zerstörung von Stimmmaterial während der Lagerung bei der Post	NIEDRIG
B9	Zerstörung von Stimmmaterial nach Versand an die Stimmberechtigten	NIEDRIG

Die **Bedrohung B6** beinhaltet den Diebstahl von Stimmmaterial während der Lagerung bei der Post. Der Aufwand für einen solchen Diebstahl wird von der UZH aufgrund der Sicherheitsmassnahmen der Post (siehe auch Abschnitt 3.3.3) als hoch eingeschätzt. Bliebe ein solcher Diebstahl jedoch unbemerkt und würde das gestohlene Stimmmaterial verwendet, wäre es für die Gemeinden schwierig, legitime Stimmabgaben von missbräuchlichen zu unterscheiden (ausser Letztere wären bereits auf den ersten Blick erkenntlich, beispielsweise dadurch, dass alle gestohlenen Stimmrechtsausweise die gleiche Unterschrift aufweisen). Allerdings kann davon ausgegangen werden, dass der Diebstahl einer substanziellen Menge an Stimmmaterial nicht unbemerkt bliebe, da zumindest ein Teil der betroffenen Stimmberechtigten bemerken würde, dass sie kein Stimmmaterial erhalten haben, und sie dieses bei der Gemeinde einfordern würden.

Die **Bedrohung B7** betrifft ebenfalls den Diebstahl von Stimmmaterial, allerdings nach dem Versand an die Stimmberechtigten, beispielsweise aus deren Briefkästen. Aus Sicht eines potenziellen Angreifers gibt es denn auch zwei deutliche Unterschiede zu B6: Zum einen dürfte der Aufwand für einen (unbemerkten) Diebstahl deutlich geringer sein, da das Stimmmaterial einfacher zugänglich ist als in den Lagern der Post. So werden etwa die Briefkästen in Wohnhäusern in aller Regel nicht gesondert (mit Video) überwacht. Zum anderen ist auch die Skalierbarkeit eines derartigen Angriffs kleiner, da jede und jeder Stimmberechtigte nur ein einziges Zustellkuvert mit Stimmmaterial erhält, wodurch sich auch das Schadenspotenzial eines allfälligen Diebstahls reduziert.

Die **Bedrohungen B8 und B9** beziehen sich auf die Zerstörung von Stimmmaterial, entweder während der Lagerung bei der Post (B8) oder nach dem Versand an die Stimmberechtigten (B9). In beiden Fällen ist die Wahrscheinlichkeit gross, dass die betroffenen Stimmberechtigten oder andere aufmerksame Personen den Angriff bemerken und melden. Die Folge wäre daher primär eine Verzögerung in der Zustellung des Stimmmaterials, nicht jedoch die Verhinderung der Stimmabgabe.

3.3.3 Bereits umgesetzte und mögliche zusätzliche Gegenmassnahmen

Um die Gefahr eines Diebstahls oder der Zerstörung von Stimmmaterial während der Lagerung bei der Post (B6 und B8) einzudämmen, sind primär die von der Post ergriffenen Massnahmen im Bereich der physischen Sicherheit (M7) massgeblich. Wie die Firma Abraxas führt auch die Post ein Informationssicherheits-Management-System, das nach ISO 27001 zertifiziert ist.[10] Dennoch lässt sich der Diebstahl oder die Zerstörung (einer geringen Menge) von Stimmmaterial durch einen Angreifer nicht völlig ausschliessen. Dies gilt insbesondere dann, wenn der Angriff durch eine beteiligte Person (also eine Mitarbeiterin oder einen Mitarbeiter der Post) mit den entsprechenden Kenntnissen erfolgen würde.

10 Weitere Informationen zur ISO-Zertifizierung der Post finden sich im Internet unter https://www.post.ch/de/ueber-uns/verantwortung/zertifikate#iso-27001.

Mit Blick auf die Verwendung von gestohlenem Stimmmaterial (B6 und B7) kommt dem Hinweis auf das Schweizerische Strafgesetzbuch (SR 311.0; abgekürzt StGB), der auf alle Stimmrechtsausweise aufgedruckt ist, zudem eine abschreckende Wirkung zu (M8). Er stellt klar, dass die unbefugte oder mehrmalige Teilnahme an einer Wahl oder Abstimmung als Wahlfälschung strafbar ist (Art. 282 StGB).

Wie in Abschnitt 3.2.3 bereits thematisiert, ist das Zeitfenster, in dem das Stimmmaterial den Stimmberechtigten zugestellt werden muss, gesetzlich geregelt und vielen Schweizerinnen und Schweizern bekannt. Es kann daher davon ausgegangen werden, dass ein gross angelegter Diebstahl bzw. eine Zerstörung von Stimmmaterial während der Lagerung bei der Post (B6 und B8) nicht unerkannt bleiben würde. Zudem würde den verantwortlichen Behörden aufgrund der eher «grosszügigen» Fristen in der Regel genügend Zeit bleiben, um den betroffenen Stimmberechtigten das gestohlene Stimmmaterial zu ersetzen oder im schlimmsten Fall einen Teil davon erneut produzieren zu lassen.

Da der Erfolg von Diebstählen oder der Zerstörung von Stimmmaterial bei einzelnen Stimmberechtigten (B7 und B9) von den individuellen Gegebenheiten von deren Briefkästen abhängig ist, existieren gegen diese Bedrohungen keine speziellen Gegenmassnahmen. Solche sind auch nicht geplant bzw. sie könnten gar nicht umgesetzt werden. Allerdings gilt es festzuhalten, dass derartige Angriffe auch nur schwer zu skalieren sind, da ein physischer Zugriff auf verschiedene Briefkästen notwendig wäre. Darüber hinaus kommen auch in diesem Fall die bereits erwähnten Gegenmassnahmen (zeitlicher Puffer zwischen der [Nicht-]Zustellung des Stimmmaterials und dessen Verwendung sowie Warnung vor den rechtlichen Folgen eines Missbrauchs) zum Tragen.

Massnahme	**Eingedämmte Bedrohungen**	**Status**
M7: Massnahmen der Post im Bereich der physischen Sicherheit	B6: Diebstahl von Stimmmaterial während der Lagerung bei der Post B8: Zerstörung von Stimmmaterial während der Lagerung bei der Post	umgesetzt
M8: Hinweis auf Strafgesetzbuch (abschreckende Wirkung)	B6: Diebstahl von Stimmmaterial während der Lagerung bei der Post B7: Diebstahl von Stimmmaterial nach Versand an die Stimmberechtigten	umgesetzt

3.4 Phase Stimmabgabe

3.4.1 Einführung und Übersicht über Arbeitsschritte

Die dritte Phase im Prozess der Vorbereitung und Durchführung von Wahlen und Abstimmungen (siehe auch Abbildung 3) beinhaltet die Stimmabgabe durch die Stimmberechtigten, also den eigentlichen Akt des «Abstimmens» bzw. des «Wählens», sowie – im Fall von brieflichen Stimmabgaben – den Rückversand der Zustellkuverts an die betreffenden Gemeinden.

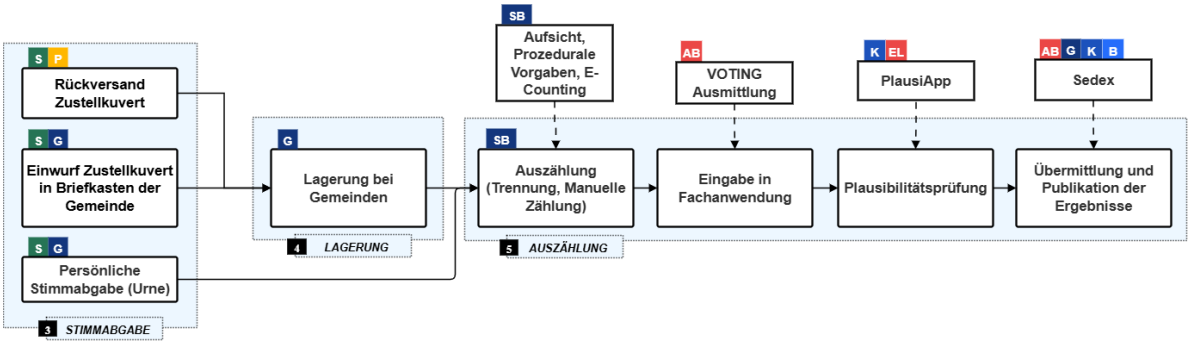

Abbildung 3: Stimmabgabe, Lagerung bei der Gemeinde und Auszählung (Quelle: UZH)

Grundsätzlich können drei alternative Möglichkeiten der Stimmabgabe unterschieden werden, zwischen denen eine stimmberechtigte Person frei wählen kann:

– Mit Abstand am häufigsten genutzt wird die Möglichkeit der brieflichen Stimmabgabe. Das heisst, das Zustellkuvert mit dem unterschriebenen Stimmrechtsausweis und dem verschlossenen Stimmzettelkuvert, das den oder die ausgefüllten Stimmzettel enthält, wird in einen Briefkasten geworfen und mit der Post zurück an die Gemeinde gesandt. Alternativ können Stimmberechtigte ihre Zustellkuverts im Vorfeld eines Urnenganges auch direkt in den Briefkasten ihrer Wohnsitzgemeinde einwerfen.

– Die zweite Option ist die persönliche Stimmabgabe an der Urne. Von Gesetzes wegen muss an einem Wahl- oder Abstimmungssonntag mindestens eine Urne in jeder Gemeinde für mindestens eine Stunde geöffnet sein (Art. 73 WAG).

– Ergänzend zu den beiden bereits genannten Optionen hat ein Teil der Stimmberechtigten im Kanton St.Gallen zudem die Möglichkeit, ihre Stimmen mittels E-Voting elektronisch abzugeben. Allerdings müssen dafür zwei Bedingungen erfüllt sein: Zum einen muss die betreffende Gemeinde ihren Bürgerinnen und Bürgern den elektronischen Stimmkanal anbieten, darüber hinaus müssen sich Stimmberechtigte, welche die Möglichkeit von E-Voting nutzen möchten, vorgängig dafür anmelden.[11] Ist beides erfüllt, erhält die oder der Stimmberechtigte einen speziellen Stimmrechtsausweis mit den für die elektronische Stimmabgabe notwendigen Sicherheitsmerkmalen.[12] Auch diese Stimmrechtsausweise können jedoch für eine briefliche Stimmabgabe oder eine Stimmabgabe an der Urne verwendet werden, sofern die Stimme zuvor nicht bereits auf elektronischem Weg abgegeben wurde.

Da im Hinblick auf die elektronische Stimmabgabe spezifische Risiken ebenso wie besondere Sicherheitsvorgaben seitens des Bundes existieren, werden diese wie eingangs erwähnt in Abschnitt 4 separat diskutiert und es wird aufgezeigt, welche Erkenntnisse und «best practices» aus den Pilotversuchen mit E-Voting für andere digitale Services im Bereich der politischen Rechte übernommen werden können. Die nachfolgenden Ausführungen in den Abschnitten 3.4.2 und 3.4.3 beschränken sich deshalb auf potenzielle Bedrohungen und geeignete Gegenmassnahmen mit Blick auf briefliche Stimmabgaben und solche an der Urne.

11 Eine Übersicht über den aktuellen Stand der Ausweitung von E-Voting sowie detaillierte Informationen zum Anmeldeverfahren finden sich auf der eigens dafür eingerichteten Webseite des Kantons St.Gallen unter https://www.sg.ch/politik-verwaltung/abstimmungen-wahlen/e-voting.html.

12 Die im Kanton St.Gallen registrierten Auslandschweizerinnen und Auslandschweizer erhalten automatisch einen Stimmrechtsausweis, mit dem sie elektronisch, brieflich oder an der Urne wählen und abstimmen können. Eine Anmeldung für E-Voting ist in ihrem Fall nicht mehr nötig.

3.4.2 Potenzielle Bedrohungen

Mit Blick auf die briefliche Stimmabgabe sowie die Stimmabgabe an der Urne wurden von der UZH fünf potenzielle Bedrohungen identifiziert.

ID	Beschreibung	Schadensausmass
B10	Abgabe von gefälschtem Stimmmaterial	HOCH
B11	Diebstahl und/oder Zerstörung von Stimmmaterial aus Gemeindebriefkasten	MITTEL
B12	Überlastung der postalischen Services durch Cyberangriffe auf die Informationssysteme der Post	MITTEL
B13	Überlastung der postalischen Services durch «Überfluten» der Briefpost	NIEDRIG
B14	Überlastung der Gemeinden durch «Überfluten» mit Briefpost	NIEDRIG

Die **Bedrohung B10** besteht in der Abgabe von gefälschtem Stimmmaterial, also in der Verwendung von gefälschten oder gestohlenen Stimmrechtsausweisen. Im Rahmen der Prüfung der Gültigkeit der Stimmabgaben (siehe Abschnitt 3.5.1) werden alle Stimmrechtsausweise durch das Stimmbüro der Gemeinde kontrolliert und anschliessend von den noch verschlossenen Stimmzettelkuverts mit den darin enthaltenen Stimmzetteln getrennt. Auf diese Weise bleibt das Stimmgeheimnis in jedem Schritt der Auszählung gewahrt. Gelingt es einem Angreifer, den Stimmrechtsausweis so zu fälschen, dass die Fälschung bei der Prüfung durch das Stimmbüro nicht erkannt wird, gelangt das Stimmzettelkuvert mit den missbräuchlich eingelangten Stimmzetteln in den Auszählungsprozess und kann zu einem späteren Zeitpunkt nicht mehr ausgesondert werden. Eine so entstandene Unregelmässigkeit könnte – selbst wenn der Betrug nachträglich erkannt wird – also nicht mehr bereinigt werden. Allerdings ist es nicht möglich, mit *einem* Stimmrechtsausweis (unabhängig davon, ob dieser echt ist oder gefälscht) mehrere Stimmzettel für die gleiche Vorlage in den Auszählungsprozess «einzuschleusen», da überzählige Stimmzettel im Rahmen der Überprüfung durch das Stimmbüro ausgesondert werden.

Die **Bedrohung B11** beschreibt das Szenario, in dem Zustellkuverts aus dem Briefkasten der Gemeinde gestohlen und/oder zerstört werden. Wie im Fall der bereits diskutierten Bedrohungen B7 und B9 wäre ein derartiger Angriff relativ einfach umzusetzen, da lediglich der physische Zugriff auf einen Briefkasten erlangt werden muss. Allerdings ist davon auszugehen, dass ein solcher Angriff auch schnell erkannt würde, typischerweise anhand von Einbruchs- oder Zerstörungsspuren. So kann das «nächtliche Fischen» von (Zustell-)Kuverts aus einem Briefkasten zwar nicht ausgeschlossen werden – ausser Letzterer ist durch besondere Sicherheitsmassnahmen geschützt –, die Experten der UZH erachten die Auswirkungen eines solchen Angriffs jedoch als eher gering. Zum einen, weil die Briefkästen der Gemeinden in der Regel (mehrmals) täglich geleert werden. Es ist daher unwahrscheinlich, dass sehr viele Zustellkuverts gleichzeitig in einem bestimmten Briefkasten liegen. Zum anderen aber auch aufgrund der räumlichen Distanz zwischen den Gemeinden, welche die Skalierbarkeit eines derartigen Angriffes erschwert.

Die **Bedrohungen B12, B13 und B14** umfassen Angriffsszenarien, die eine Sabotage der Diensterbringung («Denial-of-Service») durch die Post, also der Zustellung der brieflichen Stimmabgaben an die Gemeinden anstreben. Da die Stimmabgaben rechtzeitig bei den Gemeinden eintreffen müssen, damit die nachfolgenden Arbeitsschritte (siehe Abbildung 1) ordnungsgemäss durchgeführt werden können, ist das Ziel derartiger Angriffe stets, die Zustellung der brieflichen Stimmabgaben zu verzögern oder ganz zu unterbinden. Dies könnte beispielsweise dadurch erreicht werden, dass eine künstliche Überlastung herbeigeführt wird. So könnte ein plötzliches, sehr grosses Aufkommen an brieflichen Sendungen («Überfluten») zu einer

Verzögerung in der Zustellung führen (B13). Es ist auch denkbar, dass eine Verzögerung dadurch erreicht werden könnte, dass die zur Steuerung der Verarbeitung und Zustellung der brieflichen Stimmabgaben verwendeten Informationssysteme der Post angegriffen (B12) oder dass Postmitarbeitende an neuralgischen Stellen (z.B. in einem Verteilzentrum) bestochen würden. Theoretisch könnte eine Überlastung zudem auch bei den Gemeinden erreicht werden, indem so viele Briefe eingesandt würden, dass die personellen Ressourcen für das Aussortieren der brieflichen Stimmabgaben nicht mehr ausreichen und die ordnungsgemässe Auszählung dadurch verzögert wird (B14).

Das Schadensausmass einer «Überflutung» (B13 und B14) wird von den Experten der UZH aber als niedrig eingeschätzt, da für derart gross angelegte Angriffe beträchtliche Ressourcen (z.B. das Vorbereiten einer sehr grossen Anzahl an Briefen) nötig wären. Ferner bleibe ohne eine dezidierte Analyse der Infrastruktur der Post unklar, ob derartige Angriffe tatsächlich zu einer Verzögerung führen würden. Das Schadensausmass eines Cyberangriffs auf die Informationssysteme der Post (B12) bewertet die UZH hingegen als mittel, da ein solcher hypothetisch mit weniger Aufwand verbunden wäre als eine physische Überlastung mit einer sehr grossen Anzahl an brieflichen Sendungen. Allerdings sei eine generelle Einschätzung der tatsächlichen Verletzlichkeit der eingesetzten IT-Systeme schwierig und nur anhand konkreter Szenarien mit messbaren Details erfolgversprechend (Analyse UZH, S. 12). In Anbetracht dessen, dass Cyberangriffe wie beispielsweise «Ransomware-Angriffe»[13] relativ häufig vorkommen, kann jedoch nicht ausgeschlossen werden, dass auch die IT-Systeme der Post einmal betroffen sein könnten.

3.4.3 Bereits umgesetzte und mögliche zusätzliche Gegenmassnahmen

Um missbräuchliche Stimmabgaben abzufangen und zu verhindern, dass diese in die Auszählung einfliessen (B10), kommen verschiedene Massnahmen zum Tragen. Zum einen werden wie bereits erwähnt alle Stimmabgaben durch das Stimmbüro der betreffenden Gemeinde geprüft (M9) und ungültige Stimmabgaben (z.B. solche mit Stimmrechtsausweisen, die nicht unterschrieben sind oder von einem früheren Urnengang stammen) werden aussortiert. Es kann davon ausgegangen werden, dass die Stimmbüros bei dieser Prüfung auch offensichtliche Mehrfachstimmabgaben oder gefälschte Stimmrechtsausweise, die sich durch direkt erkennbare Unterschiede (etwa anderes Papier, anderes Format oder andere Schriften) von echten abheben, erkennen und aussondern würden. Eine missbräuchliche Stimmabgabe mit einem professionell gefälschten oder einem gestohlenen «echten» Stimmrechtsausweis würde im Rahmen der Prüfung durch das Stimmbüro jedoch wohl unerkannt bleiben.

Immerhin besteht eine grosse Wahrscheinlichkeit, dass der Betrug im Rahmen der Plausibilitätsprüfung des Gemeindeergebnisses (M5) auffallen würde – etwa, weil die Stimmbeteiligung verglichen mit früheren Abstimmungen der Gemeinde ausserordentlich hoch ist –, insbesondere dann, wenn eine grössere Anzahl an missbräuchlichen Stimmabgaben in den Auszählungsprozess gelangt sein sollte. Die Erkennung eines Einzelfalls ist hingegen auch im Rahmen der Plausibilisierung unwahrscheinlich (detaillierte Ausführungen zur Plausibilisierung der Ergebnisse folgen in Abschnitt 3.6.1). Dazu kommt, dass zum Zeitpunkt der Plausibilisierung nicht mehr eruiert werden kann, *welche* Stimmabgaben missbräuchlich waren und diese folglich auch nicht mehr aus der Auszählung ausgeschlossen werden können.

Um einen Angriff auf individueller Basis zuverlässig erkennen und verhindern zu können, wäre nach jeder Stimmabgabe ein Abgleich mit dem Stimmregister vonnöten. Auf diese Weise könnten die Echtheit des verwendeten Stimmrechtsausweises verifiziert und Mehrfachstimmabgaben verunmöglicht werden. Wie in Abschnitt 3.2.3 bereits angedeutet, wäre eine denkbare

13 Eine Übersicht über mögliche Massnahmen gegen Ransomware-Angriffe findet sich im Internet unter https://www.newsd.admin.ch/newsd/message/attachments/90430.pdf.

Möglichkeit, zu diesem Zweck einen zusätzlichen Datamatrix-Code auf die Stimmrechtsausweise aufzudrucken (M2), der von den Gemeinden gescannt und mit dem Stimmregister abgeglichen werden könnte (zudem müsste eine manuelle Sperrung – beispielsweise im Fall von gestohlenen Stimmrechtsausweisen – ebenfalls möglich sein). Allerdings müsste dieser Abgleich vor der Trennung von Stimmrechtsausweisen und Stimmzettelkuverts stattfinden, im Idealfall gleich nach dem Eintreffen der (brieflichen) Stimmabgaben bei der Gemeinde. Es müsste, mit anderen Worten, also möglich sein, den Datamatrix-Code durch das Sichtfenster des noch verschlossenen Zustellkuverts zu scannen. In Gemeinden mit der Möglichkeit der elektronischen Stimmabgabe kommt eine derartige Lösung bereits zum Einsatz (zur Verhinderung von Mehrfachstimmabgaben werden alle brieflich eingelangten E-Voting-Stimmrechtsausweise mit einem Handscanner gegen den *Voting Card Manager* der Post geprüft; es wird also automatisch abgefragt, ob bereits eine elektronische Stimme auf dem Server der Post eingegangen ist). Mit Blick auf die – zumindest in näherer Zukunft noch – deutlich grössere Zahl der brieflichen Stimmabgaben ist allerdings fraglich, ob eine derartige Prüfung mit Handscannern auch in Gemeinden mit sehr vielen Stimmberechtigten effizient durchgeführt werden könnte oder ob dafür andere technische Lösungen nötig wären. Eine zukünftige Umsetzung einer solchen zusätzlichen Sicherheitsmassnahme wäre daher nicht nur mit Anpassungen bei der Produktion des Stimmmaterials und im Auszählungsprozess bei den Gemeinden verbunden, sondern auch mit technischen Herausforderungen.

Da jede Gemeinde selbst für die Sicherheit ihrer Briefkästen zuständig ist, lassen sich keine verallgemeinerbaren Aussagen über bereits existierende oder allfällig geplante Massnahmen zur Verhinderung von Diebstählen oder der Zerstörung von Stimmmaterial aus bzw. in Briefkästen der Gemeinden (B11) formulieren. Die Zerstörung einzelner Zustellkuverts, etwa durch den Einwurf von brennbarem Material, lässt sich zwar nur schwer vollends verhindern. Es sind jedoch verschiedene niederschwellige Massnahmen umsetzbar, mit denen Diebstähle effektiv verhindert werden können (z.B. durch das Anbringen eines Entnahmeschutzes, eines tieferliegenden Fachs für die eingeworfenen Kuverts oder durch eine Videoüberwachung sowie durch regelmässiges Leeren).

Mit Blick auf die Verletzlichkeit der IT-Infrastruktur der Post durch einen Cyberangriff (B12) gehen die Verfasser der Bedrohungsanalyse davon aus, dass ein allfälliger Angriff aufgrund der bestehenden Gegenmassnahmen (M10) auch im «Erfolgsfall» primär zu einer Verzögerung in der Zustellung führen, diese jedoch nicht längerfristig verunmöglichen würde.

Da die Post auch im regulären Geschäft stark fluktuierende Lasten bewältigen kann, etwa die alljährliche Zunahme der Brief- und Paketsendungen in der Vorweihnachtszeit, ist grundsätzlich davon auszugehen, dass sie über genügend grosse Kapazitäten verfügt, um dem Versuch einer mutwilligen Überlastung ihrer Infrastruktur durch eine sehr grosse Anzahl an brieflichen Sendungen (B13) standzuhalten. Auch für den – zumindest theoretisch – denkbaren Fall der «Überflutung» einer Gemeinde mit brieflichen Sendungen (B14) sind keine spezifischen Gegenmassnahmen vorgesehen. Zum einen ist ein solcher Angriff wenig wahrscheinlich, zum andern könnte die betroffene Gemeinde dessen Erfolg durch das Aufbieten zusätzlicher Helferinnen oder Helfer ohne grosse Mühe abschwächen oder gar vollständig abwenden.

Massnahme	Eingedämmte Bedrohungen	Status
M5: Plausibilisierung der Gemeindeergebnisse durch die Staatskanzlei	B10: Abgabe von gefälschtem Stimmmaterial (ebenso B3: Manipulation des Stimmregisters; B18: Manipulation der Auszählung durch Insiderinnen und Insider)	umgesetzt
M9: Prüfung aller Stimmabgaben durch Stimmbüro	B10: Abgabe von gefälschtem Stimmmaterial	umgesetzt
M10: Vorkehrungen der Post zum Schutz ihrer IT-Infrastruktur	B12: Überlastung der postalischen Services durch Cyberangriffe auf die Informationssysteme der Post	umgesetzt
M2: Zusätzlicher Datamatrix-Code auf Stimmrechtsausweis für Abgleich mit dem Stimmregister	B10: Abgabe von gefälschtem Stimmmaterial (ebenso B1: Diebstahl und Missbrauch von Stimmmaterial; B2: Fälschung von Stimmrechtsausweisen; B4: Inkonsistenzen im Stimmregister)	zu prüfen

3.5 Phase Lagerung in der Gemeinde

3.5.1 Einführung und Übersicht über Arbeitsschritte

Die vierte Phase im Prozess der Vorbereitung und Durchführung von Wahlen und Abstimmungen (siehe auch Abbildung 3) beinhaltet die Lagerung der bereits vor dem Wahl- oder Abstimmungssonntag eingelangten Stimmabgaben in der Gemeinde. Da der weitaus grösste Teil der stimmberechtigten Schweizerinnen und Schweizer ihre Stimmen brieflich abgibt, kommt der sicheren Aufbewahrung der Zustellkuverts bis zum Beginn der Auszählung eine besondere Bedeutung zu.[14]

Organisatorisch umfasst die Phase der Lagerung der Stimmabgaben in der Gemeinde zwei zeitlich aufeinanderfolgende Arbeitsschritte: die Lagerung der Zustellkuverts bis zur Prüfung der Gültigkeit der Stimmabgaben durch einen Ausschuss des Stimmbüros sowie die anschliessende Lagerung der verschlossenen Stimmzettelkuverts bis zum Beginn der Auszählung. Das Gesetz über Wahlen und Abstimmungen schreibt vor, dass die Stimmregisterführerin oder der Stimmregisterführer oder die Schreiberin oder der Schreiber des Stimmbüros gemeinsam mit einem Ausschuss desselbigen prüft, ob die brieflichen Stimmabgaben gültig sind (Art. 61 Abs. 1 WAG). Diese Prüfung ist nicht Bestandteil der Auszählung, sie kann daher auch bereits vor dem Wahl- oder Abstimmungswochenende erfolgen. In der Praxis werden die Stimmabgaben allerdings in vielen Gemeinden erst am Sonntag geprüft, da die Mitglieder der Stimmbüros erst dann zur Verfügung stehen. Bezüglich Lagerung hält Art. 61 Abs. 3 WAG zudem fest, dass die bei der Gemeinde eingegangenen Zustellkuverts bis zur Prüfung durch das Stimmbüro unter Verschluss gehalten werden müssen.

Wird eine Stimmabgabe vom Stimmbüro der Gemeinde als gültig taxiert – der Stimmrechtsausweis ist also aktuell und korrekt unterzeichnet und die Stimmzettel befinden sich in einem separaten Kuvert –, werden die Stimmzettelkuverts von den Stimmrechtsausweisen getrennt und bis zum Beginn der Auszählung separat aufbewahrt. Auf diese Weise bleibt das Stimmgeheimnis jederzeit gewahrt. Auch für diese zweite Phase der Lagerung in der Gemeinde schreibt das Gesetz wiederum ein verschlossenes Behältnis vor (Art. 61 Abs. 3 WAG).

[14] Im Kanton St.Gallen lag der durchschnittliche Anteil der brieflichen Stimmabgaben im Jahr 2024 gemäss einer Berechnung der Staatskanzlei bei rund 96 Prozent.

3.5.2 Potenzielle Bedrohungen

Hinsichtlich der Lagerung der brieflichen Stimmabgaben in den Gemeinden haben die Experten der UZH eine generelle Bedrohung identifiziert, je nach Zeitpunkt und Urheberschaft eines potenziellen Angriffs lassen sich zudem zwei weitere spezifische Bedrohungen ableiten.

ID	Beschreibung	Schadensausmass
B15	Zugriff auf gelagerte Stimmabgaben	HOCH
B16	Diebstahl und/oder Zerstörung von Zustellkuverts	NIEDRIG
B17	Manipulation, Austausch oder Einspeisung von (zusätzlichen) Stimmzetteln	NIEDRIG

Die **Bedrohung B15** besteht ganz generell in der Möglichkeit eines unberechtigten Zugriffs auf die zwischengelagerten Stimmabgaben. Je nachdem, welche Sicherheitsmassnahmen eine Gemeinde getroffen hat, ist ein erfolgreicher Angriff allerdings nur unter Anwendung von physischer Gewalt möglich, etwa um den Safe oder die Tür des Raums aufzubrechen, in dem die Stimmabgaben gelagert werden. Ein unbemerkter Zugriff wäre unter dieser Voraussetzung nur sehr schwer zu realisieren. Würde ein derartiger Angriff allerdings durch eine interne Person durchgeführt, die über den Lagerort Bescheid weiss und womöglich auch über den nötigen Zugang (z.B. Schlüssel oder PIN-Code für den Safe) verfügt, ist die Wahrscheinlichkeit deutlich höher, dass der Zugriff unbemerkt bleibt.

Sollte es einem Angreifer gelingen, unbemerkt physischen Zugriff auf die gelagerten Stimmabgaben zu erhalten, so ist zwischen zwei spezifischeren Bedrohungsszenarien zu unterschieden:

– Erfolgt der Zugriff vor der Prüfung der Gültigkeit der Stimmabgaben durch das Stimmbüro, ist denkbar, dass ein Teil der Zustellkuverts gestohlen und/oder zerstört wird (**B16**).[15]

– Sind die Stimmzettelkuverts zum Zeitpunkt des Zugriffs bereits von den Stimmrechtsausweisen getrennt, könnte ein Angreifer versuchen, Stimmzettel zu manipulieren oder auszutauschen oder zusätzliche Stimmzettel in den Auszählungsprozess einzuspeisen (**B17**).

Die Wahrscheinlichkeit, dass ein Angriff unerkannt gelingt, ist auch hier um ein Vielfaches grösser, wenn es sich beim Angreifer um eine interne Person handelt. Dies umso mehr, wenn diese Person auch über Zugang zum Reserve-Stimmmaterial (also zu echten, jedoch nicht verwendeten Stimmzetteln und Stimmzettelkuverts) verfügt. Im Fall von B17 kommt hinzu, dass der Nachweis eines mutmasslichen Angriffs auch mit forensischen Mitteln (z.B. Nachweis von Fingerabdrücken) deutlich schwieriger ist, weil im Rahmen der Prüfung der Gültigkeit der Stimmabgaben durch das Stimmbüro in der Regel bereits mehrere (autorisierte) Personen mit den Stimmzettelkuverts und den Stimmzetteln in Kontakt waren.

3.5.3 Bereits umgesetzte und mögliche zusätzliche Gegenmassnahmen

Obwohl die sichere Lagerung des Stimmmaterials und insbesondere der brieflich eingelangten Stimmabgaben in den Gemeinden eine besonders kritische Phase in der Vorbereitung und Durchführung von Wahlen und Abstimmungen darstellt, ist sie im geltenden Recht lediglich allgemein reguliert (M11). So hält Art. 61 WAG zwar fest, dass Zustellkuverts «unter Verschluss» bzw. Stimmzettelkuverts «in einem verschlossenen Behältnis» aufbewahrt werden müssen. Im Gesetz selbst wird jedoch nicht konkretisiert, was genau darunter zu verstehen ist und wer – und unter welchen Umständen – Zugang zum Stimmmaterial haben darf.

15 Im Fall eines Diebstahls von Zustellkuverts kann zudem auch die Verletzung des Stimmgeheimnisses nicht ausgeschlossen werden.

Entsprechend erfolgt die Lagerung je nach Gemeinde gemäss den eigens dafür definierten organisatorischen Sicherheitsvorkehrungen. Mit Blick auf die physische Zugriffskontrolle ist allerdings kaum eine angewendete Regelung bekannt, die sicherstellt, dass jeweils immer nur zwei Angestellte der Gemeinde gleichzeitig Zugang zum Safe mit dem Stimmmaterial haben (sofern Letzteres überhaupt in einem Safe aufbewahrt wird), was einer konsequenten Umsetzung des Vieraugenprinzips entsprechen würde. Stattdessen wird für die Überwachung typischerweise auf vertrauensvolle Einzelpersonen abgestellt. Das hat allerdings zur Folge, dass potenzielle Angriffe durch ebendiese Vertrauensträgerinnen und Vertrauensträger de facto kaum zu verhindern sind und in der Regel wohl auch nicht erkannt werden können.
Eine mögliche Massnahme, um die Sicherheit des Wahl- und Abstimmungsprozesses weiter zu verbessern, könnte deshalb darin bestehen, die bestehenden Vorgaben betreffend die korrekte Lagerung des Stimmmaterials in den Gemeinden zu konkretisieren (M12; beispielsweise in einer Verordnung der Regierung oder in einem Leitfaden von Kanton und Gemeinden). So könnte beispielsweise präzisiert werden, dass die Lagerung zwingend in einem Safe erfolgen muss (statt «lediglich» in einem abschliessbaren Schrank oder Raum) und dass sichergestellt sein muss, dass dieser lediglich von einer überschaubaren Anzahl an (berechtigten) Personen geöffnet werden kann – im Idealfall nur von zwei Personen gemeinsam[16] (B15) –, um einen Diebstahl oder die Zerstörung von Stimmmaterial (B16) zu verhindern. Darüber hinaus wäre ebenfalls prüfenswert, ob die bestehenden Vorgaben dahingehend erweitert werden sollten, dass sie in Zukunft auch die Lagerung des Reserve-Stimmmaterials umfassen (M13). Diesbezüglich gibt es bislang keine spezifischen Vorschriften. Es kann jedoch davon ausgegangen werden, dass mit einer fortlaufenden Protokollierung des jeweils aktuellen Bestands – idealerweise ebenfalls im Vieraugenprinzip – und einer zugriffssicheren Lagerung (analog zu oder gemeinsam mit den bereits eingelangten Stimmabgaben) ein unbemerkter Austausch oder eine Einspeisung von zusätzlichen Stimmzetteln (B17) weitestgehend verhindert werden könnten.

Selbst wenn derartige Angriffe schwierig zu skalieren sind, weil (zu) grosse Unterschiede in der Anzahl der Stimmrechtsausweise und der Stimmzettel auffallen und eine Ausweitung auf mehrere Gemeinden zwingend Absprachen zwischen Vertrauensträgerinnen und Vertrauensträgern dieser verschiedenen Gemeinden bedingen würde, kann bereits ein (entdeckter) Betrugsversuch einer Einzelperson in einer Gemeinde einen beträchtlichen Reputationsschaden nach sich ziehen, wie der so genannte «Fall Frauenfeld» (weitere Ausführungen dazu folgen in Abschnitt 5.1) gezeigt hat. Als generelle Erkenntnis kann daher festgehalten werden, dass für den Zugriff auf Stimmmaterial während eines laufenden Urnengangs grundsätzlich wann immer möglich das Vieraugenprinzip angewendet werden sollte.

Massnahme	**Eingedämmte Bedrohungen**	**Status**
M11: Gesetzliche Vorgaben betreffend Lagerung	B15: Zugriff auf gelagerte Stimmabgaben (ebenso B22: Manipulation des gelagerten Stimmmaterials)	umgesetzt (aber ungenügend)
M12: Weiterführende Vorgaben betreffend sichere Lagerung	B15: Zugriff auf gelagerte Stimmabgaben B16: Diebstahl und/oder Zerstörung von Zustellkuverts (ebenso B22: Manipulation des gelagerten Stimmmaterials)	zu prüfen
M13: Reserve-Stimmmaterial: sichere Lagerung und fortlaufende Protokollierung	B17: Manipulation, Austausch oder Einspeisung von (zusätzlichen) Stimmzetteln (ebenso B22: Manipulation des gelagerten Stimmmaterials)	zu prüfen

16 Eine kostengünstige Möglichkeit, dies zu erreichen, besteht beispielsweise darin, unterschiedlichen Personen oder Personengruppen jeweils nur die erste oder die zweite Hälfte des PIN-Codes für den Safe anzuvertrauen.

3.6 Phase Auszählung

3.6.1 Einführung und Übersicht über Arbeitsschritte

Die fünfte und unmittelbar zentrale Phase des Wahl- und Abstimmungsprozesses ist jene der Auszählung. Sie lässt sich in vier aufeinanderfolgende Arbeitsschritte unterteilen. Typischerweise erfolgt die Auszählung am Morgen des Wahl- oder Abstimmungssonntags, unter bestimmten Umständen (bei Proporzwahlen, Erneuerungswahlen der Gemeinde sowie bei mehr als 10'000 Stimmberechtigten) dürfen die Gemeinden aber auch bereits am Samstag mit der Auszählung beginnen.

Im ersten Schritt öffnet das Stimmbüro der Gemeinde die Zustellkuverts und prüft die Gültigkeit der darin enthaltenen Stimmrechtsausweise (sofern diese Prüfung nicht bereits vorgängig erfolgt ist; siehe Abschnitt 3.5.1). Anschliessend werden die Stimmrechtsausweise von den Stimmzettelkuverts getrennt, um sicherzustellen, dass das Stimmgeheimnis gewahrt bleibt. Als nächstes werden die Stimmzettelkuverts geöffnet und die darin enthaltenen Stimmzettel nach Vorlagen getrennt und gezählt. Je nachdem, um welche Art von Vorlage es sich handelt, folgen weitere Sortierrunden – im Fall einer Abstimmung werden in der Regel separate Stapel für die Ja-Stimmen, die Nein-Stimmen, die leeren und die ungültigen Stimmzettel gebildet – und zum Abschluss wird jeder Stapel noch einmal einzeln gezählt. Damit ist die eigentliche Ergebnisermittlung abgeschlossen.

Im zweiten Schritt werden die ermittelten Zahlen dann von der für Wahlen und Abstimmungen verantwortlichen Person der Gemeinde im Ergebnisermittlungssystem erfasst. Seit dem Jahr 2023 wird im Kanton St.Gallen als Ergebnisermittlungssystem die Applikation *VOTING Ausmittlung* der Firma Abraxas verwendet. Zum Zweck einer lückenlosen Nachvollziehbarkeit verfügt jede Benutzerin und jeder Benutzer über ein persönliches Login und sämtliche Eingaben werden in Transaktions-Logs aufgezeichnet. Im Fall von eidgenössischen und kantonalen Vorlagen werden die Gemeindeergebnisse anschliessend in einem dritten Schritt für die Plausibilisierung durch die Staatskanzlei freigegeben. Damit verschiebt sich der Prozess von der kommunalen auf die kantonale Ebene.

Die Staatskanzlei prüft die von der Gemeinde freigegebenen Zahlen auf deren Plausibilität, indem sie die Ergebnisse aller Vorlagen miteinander sowie mit den Ergebnissen aller anderen, zum Zeitpunkt der Prüfung bereits ausgezählten Gemeinden vergleicht. Zu diesem Zweck kommt die vom Statistischen Amt des Kantons Zürich entwickelte *PlausiApp* zur Anwendung, ein statistisches Plausibilisierungs-Tool, das von den Kantonen Zürich, St.Gallen und Thurgau seit mehreren Jahren eingesetzt wird.[17] Fördert die Plausibilitätsprüfung Auffälligkeiten zutage, werden die betreffenden Gemeinden kontaktiert. Sobald die (Teil-)Ergebnisse aller Gemeinden geprüft und – soweit nötig – korrigiert sind, werden sie im vierten und letzten Schritt der Auszählung zum kantonalen Endergebnis zusammengetragen und – im Fall von eidgenössischen Vorlagen – über einen sicheren Kanal (SEDEX) an den Bund übermittelt. Anschliessend veröffentlicht die Staatskanzlei das vorläufige Endergebnis auf der Ergebnis-Webseite des Kantons (wab.sg.ch). Amtlich werden die Ergebnisse von eidgenössischen oder kantonalen Wahlen und Abstimmungen allerdings erst mit der Veröffentlichung im Amtsblatt.[18] Diese erfolgt im Kanton St.Gallen in aller Regel acht Tage nach dem Wahl- oder Abstimmungssonntag.

---

17 Weitere Informationen zur *PlausiApp* und den statistischen Tests, die damit durchgeführt werden, finden sich im Internet unter https://machinelearningzh.github.io/plausi/.

18 Ab diesem Zeitpunkt läuft grundsätzlich auch die dreitägige Frist für allfällige Wahl- oder Abstimmungsbeschwerden (vgl. Art. 108 Abs. 2 WAG: «Die Beschwerde muss innert dreier Tage seit Bekanntwerden des Beschwerdegrunds, spätestens am dritten Tag nach der amtlichen Veröffentlichung des Ergebnisses, eingeschrieben eingereicht werden.»).

3.6.2 Potenzielle Bedrohungen

Mit Blick auf die Auszählung der eingegangenen Stimmen und die dazugehörige Publikation der Ergebnisse hat die UZH vier potenzielle Bedrohungen identifiziert.

ID	Beschreibung	Schadensausmass
B18	Manipulation der Auszählung durch Insiderinnen oder Insider	HOCH
B19	Manipulation oder Überlastung der Online-Infrastruktur des Ergebnisermittlungs-systems	HOCH
B20	Manipulation oder Überlastung der E-Counting-Software	HOCH
B21	Manipulation der Publikation der vorläufigen Ergebnisse	MITTEL

Unter der **Bedrohung B18** werden verschiedene mögliche Manipulationen der Auszählung durch Vertrauensträgerinnen und Vertrauensträger, also durch beteiligte Personen subsumiert. So wäre beispielsweise denkbar, dass eine oder mehrere Stimmenzählerinnen oder ein oder mehrere Stimmzähler einen Teil der Stimmzettel verändern oder missbräuchlich für ungültig erklären könnten. Ebenso kann nicht vollends ausgeschlossen werden, dass die für Wahlen und Abstimmungen verantwortliche Person einer Gemeinde bestochen oder erpresst wird, dass sie falsche Zahlen im Ergebnisermittlungssystem erfasst. Allerdings dürften sich die Auswirkungen einer derartigen Manipulation primär auf die betroffene Gemeinde beschränken. Auf das Ergebnis einer schweizweiten Abstimmung hätte eine Manipulation der Auszählung auf lokaler Ebene hingegen wohl in den allermeisten Fällen keinen statistisch relevanten Effekt. Nichtsdestoweniger können aber gerade im Fall von kommunalen Wahlen auch bereits verhältnismässig geringe Veränderungen signifikante Auswirkungen haben und das Ergebnis messbar verfälschen (an dieser Stelle sei abermals auf Abschnitt 5.1 und den dort diskutierten «Fall Frauenfeld» verwiesen).

Die **Bedrohung B19** beschreibt das Szenario eines Angriffs auf den Betrieb bzw. auf die Infrastruktur von *VOTING Ausmittlung*. Das Ergebnisermittlungssystem ist insbesondere bei (Proporz-)Wahlen ein nahezu unverzichtbares Hilfsmittel, da es – im Vergleich zu einer manuellen Auszählung – eine rasche und effiziente Ermittlung aller für die Sitzverteilung benötigten Werte ermöglicht. Würde es einem Angreifer gelingen, die Datenbank des Ergebnisermittlungssystems zu manipulieren, könnte er theoretisch den Ausgang einer Abstimmung oder eben die Verteilung der Sitze im Fall einer Wahl beeinflussen. Eine mutwillige Überlastung der Infrastruktur von *VOTING Ausmittlung*, beispielsweise durch einen so genannten «Denial-of-Service»-Angriff, könnte zudem zu Verzögerungen bei der Ergebnisermittlung führen.

Die **Bedrohung B20** bezieht sich auf einen Spezialfall der Auszählung: das Einscannen und computergestützte Auswerten von maschinenlesbaren Stimmzetteln (E-Counting). Dieses Verfahren kommt aktuell in drei Gemeinden im Kanton St.Gallen zum Einsatz (in den Städten St.Gallen und Rapperswil-Jona sowie zur Auszählung der Stimmabgaben der Auslandschweizerinnen und Auslandschweizer).[19] Für das Scanning kommt die Software «SuisseVote» der Firma Kaiser Data AG zum Einsatz. Sie verwendet die Technik der *Optical Mark Recognition* (OMR), die eine Erkennung von Markierungen auf Papier ermöglicht und oft auch zur automatischen Auswertung von Formularen oder Multiple-Choice-Tests eingesetzt wird. Aktuell werden die Ergebnisse nach dem Scannen anhand eines Protokolls, das durch die Scan-Software generiert wird, manuell von der für Wahlen und Abstimmungen verantwortlichen Person der Gemeinde in *VOTING Ausmittlun*g übertragen. In einem laufenden Projekt ist die Staatskanzlei

19 In anderen Kantonen, namentlich solchen aus der Romandie, ist der Einsatz von E-Counting bereits deutlich weiter verbreitet. Auch im Kanton St.Gallen planen schon zusätzliche Gemeinden, ihre Stimmzettel künftig ebenfalls zu scannen, statt von Hand auszuwerten.

jedoch dabei, gemeinsam mit Abraxas und Kaiser Data AG eine Schnittstelle zu realisieren, über welche die E-Counting-Ergebnisse direkt ins Ergebnisermittlungssystem übertragen werden können. Zu diesem Zweck wird in Zukunft eine signierte Ergebnisdatei in einem standardisierten Format (eCH-0222)[20] verwendet, die mittels USB-Stick in *VOTING Ausmittlung* eingelesen werden kann. Ein potenzieller Angreifer könnte versuchen, sich Zugang zum Computer zu verschaffen, auf dem die Scan-Software betrieben wird, mit dem Ziel, die Software zu manipulieren und dadurch die Ergebnisermittlung zu behindern oder das Ergebnis zu verfälschen. Für den Fall, dass der Scan-Computer an ein Netzwerk angeschlossen sein sollte (beispielsweise um neue Releases der Software einzuspielen), ist denkbar, dass auch dieses für einen Angriff genutzt werden könnte. Allerdings verlangt der Bundesrat in einem für alle Kantone und Gemeinden verbindlichen Kreisschreiben[21], dass Abstimmungsergebnisse, die mit technischen Mitteln ermittelt wurden, in jedem Fall durch den Vergleich mit einer manuell ausgezählten, repräsentativen Zufallsstichprobe plausibilisiert werden müssen. Ein unbemerkter Angriff wäre daher für einen internen wie für einen externen Angreifer mit einem hohen Aufwand verbunden. Zudem bliebe im Fall eines erkannten Angriffs immer noch die Möglichkeit der manuellen Auszählung der Stimmzettel durch das Stimmbüro, auch wenn eine solche gerade in grossen Gemeinden natürlich eine beträchtliche Verzögerung zur Folge hätte.

Die **Bedrohung B21** beschreibt die Möglichkeit, dass die Übermittlung der ausgezählten Ergebnisse manipuliert werden könnte. Dieses Szenario wurde 2019 im Rahmen einer wissenschaftlichen Studie der ETH Zürich beschrieben.[22] So ist denkbar, dass auf Gemeindeebene die zentralisierte Ergebniserfassung oder auf kantonaler Ebene die Übermittlung der vorläufigen Endergebnisse an die Ergebnis-Webseite des Kantons das Ziel eines Angriffs werden könnten. Darüber hinaus könnte ein Angreifer versuchen, gefälschte Protokolle mit abgeänderten vorläufigen Ergebnissen in Umlauf bringt (viele Gemeinden veröffentlichen ihre Ergebnisse nach Beendigung der Auszählung jeweils auf ihrer Webseite). Zwar ist die Erkennung eines derartigen Angriffs durch den Abgleich der verfälschten Ergebnisse mit den vom Stimmbüro unterzeichneten Protokollen, welche die Gemeinden der Staatskanzlei zustellen müssen, gut möglich – zumindest im Nachhinein. Dennoch könnten damit bis zur Entdeckung der Manipulation und der Richtigstellung durch den Kanton oder die betroffene Gemeinde falsche Erwartungen geweckt werden.

3.6.3 Bereits umgesetzte und mögliche zusätzliche Gegenmassnahmen

Mit Blick auf mögliche Manipulationen der Auszählung durch beteiligte Personen (B18) steht insbesondere der Fall im Fokus, in dem eine einzelne Person allein Zugang zum Stimmmaterial oder zum Ergebnisermittlungssystem hat. Wird hingegen das Vieraugenprinzip (M14) konsequent angewendet, wird dadurch jeder potenzielle Angriff deutlich erschwert. Kritische Prozessschritte sollten deshalb grundsätzlich immer in Zweierteams durchgeführt werden. Im Idealfall sind diese zudem aus Personen mit unterschiedlichen Interessen zusammengesetzt (z.B. aus Vertreterinnen oder Vertretern verschiedener Parteien), da so ein grösserer Anreiz zur gegenseitigen Kontrolle besteht. Eine mögliche Massnahme, um das Bewusstsein für die Kritikalität der einzelnen Prozessschritte weiter zu fördern, könnte darin bestehen, den Stimmbüros eine Checkliste für die Auszählung von Wahlen und Abstimmungen zur Verfügung zu stellen (M15). Eine solche könnte von der Staatskanzlei gemeinsam mit den Gemeinden erarbeitet werden. Darüber hinaus empfiehlt es sich, gerade die Anzahl der unveränderten Wahlzettel im Fall von Proporzwahlen immer auf mehrere, unterschiedliche Weisen zu erheben (siehe dazu auch Abschnitt 5.1) und die ermittelten Zahlen anschliessend miteinander zu vergleichen. Zudem sollten Unterlagen, anhand derer die Korrektheit der Auszählung nachgeprüft werden kann

20 Vgl. https://www.ech.ch/de/ech/ech-0222/1.1.

21 Vgl. BBl 2018, 7683.

22 Die Studie mit dem Titel «Cyber-Risks in Paper Voting» ist im Internet abrufbar unter arxiv.org/abs/1906.07532.

(Bundblätter, Protokolle usw.), ebenfalls immer von mehreren Mitgliedern des Stimmbüros unterschrieben werden.

Neben solchen prozeduralen Kontrollen tragen auch verschiedene technische Vorkehrungen zur Erhöhung der Sicherheit des Auszählungsprozesses bei. So kommen in *VOTING Ausmittlung* im Unterschied zur Vorgängerlösung nur noch personalisierte Logins in Kombination mit einer 2-Faktor-Authentifizierung (2FA) zum Einsatz und sämtliche Eingaben und Mutationen im System werden in Form von Transaktions-Logs protokolliert (M16). Darüber hinaus müssen zentrale Prozessschritte wie die Freigabe der Gemeindeergebnisse für die Plausibilisierung durch die Staatskanzlei oder die Auslösung der Sitzverteilung im Fall von Proporzwahlen von den dafür verantwortlichen Personen ebenfalls mittels 2FA bestätigt werden. Dadurch kann verhindert werden, dass eine nicht autorisierte Person unbemerkt Aktionen oder Berechnungen auslöst (etwa in dem sie sich unbeobachtet an den Computer der verantwortlichen Person setzt), die zu einem falschen Ergebnis oder einer Verzögerung der Auszählung führen könnten.

Neben mutwilligen Manipulationen müssen bei der Ergebnisermittlung jedoch auch unabsichtliche Fehler beim Erfassen von Wahl- oder Abstimmungsergebnissen mitberücksichtigt werden. Sowohl *VOTING Ausmittlung* als auch bereits die Vorgängerlösung führen daher für sämtliche Arten von Geschäften standardmässig mathematische Validierungen der erfassten Werte durch, um sicherzustellen, dass diese (zumindest) rechnerisch möglich sind (M17). Diese mathematischen Validierungsprüfungen sind nicht zu verwechseln mit der in Abschnitt 3.6.1 bereits erläuterten «inhaltlichen» Plausibilisierung der Gemeindeergebnisse durch die Staatskanzlei (M5). Beide tragen aber dazu bei, bis dahin unbemerkte Fehler oder Manipulationen kenntlich zu machen. Zudem werden die Ergebnisse aller eidgenössischen und kantonalen Wahlen und Abstimmungen nach der Plausibilisierung durch die Staatskanzlei veröffentlicht. Sie können damit nachträglich also auch durch unabhängige Beobachterinnen und Beobachter jederzeit nachvollzogen und überprüft werden.

Hinsichtlich der getroffenen Vorkehrungen gegen potenzielle (Cyber-)Angriffe auf die Online-Infrastruktur des Ergebnisermittlungssystems (B19) muss unterschieden werden zwischen Massnahmen, die dazu dienen, solche Angriffe zu erkennen, und Massnahmen, um diese zu verhindern. Eine bereits existierende Massnahme, mit der allfällige Manipulationen in der Datenbank von *VOTING Ausmittlung* erkannt werden können, insbesondere im Fall der besonders kritischen Proporzwahlen, sind die so genannten Bundkontrollen (M18)[23]. Dabei werden die Stimmzettel von zufällig ausgewählten Bunden – bzw. die auf diesen Stimmzetteln aufgeführten Namen der Kandidierenden, die Stimmen erhalten haben – von den Mitgliedern des Stimmbüros mit den im Ergebnisermittlungssystem erfassten Einträgen für die gleichen Stimmzettel abgeglichen. Im Fall einer Manipulation der Datenbank von *VOTING Ausmittlung* käme es unweigerlich zu Abweichungen, wodurch eine unerkannte Durchführung eines derartigen Angriffs deutlich erschwert wird.

Was Massnahmen zur Verhinderung von Cyberangriffen angeht, kann namentlich die Bedrohung einer Überlastung der Online-Infrastruktur des Ergebnisermittlungssystems durch so genannte «Denial-of-Service»-Angriffe (kurz «DoS-Angriffe») durch operative Vorkehrungen (z.B. einen Härtetest der Software durch «Penetration Testing»[24] oder den Einsatz von «Scrubbing-

---

23 Bei Proporzwahlen werden die veränderten Stimmzettel nach Listen sortiert und zu Bunden zusammengefasst. Der Umfang dieser Bunde variiert zwischen den Gemeinden, wobei typischerweise mit 25er- oder 50er-Bunden gearbeitet wird. Jeder Bund und jeder Stimmzettel innerhalb eines Bundes wird nummeriert und ist damit sowohl bei der Erfassung im Ergebnisermittlungssystem als auch im Rahmen der nachfolgenden Bundkontrolle jederzeit identifizierbar.

24 Unter einem Penetration Test versteht man einen kontrollierten Angriff durch einen unabhängigen Dienstleister mit dem Ziel, Schwachstellen in einem System zu identifizieren und deren Ausnutzbarkeit zu evaluieren.

Diensten»[25]) auf Seiten der Systemanbieterin minimiert werden (M19).[26] Vor dem ersten Einsatz von *VOTING Ausmittlung* hat Abraxas verschiedene solcher Härtetests sowie ein zweistufiges Bug-Bounty-Programm (siehe dazu Abschnitt 4.6) durchgeführt. Zudem werden sämtliche VOTING-Applikationen von einer vorgeschalteten *Web Application Firewall* (WAF) geschützt. Um volumetrische Netzwerkangriffe, eine Spezialform von DoS-Angriffen, abzuwehren, sind die VOTING-Applikationen darüber hinaus nur im kantonsinternen KOMSG-Netz erreichbar. Dadurch können die Server nicht direkt angegriffen werden. Zusätzlich werden die «DDoS»-Schutzleistungen der Internet Service Provider (wie zum Beispiel Swisscom, Sunrise oder UPC/Cablecom) genutzt.

Die einwandfreie Funktionsweise des E-Counting-Systems sowie die Korrektheit der damit ermittelten Ergebnisse (B20) werden aktuell primär durch die vom Bund vorgeschriebenen Plausibilitätsprüfungen der E-Counting-Ergebnisse (M20) gesichert. Sobald die sich gegenwärtig in der Realisierung befindende Schnittstelle zu *VOTING Ausmittlung* in Betrieb ist, können die Ergebnisse zudem mittels einer signierten Ergebnisdatei (M21) direkt ins Ergebnisermittlungssystem eingelesen werden. Durch die Prüfung der Signaturen kann einwandfrei sichergestellt werden, dass die Dateien auf dem Weg ins Ergebnisermittlungssystem nicht verändert wurden und dem ursprünglichen Stand aus dem E-Counting entsprechen, was die Sicherheit des Prozesses zusätzlich erhöht. Zudem wird durch den Wegfall der händischen Erfassung der gescannten Ergebnisse auch eine potenzielle Fehlerquelle eliminiert. Denkbar wäre, dass der Kanton darüber hinaus weiterführende Vorgaben bezüglich der Sicherheit der eingesetzten Scan-Computer machen würde. So könnte beispielsweise vorgeschrieben werden, dass die Geräte grundsätzlich ohne Netzzugang betrieben werden müssen oder dass darauf neben der Scan-Software keine weiteren Programme installiert sein dürfen. Da die Betriebskonzepte der Gemeinden, in denen E-Counting bereits zum Einsatz kommt, schon heute die Verwendung von Offline-Geräten vorsehen, sind aktuell allerdings keine zusätzlichen Massnahmen in diese Richtung geplant.

Eine Manipulation der vom Kanton oder einer Gemeinde veröffentlichten vorläufigen Ergebnisse (B21) kann dadurch erschwert werden, dass die betreffenden Protokolle digital signiert werden (M22). Der Kanton St.Gallen hat im Frühjahr 2025 mittels öffentlicher Ausschreibung eine entsprechende Lösung (*DeepSign*) beschafft und diese wird aktuell für die Signierung der Protokolle in *VOTING Ausmittlung* eingebaut. Die Übermittlung der vorläufigen Ergebnisse aus *VOTING Ausmittlung* an die Ergebnis-Webseite des Kantons erfolgt bereits heute in Form einer verschlüsselten zip-Datei, die über eine mit SSL gesicherte Verbindung übertragen wird. In dieser Hinsicht sind aktuell keine weiterführenden Massnahmen vorgesehen.

---

25 Mit einem Scrubbing-Dienst wird der Netzwerkverkehr eines Services an einen kommerziellen Dienstleiter weiterleitet, welcher diesen dann säubert (d.h. er filtert allfällige bösartige «Pakete» heraus und leitet lediglich die gutartigen an den Servicebetreiber weiter).

26 Wird ein DoS-Angriff dadurch skaliert, dass er durch mehrere Angreifer (gleichzeitig) ausgeführt wird, spricht man auch von einem «Distributed-Denial-of-Service»- oder kurz DDoS-Angriff.

Massnahme	Eingedämmte Bedrohungen	Status
M5: Plausibilisierung der Gemeindeergebnisse durch die Staatskanzlei	B18: Manipulation der Auszählung durch Insiderinnen oder Insider (ebenfalls B3: Manipulation des Stimmregisters; B10: Abgabe von gefälschtem Stimmmaterial)	umgesetzt
M14: Prozedurale Kontrollen (Vieraugenprinzip)	B18: Manipulation der Auszählung durch Insiderinnen oder Insider	umgesetzt
M16: 2-Faktor-Authentifizierung und Transaktions-Logs	B18: Manipulation der Auszählung durch Insiderinnen oder Insider	umgesetzt
M17: Mathematische Validierungsprüfungen	B18: Manipulation der Auszählung durch Insiderinnen oder Insider	umgesetzt
M18: Bundkontrolle	B19: Manipulation oder Überlastung der Online-Infrastruktur des Ergebnisermittlungssystems	umgesetzt
M19: Härtetests der Software und Web Application Firewall	B19: Manipulation oder Überlastung der Online-Infrastruktur des Ergebnisermittlungssystems	umgesetzt
M20: Plausibilitätsprüfungen der E-Counting-Ergebnisse (durch Bund vorgeschrieben)	B20: Manipulation oder Überlastung der E-Counting-Software	umgesetzt
M21: Digitale Signierung der Ergebnisdateien	B20: Manipulation oder Überlastung der E-Counting-Software	in Umsetzung
M22: Digitale Signierung der Protokolle und verschlüsselte Übermittlung an Ergebnis-Webseite	B21: Manipulation der Publikation der vorläufigen Ergebnisse	in Umsetzung
M15: Definition von kritischen Prozessschritten und Erarbeitung einer entsprechenden Checkliste für Stimmbüros	B18: Manipulation der Auszählung durch Insiderinnen oder Insider	zu prüfen

3.7 Phase Erwahrung

3.7.1 Einführung und Übersicht über Arbeitsschritte

Auf die Auszählung der Stimmen folgt als sechste Phase im Prozess der Vorbereitung und Durchführung von Wahlen und Abstimmungen jene der Erwahrung der Ergebnisse. Nach der Veröffentlichung der Ergebnisse im Amtsblatt und dem Ablauf der dreitägigen Beschwerdefrist (siehe dazu auch Abschnitt 3.6.1) stellt die Regierung im Fall von kantonalen Wahlen oder Abstimmungen das endgültige Ergebnis fest.[27] Mit dieser so genannten «Erwahrung», die anschliessend auch im Amtsblatt veröffentlicht wird, ist der Rechtsweg abgeschlossen und das Ergebnis kann nicht mehr geändert werden. Voraussetzung dafür, dass die Regierung das endgültige Ergebnis einer Wahl oder einer Abstimmung feststellen kann, ist daher, dass die Beschwerdefrist ungenutzt verstrichen ist oder dass allfällige Beschwerden rechtskräftig erledigt sind (Art. 111 Abs. 1 WAG).

Da die Möglichkeit besteht, dass bei Bekanntwerden allfälliger Unregelmässigkeiten eine Nachzählung der Ergebnisse einer oder mehrerer Gemeinden angeordnet wird (entweder durch die Regierung als leitende Behörde oder durch ein Gericht im Rahmen eines Beschwerdeverfahrens), müssen die ausgezählten Stimmzettel bis zur Erwahrung durch die Regierung in allen Gemeinden noch einmal sicher verpackt und versiegelt aufbewahrt werden (Art. 87 WAG).

[27] Im Fall von eidgenössischen Wahlen oder Abstimmungen erfolgt die Erwahrung der Ergebnisse gemäss Art. 15 des Bundesgesetzes über die politischen Rechte (SR 161.1; abgekürzt BPR) durch den Bundesrat.

Erst nach der Feststellung des endgültigen Ergebnisses und des entsprechenden Bescheids der Staatskanzlei zuhanden der für Wahlen und Abstimmungen verantwortlichen Personen der Gemeinden darf das Stimmmaterial vernichtet werden.

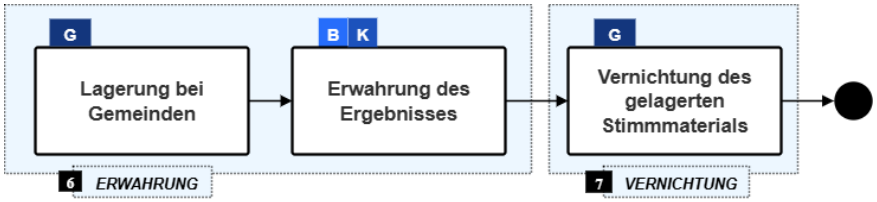

Abbildung 4: Erwahrung und Vernichtung des Stimmmaterials (Quelle: UZH)

3.7.2 Potenzielle Bedrohungen

Im Hinblick auf die Lagerung des Stimmmaterials nach der Auszählung und die Erwahrung der Ergebnisse hat die UZH zwei potenzielle Bedrohungen identifiziert.

ID	Beschreibung	Schadensausmass
B22	Manipulation des gelagerten Stimmmaterials	MITTEL
B23	Verfrühte Vernichtung des Stimmmaterials aufgrund eines gefälschten Erwahrungs-bescheids	NIEDRIG

Die **Bedrohung B22** ähnelt den in Abschnitt 3.5.2 bereits besprochenen Bedrohungen B15 bis B17. Sollte es einem Angreifer gelingen, sich unbemerkt Zugang zum gelagerten Stimm-material zu verschaffen, könnte das Ergebnis einer allfälligen Nachzählung dadurch manipuliert werden, dass Stimmmaterial entweder entfernt und/oder zerstört wird oder dass zusätzliche Stimmzettel zum gelagerten Material hinzugefügt werden (siehe auch Ausführungen zum «Fall Frauenfeld» in Abschnitt 5.1). In beiden Fällen wäre eine exakte Nachzählung zwar möglich, das Ergebnis dieser Auszählung wäre jedoch bereits verfälscht. Die Hürden für die Anordnung einer Nachzählung sind allerdings hoch (neben der Feststellung einer Unregel-mässigkeit verlangt Art. 83 WAG auch, dass diese «nach Art und Umfang geeignet sein muss, das Ergebnis wesentlich zu beeinflussen») und Nachzählungen dementsprechend selten.

Die **Bedrohung B23** beinhaltet die Möglichkeit, dass einzelne oder mehrere Gemeinden mit einer gefälschten Mitteilung betreffend die Erwahrung der Ergebnisse einer Wahl oder Abstim-mung dazu verleitet werden könnten, das entsprechende Stimmmaterial zu früh zu vernichten. Da die Gemeinden in der Durchführung von Wahlen und Abstimmungen erfahren sind, würde ein verfrüht oder auf einem unerwarteten Weg eintreffender Bescheid, dass das Stimmmaterial vernichtet werden kann, jedoch mit einer hohen Wahrscheinlichkeit auffallen. Dazu kommt, dass Nachzählungen wie bereits erwähnt selten sind. Nichtsdestotrotz wäre es problematisch, wenn auch nur eine einzige Gemeinde ihr Stimmmaterial zu früh vernichten würde, da dadurch eine umfassende Nachzählung de facto verunmöglicht würde.

3.7.3 Bereits umgesetzte und mögliche zusätzliche Gegenmassnahmen

Analog zur Lagerung des Stimmmaterials vor der Auszählung und den Bedrohungen, die sich aus einem unrechtmässigen Zugriff auf selbiges ergeben können (B15 bis B17), bestehen die wirkungsvollsten Massnahmen gegen eine (nachträgliche) Manipulation des Stimmmaterials (B22) in der konsequenten Anwendung des Vieraugenprinzips in der Gemeinde – namentlich mit Blick auf den Zugang zum Safe, in dem die ausgezählten Stimmzettel und Stimmrechts-ausweise aufbewahrt werden (M12) – sowie der fortlaufenden Protokollierung des aktuellen Bestands an Reserve-Material (M13). Aktuell gibt es jedoch (noch) keine verbindlichen Vor-

gaben dazu, wie diese Massnahmen umgesetzt werden müssen (siehe auch Ausführungen in Abschnitt 3.5.3). Die ergriffenen Massnahmen unterscheiden sich demnach von Gemeinde zu Gemeinde.

Das Risiko einer verfrühten Vernichtung des Stimmmaterials aufgrund eines gefälschten Erwahrungsbescheids (B23) wird einerseits dadurch abgeschwächt, dass die geltenden gesetzlichen Bestimmungen (M23) klar festhalten, dass die Gemeinden ihr Stimmmaterial in jedem Fall bis mindestens einen Monat nach dem Wahl- oder Abstimmungssonntag sicher verpackt und versiegelt aufbewahren müssen (Art. 87 WAG). Zu diesem Zeitpunkt hat die Regierung in aller Regel bereits das endgültige Ergebnis festgestellt. Darüber hinaus haben die Gemeinden jederzeit die Möglichkeit, sich auf einer zu diesem Zweck eingerichteten Seite im kantonseigenen Intranet (M24) über den aktuellen Stand der Erwahrungen zu informieren und auf diese Weise die Korrektheit einer möglicherweise als «zweifelhaft» empfundenen Aufforderung zu verifizieren.

Massnahme	**Eingedämmte Bedrohungen**	**Status**
M23: Gesetzliche Vorgaben betreffend Aufbewahrung von sicher verpacktem und versiegeltem Stimmmaterial	B23: Verfrühte Vernichtung des Stimmmaterials aufgrund eines gefälschten Erwahrungsbescheids	umgesetzt
M24: Intranetseite zum Stand der Erwahrungen	B23: Verfrühte Vernichtung des Stimmmaterials aufgrund eines gefälschten Erwahrungsbescheids	umgesetzt
M12: Weiterführende Vorgaben betreffend sichere Lagerung	B22: Manipulation des gelagerten Stimmmaterials (ebenso B15: Zugriff auf gelagerte Stimmabgaben; B16: Diebstahl und/oder Zerstörung von Zustellkuverts)	zu prüfen
M13: Reserve-Stimmmaterial: sichere Lagerung und fortlaufende Protokollierung	B22: Manipulation des gelagerten Stimmmaterials (ebenso B17: Manipulation, Austausch oder Einspeisung von [zusätzlichen] Stimmzetteln)	zu prüfen

3.8 Phase Vernichtung

Die siebte und letzte Phase im Prozess der Vorbereitung und Durchführung von Wahlen und Abstimmungen umfasst die Vernichtung des physischen Stimmmaterials nach der Erwahrung durch den Bundesrat (bei eidgenössischen Abstimmungen) oder durch den neu gewählten Nationalrat (bei den Nationalratswahlen) bzw. durch die Regierung (bei kantonalen Wahlen und Abstimmungen). In dieser Phase wurden keine relevanten Bedrohungen identifiziert, da das endgültige Ergebnis bereits festgestellt wurde und der Rechtsweg damit abgeschlossen ist. Zudem enthalten die Stimmzettel keine Informationen, die datenschutzrechtlichen Belangen genügen müssten. Einzig auf den Stimmrechtsausweisen finden sich personenbezogene Angaben. Im Fall eines Angriffs, beispielsweise des Diebstahls der Stimmrechtsausweise vor deren endgültiger Vernichtung, stellt eine Verletzung der Privatsphäre der Stimmenden daher die einzige mögliche Bedrohung dar. Da die Stimmrechtsausweise bereits vor der Auszählung von den Stimmzetteln separiert wurden, ist das Stimmgeheimnis jedoch in jedem Fall gewährleistet und Rückschlüsse auf die politische Gesinnung einzelner Stimmenden sind ausgeschlossen.

3.9 Übersicht über zu prüfende Massnahmen

In den vorangegangen sieben Abschnitten wurden vier mögliche Massnahmen zur weiteren Stärkung der Sicherheit und Vertrauenswürdigkeit der Wahlen und Abstimmungen im Kanton St.Gallen identifiziert. Zusammen mit den Erkenntnissen aus den folgenden Abschnitten 4 und 5 bilden sie die Basis für die in Abschnitt 6 definierten weiterführenden Massnahmen, welche die Regierung konkret umzusetzen oder zu prüfen beabsichtigt.

Zur besseren Übersicht werden die vier Massnahmen in der nachfolgenden Tabelle noch einmal zusammengefasst:

Massnahme	Eingedämmte Bedrohungen	Status
M2: Zusätzlicher Datamatrix-Code auf Stimmrechtsausweis für Abgleich mit dem Stimmregister	B1: Diebstahl und Missbrauch von Stimmmaterial B2: Fälschung von Stimmrechtsausweisen B4: Inkonsistenzen im Stimmregister B10: Abgabe von gefälschtem Stimmmaterial	zu prüfen
M12: Weiterführende Vorgaben betreffend sichere Lagerung	B15: Zugriff auf gelagerte Stimmabgaben B16: Diebstahl und/oder Zerstörung von Zustellkuverts B22: Manipulation des gelagerten Stimmmaterials	zu prüfen
M13: Reserve-Stimmmaterial: sichere Lagerung und fortlaufende Protokollierung	B17: Manipulation, Austausch oder Einspeisung von (zusätzlichen) Stimmzetteln B22: Manipulation des gelagerten Stimmmaterials	zu prüfen
M15: Definition von kritischen Prozessschritten und Erarbeitung einer entsprechenden Checkliste für Stimmbüros	B18: Manipulation der Auszählung durch Insiderinnen oder Insider	zu prüfen

4 Fokus E-Voting: Erfahrungen aus Pilotversuchen und Übertragbarkeit auf andere Bereiche

4.1 Entwicklung von E-Voting im Kanton St.Gallen

Bereits seit dem Jahr 2009 verfolgt der Kanton St.Gallen eine Strategie der schrittweisen Einführung der elektronischen Stimmabgabe (E-Voting). In einer ersten Pilotphase bis zum Jahr 2015 stand der elektronische Stimmkanal ausschliesslich den im Kanton gemeldeten Auslandschweizerinnen und Auslandschweizern zur Verfügung. Ab dem Jahr 2016 hatten dann im Rahmen der zweiten Pilotphase auch die Stimmberechtigten von fünf Pilotgemeinden (Goldach, Kirchberg, Rapperswil-Jona, Vilters-Wangs und Widnau) die Möglichkeit, ihre Stimmen per E-Voting abzugeben. Während gut dreier Jahre hatte die Staatskanzlei damit die Gelegenheit, wichtige Erkenntnisse zu den Prozessen und Abläufen der elektronischen Stimmabgabe zu gewinnen, bevor die zweite Phase der Pilotversuche mit der Abstimmung vom 19. Mai 2019 abgeschlossen wurde. Gestützt auf die bisherigen Erfahrungen hat die Staatskanzlei anschliessend die Planung der dritten Pilotphase in Angriff genommen. Diese zeichnet sich durch zwei Neuerungen aus: Zum einen soll die elektronische Stimmabgabe über ein so genanntes Anmeldeverfahren neu allen Stimmberechtigten im Kanton offenstehen – unabhängig von ihrer Gemeindezugehörigkeit.[28] Zum anderen wurde das bislang eingesetzte E-Voting-System des Kantons Genf durch das neue System der Schweizerischen Post mit vollständiger Verifizierbarkeit ersetzt.

[28] Die diesbezüglichen kantonalen Rechtsgrundlagen wurden in Art. 62 ff. des Gesetzes über Wahlen und Abstimmungen (sGS 125.3), in Vollzug ab 1. Januar 2019, geschaffen.

Mit Beschlüssen vom 3. März 2023 und 25. Juni 2025 erteilte der Bundesrat den Kantonen St.Gallen, Basel-Stadt, Thurgau und Graubünden (separater BR-Beschluss vom 22. November 2023) die Grundbewilligung[29] für weitere Versuche[30] mit der elektronischen Stimmabgabe mit dem neuen System der Post. Da die Anforderungen an die Sicherheit und die Nachvollziehbarkeit der elektronischen Stimmabgabe im Vorfeld zu dieser jüngsten Pilotphase vom Bund in Zusammenarbeit mit den Kantonen und der Wissenschaft noch einmal geschärft wurden, spricht man in diesem Zusammenhang auch von der «Neuausrichtung des Versuchsbetriebs». Seit dem Urnengang vom 18. Juni 2023 haben damit alle im Kanton St.Gallen gemeldeten Auslandschweizerinnen und Auslandschweizer sowie die im Kanton wohnhaften und für E-Voting angemeldete Stimmberechtigten (wieder) die Möglichkeit, ihre Stimmen bei eidgenössischen Volksabstimmungen und allen gleichzeitig an die Urne gelangenden kantonalen und kommunalen Vorlagen elektronisch abzugeben. Auch im Rahmen der Erneuerungswahl des Nationalrates vom 22. Oktober 2023 kam das E-Voting-System der Post erstmalig zum Einsatz.

Während die elektronische Stimmabgabe für den Urnengang vom 18. Juni 2023 noch auf die Auslandschweizerinnen und Auslandschweizer sowie die Stimmberechtigten der fünf ursprünglichen Pilotgemeinden beschränkt war, wie bereits in der zweiten Pilotphase, arbeitet die Staatskanzlei seit 2024 an der schrittweisen Etablierung des dritten Stimmkanals in weiteren interessierten Gemeinden. Mittlerweile ist die Ausweitung des E-Votings weit fortgeschritten und im Rahmen des Urnengangs vom 30. November 2025 konnte die elektronische Stimmabgabe bereits in 66 der 75 politischen Gemeinden angeboten werden.

4.2 Mehrwert von E-Voting

Seit dem Beginn der dritten Pilotphase wurde das E-Voting-System der Post mit vollständiger Verifizierbarkeit im Kanton St.Gallen bei 14 Urnengängen erfolgreich eingesetzt, für eidgenössische und kantonale Wahlen und Abstimmungen ebenso wie für kommunale. Im Rahmen des Urnengangs vom 30. November 2025 nutzten 67 Prozent der teilnehmenden Auslandschweizerinnen und Auslandschweizer die Möglichkeit der elektronischen Stimmabgabe. In den anderen Gemeinden, in denen E-Voting bereits angeboten wird, haben sich bislang je nach Gemeinde zwischen zwei und 16 Prozent der Stimmberechtigten dafür angemeldet. Diese Nutzerzahlen belegen, dass ein Bedarf für die elektronische Stimmabgabe besteht.

Mit Blick auf den Mehrwert von E-Voting muss zwischen Vorteilen für die Stimmberechtigten und Vorteilen für die Verwaltung (also für den Kanton und die an den Pilotversuchen teilnehmenden Gemeinden) unterschieden werden:

Vorteile für die Stimmberechtigten

– Die elektronische Stimmabgabe ist orts- und zeitunabhängig.
– Die Ausübung der politischen Rechte wird für Auslandschweizerinnen und Auslandschweizer erleichtert (bzw. in einzelnen Fällen gar erst ermöglicht). Mittels E-Voting können sie ihr Stimm- und Wahlrecht aus dem Ausland mit weniger Einschränkungen wahrnehmen, da die postalische Rücksendung der Stimmunterlagen entfällt. Damit erübrigen sich sowohl allfällige Verspätungen als auch die anfallenden Portokosten.

---

29 Eine Übersicht über das Bewilligungsverfahren und die damit verbundenen Anforderungen findet sich im Leitfaden der Bundeskanzlei, der im Internet unter https://www.bk.admin.ch/bk/de/home/politische-rechte/e-voting/versuchsbedingungen.html abgerufen werden kann. Die wichtigsten Dokumente und Grundsätze für die Einführung und den Betrieb der elektronischen Stimmabgabe im Kanton St.Gallen finden sich unter https://www.sg.ch/politik-verwaltung/abstimmungen-wahlen/e-voting/Bewilligungsverfahren-Dokumentation-Weiterentwicklung.html.

30 Gemäss den für die Erteilung einer Bewilligung relevanten Rechtsgrundlagen auf eidgenössischer Ebene wird im Rahmen von E-Voting stets von «Versuchen» gesprochen. Bei E-Voting handelt es sich um eine örtlich, zeitlich und sachlich begrenzte Erprobung eines neuen Stimmkanals.

– Mit E-Voting ist es nicht möglich, eine ungültige Stimme abzugeben. Stimmberechtigte Personen machen – oftmals unbewusst – formale Fehler (u.a. fehlende Unterschrift, mehrere Stimmabgaben offen im gleichen Zustellkuvert). Im Zuge der elektronischen Stimmabgabe kann dies nicht passieren.
– Stimmberechtigte können eigenständig verifizieren, dass ihre Stimme unverändert in der elektronischen Urne registriert wurde (im Gegensatz zur brieflichen Stimmabgabe).
– Mittels E-Voting können Stimmberechtigte mit besonderen Bedürfnissen, beispielsweise mit einer Behinderung, autonom und damit unter Wahrung des Stimmgeheimnisses von ihren politischen Rechten Gebrauch machen.

Vorteile für den Kanton und die Gemeinden
– Die elektronischen Stimmen werden zentral und automatisch ausgezählt. Damit reduziert sich der Zeitaufwand für die Auszählung und die Kontrolle beträchtlich – gerade im Fall von Proporzwahlen, bei denen die Möglichkeit besteht, Listen nahezu beliebig zu verändern – und die Ergebnisse des Urnengangs können schneller ermittelt werden.
– Durch die computergestützten Prozesse werden beim E-Voting manuelle Fehler bei der Auszählung und der Übertragung der Daten vermieden.
– Der Kanton kann der Bevölkerung mit der elektronischen Stimmabgabe eine oft nachgefragte digitale Leistung zur Verfügung stellen.

4.3 Bundesrechtliche Vorgaben

Die Voraussetzungen, die erfüllt sein müssen, um Versuche mit der elektronischen Stimmabgabe durchführen zu können, sind im Bundesgesetz über die politischen Rechte sowie zwei weiterführenden Verordnungen geregelt.[31] Die bundesrechtlichen Bestimmungen legen die technischen, betrieblichen und organisatorischen Anforderungen für den Einsatz von E-Voting fest. Die zu erfüllenden Anforderungen richten sich dabei an die Kantone. Diese müssen die Bestimmungen entweder selbst oder durch Dritte (z.B. die Systemanbieterin) umsetzen (lassen), wobei gewisse Aufgaben nicht delegiert werden dürfen. Die zentralen Anforderungen seitens des Bundes werden nachfolgend anhand von vier Kategorien zusammengefasst.

[31] Die einschlägigen Bestimmungen finden sich in Art. 8a BPR, in Art. 27a–q der eidgenössischen Verordnung über die politischen Rechte (SR 161.11; abgekürzt VPR) sowie in der Verordnung der BK über die elektronische Stimmabgabe (SR 161.116; abgekürzt VEleS).

Kategorie	Anforderungen
Vollständige Verifizierbarkeit	Die vollständige Verifizierbarkeit stellt sicher, dass jede Manipulation, die zu einer Verfälschung des Ergebnisses führt, unter Einhaltung des Stimmgeheimnisses festgestellt werden kann. Sie ist gegeben, wenn die Anforderungen an die individuelle sowie an die universelle Verifizierbarkeit erfüllt sind: – Die individuelle Verifizierbarkeit ermöglicht es der stimmenden Person, durch Beweise (Prüfcodes) zu kontrollieren, ob ihre Stimme korrekt und unverändert in der elektronischen Urne registriert wurde. – Die universelle Verifizierbarkeit gewährleistet, dass systematische Fehlfunktionen infolge von Softwarefehlern, menschlichen Fehlleistungen oder Manipulationsversuchen erkannt werden. Dafür generiert das System bei verschiedenen Schritten im Wahl- und Abstimmungsprozess kryptografische Beweise, die von durch den Kanton mandatierte Prüferinnen und Prüfer mittels einer Verifikationssoftware ausgewertet werden.
Transparenz	Transparenzschaffende Massnahmen: – Offenlegung des Quellcodes und der Dokumentation zum System; – Offenlegung der Betriebsdokumentationen von Post und Kanton; – Publikation der Prüfergebnisse der unabhängigen Experten; – Veröffentlichung der (Teil-)Ergebnisse der mittels E-Voting abgegebenen Stimmen bei eidgenössischen Wahlen und Abstimmungen: – transparente Kommunikation im Fall von Mängeln oder Unregelmässigkeiten.
Überprüfung	Mechanismen für regelmässige Überprüfungen durch unabhängige Stellen: – unabhängige Überprüfung des Systems sowie der Betriebsprozesse der Post, des Kantons und der Druckerei im Auftrag der Bundeskanzlei (siehe auch Abschnitt 4.3.2); – öffentliche Überprüfung des Quellcodes durch externe Expertinnen und Experten (Offenlegung im Rahmen eines Bug-Bounty-Programms); – öffentliche Intrusionstests (als Teil des Bug-Bounty-Programms) .
Verteilung der Verantwortung	Sicherstellung der Aufgabentrennung: – Der Kanton muss wichtige Aufgaben selbst durchführen (u.a. Installation der Software, Konfiguration des Urnengangs, Generieren der Stimmrechtsausweise). – Das E-Voting-System ist auf eine Vielzahl verschiedener Computer verteilt, die bis auf wenige Ausnahmen nicht ans Internet angeschlossen sein dürfen. – Kritische Prozessschritte im Zusammenhang mit der elektronischen Urne erfolgen ausschliesslich im Vieraugenprinzip.

4.3.1 Zugelassenes Elektorat

Da es sich bei E-Voting wie erwähnt noch immer um einen Versuchsbetrieb handelt, kann der elektronische Stimmkanal aktuell nur einem Teil der Stimmberechtigten angeboten werden. So schreibt Art. 27f Abs. 1 VPR vor, dass höchstens 30 Prozent des kantonalen Elektorats zur elektronischen Stimmabgabe zugelassen werden dürfen (und zudem die Limite von 10 Prozent des gesamtschweizerischen Elektorats nicht überschritten werden darf). Die stimmberechtigten Auslandschweizerinnen und Auslandschweizer sind von diesen Limiten allerdings ausgenommen.

Im Kanton St.Gallen können, wie in Abschnitt 4.1 bereits erwähnt, sowohl die Auslandschweizerinnen und Auslandschweizer wie auch angemeldete Stimmberechtigte aus den übrigen Gemeinden ihre Stimmen elektronisch abgeben, vorausgesetzt die betreffende Gemeinde hat sich dafür entschieden, ihren Stimmbürgerinnen und Stimmbürgern E-Voting anzubieten. Ist dies der Fall, kann sich eine interessierte Person über eine eigens dafür eingerichtete Web-

seite des Kantons für die elektronische Stimmabgabe anmelden.[32] Die Verifizierung der Stimmberechtigung bei der Anmeldung erfolgt durch einen automatisierten Datenabgleich mit dem stehenden Stimmregister (siehe auch Abschnitt 3.2.2). Im gleichen Arbeitsschritt wird zudem geprüft, ob die betreffende Gemeinde tatsächlich E-Voting anbietet. Fallen beide Prüfungen positiv aus, wird der sich anmeldenden Person direkt auf der Webseite angezeigt, dass die Anmeldung erfolgreich war. Zudem wird ihr im Nachgang eine schriftliche Bestätigung per Post zugestellt. Gemeinsam mit allen anderen angemeldeten Stimmberechtigten erhält sie ab dem folgenden Urnengang nun jeweils einen E-Voting-Stimmrechtsausweis mit den für die elektronische Stimmabgabe nötigen Sicherheitsmerkmalen.

Sobald die Limite von 30 Prozent des kantonalen Elektorats einmal erreicht ist, wird die Staatskanzlei die Möglichkeit für weitere Anmeldungen von innerhalb des Kantons wohnhaften Stimmberechtigten sperren.[33] Die im Kanton St.Gallen gemeldeten Auslandschweizerinnen und Auslandschweizer sind hingegen automatisch für E-Voting registriert (siehe auch Abschnitt 3.4.2), eine zusätzliche Anmeldung ihrerseits ist deshalb nicht nötig.

4.3.2 Unabhängige Überprüfung und Massnahmenkatalog von Bund und Kantonen

Im Zentrum der bereits erwähnten Neuausrichtung des Versuchsbetriebs steht ein kontinuierlicher Verbesserungsprozess. Deshalb führt die Bundeskanzlei in regelmässigen Abständen oder bei wesentlichen Anpassungen am E-Voting-System oder an den Betriebsmodalitäten eine unabhängige Überprüfung des Systems sowie der Betriebsprozesse bei der Post, beim Kanton und bei der Druckerei durch, welche die E-Voting-Stimmrechtsausweise druckt und verpackt. Die Kosten für diese Überprüfungen trägt die Bundeskanzlei, um deren Unabhängigkeit sicherzustellen.

Die von der Bundeskanzlei beauftragten unabhängigen Expertinnen und Experten prüfen das kryptografische Protokoll, die Software des Systems, die Sicherheit der Infrastruktur und des Betriebs sowie den Schutz gegen Versuche, in die Infrastruktur einzudringen. Ziel der unabhängigen Überprüfung ist es, sicherzustellen, dass alle Anforderungen der Bundeskanzlei erfüllt sind und die Sicherheitsvorkehrungen und das E-Voting-System dem neuesten Stand entsprechen. Der Kanton St.Gallen und die von ihm beauftragte Druckerei (Abraxas) wurden seit der Wiederaufnahme der E-Voting-Versuche im März 2023 bereits mehrfach überprüft, das letzte Mal im Februar 2025 im Vorfeld der Erneuerung der Grundbewilligung durch den Bundesrat. Sämtliche Prüfberichte sind auf der Webseite der Bundeskanzlei offengelegt.[34]

Um sicherzustellen, dass die neusten Entwicklungen mit Blick auf die Sicherheit von E-Voting berücksichtigt und bekannter Handlungsbedarf angemessen adressiert werden, führen der Bund und die Kantone zudem einen gemeinsamen Massnahmenkatalog. Dieser zeigt auf, in welchen Bereichen Handlungsbedarf identifiziert wurde und wo bereits Weiterentwicklungen am System oder der elektronischen Stimmabgabe zugrundeliegenden Prozesse geplant sind. Der Massnahmenkatalog wird laufend überprüft und angepasst und die jeweils aktuelle Version ist ebenfalls im Internet frei zugänglich.[35]

---

32 Weiterführende Informationen zum Anmeldeverfahren und zu den teilnehmenden Gemeinden finden sich im Internet unter https://www.sg.ch/politik-verwaltung/abstimmungen-wahlen/e-voting/anmeldeverfahren.html. Eine allfällige Abmeldung von E-Voting erfolgt über die gleiche Webseite und ist jederzeit möglich.

33 Um zu verhindern, dass das Limit bereits erreicht ist, bevor sich die Stimmberechtigten der letzten interessierten Gemeinden überhaupt für E-Voting anmelden können, ist der Anteil an E-Voterinnen und E-Votern aktuell auf 30 Prozent des Elektorats *je Gemeinde* limitiert.

34 Vgl. https://www.bk.admin.ch/bk/de/home/politische-rechte/e-voting/ueberpruefung_systeme.html.

35 Vgl. https://www.bk.admin.ch/bk/de/home/politische-rechte/e-voting/versuchsuebersicht.html.

4.4 Spezifische Risiken von E-Voting und Gegenmassnahmen zu deren Eindämmung

Da die Vorbereitung und Durchführung eines Urnengangs mit E-Voting aufgrund der vielen Vorgaben, die berücksichtigt werden müssen, relativ aufwändig ist, gibt es verschiedene kritische Funktionalitäten, die zentralisiert organisiert und betrieben werden müssen, damit Kosten und Nutzen der elektronischen Stimmabgabe in einem positiven Verhältnis stehen können. Dazu gehört insbesondere die zentrale Entschlüsselung aller elektronischen Urnen – also auch jener der Gemeinden – durch das so genannte *Electoral Board* (bestehend aus dem E-Voting-Ausschuss des kantonalen Stimmbüros) und das *Admin-Board* der Staatskanzlei (bestehend aus der Leitung elektronische Stimmabgabe und jeweils einer weiteren Person).

Ebenfalls zentral für alle Gemeinden erfolgt das Einspielen aller elektronisch abgegebenen Stimmen ins Ergebnisermittlungssystem. Im Vergleich mit der dezentral stattfindenden Auszählung der brieflich und an der Urne eingelangten Stimmabgaben in den verschiedenen Gemeinden (siehe Abschnitt 3.6), kommt den organisatorischen und technischen Sicherheitsvorkehrungen beim E-Voting deshalb eine besondere Bedeutung zu.

Da der Bund, die Kantone und die Post im Kontext von E-Voting unterschiedliche Aufgaben wahrnehmen, erstellt jeder der beteiligten Akteure eine eigene Beurteilung der mit der elektronischen Stimmabgabe verbundenen Risiken in seinem Zuständigkeitsbereich, wobei sich diese Risikobeurteilungen zwingend an den in Art. 4 Abs. 3 VEleS definierten Sicherheitszielen orientieren müssen:

– Korrektheit des Ergebnisses;
– Wahrung des Stimmgeheimnisses und Ausschluss von vorzeitigen Teilergebnissen;
– Erreichbarkeit und Funktionsfähigkeit des Stimmkanals;
– Schutz der persönlichen Informationen über die stimmberechtigten Personen;
– Schutz der für die stimmberechtigten Personen bestimmten Informationen vor Manipulationen;
– keine missbräuchliche Verwendung von Beweisen zum Stimmverhalten.

Die Risikobeurteilung der Bundeskanzlei deckt primär die mit der elektronischen Stimmabgabe verbundenen Risiken mit nationaler Tragweite ab. Dazu würden etwa erhebliche Sicherheitsmängel im System oder eine mangelnde Akzeptanz von E-Voting gehören. Der Kanton St.Gallen betreibt gemeinsam mit den anderen E-Voting-Kantonen ein umfangreiches Risikomanagement. Dieses stützt sich auf eine gemeinsam erarbeitete, dezidierte Richtlinie, die regelmässig überprüft und aktualisiert wird.[36]

Die nachfolgend beschriebenen Risiken – und die zu ihrer Eindämmung getroffenen Gegenmassnahmen – lassen sich in chronologischer Hinsicht unterscheiden, je nachdem ob sie während der ganzen Vorbereitung und Durchführung eines Urnenganges mit E-Voting bestehen oder primär vor der Öffnung der elektronischen Urne, während der Stimmabgabe oder bei der Auszählung der elektronisch abgegebenen Stimmen.

4.4.1 Während des gesamten E-Voting-Prozesses

Um das Risiko durch *technische Bedrohungen* wie Malware oder Hacking zu reduzieren, hat der Kanton verschiedene vorbeugende Massnahmen ergriffen.[37] So werden unter anderem sämtliche kritischen Prozessschritte ausschliesslich auf gehärteten Offline-Geräten durch-

[36] Die «Richtlinie Risikomanagement» sowie das gesamte Risikoportfolio der E-Voting-Kantone sind im Internet frei zugänglich unter https://www.sg.ch/politik-verwaltung/abstimmungen-wahlen/e-voting/Bewilligungsverfahren-Dokumentation-Weiterentwicklung.html.

[37] Die Möglichkeit von Cyberangriffen auf andere digitale Services wie etwa das Ergebnisermittlungssystem oder das E-Counting wurde bereits in Abschnitt 3.6 thematisiert.

geführt. Diese Geräte sind zu keiner Zeit mit dem Internet verbunden, auch nicht für die Installation oder die Aktualisierung der benötigten Software. Vor jedem Urnengang analysieren die vier E-Voting-Kantone zusammen mit den IT-Sicherheitsexperten des Bundesamtes für Cybersicherheit (BACS) und der Post zudem die Bedrohungslage und treffen bei Bedarf weiterführende Vorkehrungen.

In Anbetracht der beträchtlichen Risiken kommt auch dem so genannten *Business Continuity Management* eine grosse Bedeutung zu. Mit regelmässigen Back-ups und jederzeit einsatzbereiten Ersatzgeräten stellt der Kanton sicher, dass sämtliche Prozessschritte (und damit letztlich der Urnengang) auch tatsächlich durchgeführt werden können. Zudem müssen kritische manuelle Prozessschritte wie die Installation der Software oder die Konfiguration eines Urnengangs zwingend im Vieraugenprinzip durchgeführt werden und es wird protokolliert, welche Mitglieder des «Electoral Boards» wann wofür eingesetzt worden sind.

Generell spielt der Mensch im Prozess der elektronischen Stimmabgabe eine wesentliche Rolle. Daher kommt auch dem *Management der Informationssicherheit* eine nicht zu unterschätzende Bedeutung zu. Sämtliche am Betrieb des E-Voting-Systems beteiligten Personen werden regelmässig für die Inhalte der «Richtlinie Informationssicherheit»[38] und die sich daraus ergebenden, zwingend einzuhaltenden Regeln sensibilisiert. Darin werden die Ziele, Anforderungen und Massnahmen zur Gewährleistung der Informationssicherheit beim Betrieb des elektronischen Stimmkanals definiert und es wird festgehalten, dass das Stimmgeheimnis, die Verifizierbarkeit und die Systemverfügbarkeit gewährleistet und die kantonalen sowie die bundesrechtlichen Vorgaben eingehalten werden müssen.

4.4.2 Vor Öffnung der elektronischen Urne

Um das Risiko zu minimieren, dass *Fehler während der Vorbereitung* eines Urnengangs (wie beispielsweise die Konfiguration falscher Urnenöffnungszeiten) dessen ordnungsgemässe Durchführung letztlich verhindern, führt der Kanton vor jedem Urnengang einen so genannten End-to-End-Test durch. In diesem wird der komplette Urnengang von der Konfiguration über die Stimmabgabe und die Auszählung bis hin zum Einspielen der E-Voting-Ergebnisse ins Ergebnisermittlungssystem durchgespielt. Nach Abschluss der Vorbereitungsarbeiten – aber noch vor dem Versand des Stimmmaterials – wird zudem immer mindestens eine Teststimme in eine Test-Urne abgegeben. Diese wird anschliessend ausgezählt und es wird geprüft, ob die in der Urne registrierten Stimmen mit den abgegebenen Teststimmen übereinstimmen. Auf diese Weise kann verifiziert werden, ob die Vorbereitungsarbeiten vollständig und fehlerfrei durchgeführt wurden.

Wie in der Einleitung zu Abschnitt 4.4 bereits erwähnt, sind beim E-Voting im Vergleich zum herkömmlichen Prozess der Vorbereitung und Durchführung von Wahlen und Abstimmungen einzelne Prozessschritte deutlich stärker zentralisiert. Das gilt auch für die Aufbereitung und den Druck der E-Voting-Stimmrechtsausweise und insbesondere für die in diesem Zusammenhang zentrale Generierung der persönlichen Codes für die angemeldeten Wählerinnen und Wähler. Dabei muss, so die relevante Vertrauensannahme, davon ausgegangen werden können, dass die betreffende Druckerei (im Fall des Kantons St.Gallen ist es jene von Abraxas) diese Arbeiten zuverlässig, sicher und offline erledigt – also ohne dass die eingesetzten Geräte über einen aktiven Netzwerkzugang verfügen. Wäre dies nicht der Fall, so würden verschiedene der in den Abschnitten 3.2 und 3.4 erläuterten Bedrohungen nicht nur manifest, das potenzielle Schadensausmass im Fall eines Angriffs wäre zudem einfacher skalierbar. Deshalb

[38] Die von der Staatskanzlei erlassene «Richtlinie Informationssicherheit E-Voting» wurde explizit mit Blick auf den Einsatz von E-Voting-Systemen erlassen. Gemäss Art. 14 Ziff. 3 Bst. a VEleS ist jeder Kanton verpflichtet, eine entsprechende Richtlinie zu erlassen und sicherzustellen, dass alle beteiligten Personen darüber informiert werden.

wird regelmässig überprüft, ob die *Infrastruktur und die Prozesse der Druckerei* die bundesrechtlichen Anforderungen erfüllen. Dabei wird insbesondere kontrolliert, ob die Infrastruktur aktuell ist und ob die Arbeiten für E-Voting offline und, wo nötig, im Vieraugenprinzip erfolgen. Darüber hinaus ist die Druckerei von Abraxas nach ISO27001 zertifiziert und hat damit den Umgang mit vertraulichen Informationen in ihren Abläufen verankert (siehe auch Abschnitt 3.2.3).

4.4.3 Während der Stimmabgabe

Nebst dem sicheren Betrieb der Software des E-Voting-Systems sowie der soeben besprochenen sicheren Generierung der persönlichen Codes in einer zertifizierten Druckerei ist beim E-Voting auch die *Sicherheit der Endgeräte*, von denen die Stimmberechtigten ihre Stimmen abgeben, von zentraler Bedeutung. Dabei ist das Augenmerk nicht nur auf die Heterogenität der Geräte an sich zu richten, sondern auch auf die darauf betriebene Software (z.B. verschiedene Betriebssysteme oder Browser für den Zugang zum E-Voting), respektive deren jeweilige Versionen.

Die *Nutzerinnen und Nutzer* können ebenfalls ihren Teil zur Sicherheit beitragen, indem sie sich an die Instruktionen auf dem Stimmrechtsausweis halten und dadurch das Risiko eines Missbrauchs durch Dritte minimieren. Insbesondere wird allen E-Voterinnen und E-Votern empfohlen, vor der Anmeldung anhand einer Prüfung der Hashwerte zu kontrollieren, ob sie sich auf der richtigen Webseite befinden.[39] Zusätzlich wird jeder für E-Voting angemeldeten Person zusammen mit dem Stimmrechtsausweis eine Anleitung zugestellt, in der Schritt für Schritt erklärt wird, wie bei der elektronischen Stimmabgabe vorzugehen ist. Wird bei der Abgabe der elektronischen Stimme eine Unregelmässigkeit festgestellt, z.B. dass der im E-Voting-Portal angezeigt Prüfcode nicht mit dem auf dem Stimmrechtsausweis aufgedruckten übereinstimmt, so muss der Wahl- oder Abstimmungsprozess abgebrochen und die zuständige Stelle kontaktiert werden.[40]

Ein weiterer wichtiger Aspekt ist die *Erreichbarkeit des E-Voting-Portals*: Steht dieses nicht zur Verfügung, können die Stimmberechtigten ihre Stimmen nicht elektronisch abgeben. Ein potenzieller Ausfall des E-Voting-Portals wurde explizit in die Risikobeurteilung aufgenommen und analysiert. Die Post hat unterschiedliche Massnahmen ergriffen, um einen solchen Ausfall möglichst zu verhindern. So wurden beispielsweise Vorkehrungen gegen potenzielle «DDoS-Attacken» ergriffen, mit denen unter Umständen eine mutwillige Überlastung des E-Voting-Portals provoziert werden könnte.[41] Zudem gewährleistet die Post mit einer redundanten Infrastruktur dass selbst im Fall eines Ausfalls keine Daten verloren gehen. Allerdings gilt es auch zu erwähnen, dass der elektronische Stimmkanal immer als komplementär zu den anderen beiden Kanälen zu verstehen ist. Entsprechend können die für E-Voting angemeldeten Stimmberechtigten jederzeit wählen, welchen Kanal sie für ihre Stimmabgabe verwenden möchten. Falls das E-Voting-Portal einmal nicht zur Verfügung stehen sollte, können die Betroffenen ihre Stimmen somit immer noch brieflich oder an der Urne abgeben (siehe auch Abschnitt 3.4.1).

---

39 Wie die Prüfung der Hashwerte funktioniert und welche zusätzlichen Sicherheitsmassnahmen die E-Voterinnen und E-Voter ergreifen können, wird auf der gemeinsam betriebenen Informationsplattform der Kantone im Detail erläutert (vgl. https://www.evoting-info.ch/sicherheit/einfache-tipps-fuer-mehr-sicherheit).

40 Die notwendigen Kontaktangaben finden sich sowohl auf dem Stimmrechtsausweis als auch in der Anleitung zur elektronischen Stimmabgabe. Letztere kann auch auf der Webseite des Kantons heruntergeladen werden (vgl. https://www.sg.ch/politik-verwaltung/abstimmungen-wahlen/e-voting.html).

41 Das Risiko von «DDoS-Attacken» (weitere Ausführungen zum Thema finden sich auch in Abschnitt 3.6.2) wird vom Bundesamt für Cybersicherheit, der Post und den Kantonen kontinuierlich überwacht.

4.4.4 Bei der Auszählung

Die Auszählung der elektronisch abgegebenen Stimmen unterscheidet sich dadurch von jener der herkömmlich eingelangten, dass die Zählung nicht in jeder Gemeinde separat vorgenommen werden kann. Vielmehr findet die Entschlüsselung der elektronischen Urnen aller Gemeinden zentral statt (siehe auch Einleitung zu Abschnitt 4.4), was theoretisch die Skalierbarkeit eines allfälligen Angriffs erhöhen könnte. Allerdings gilt es in diesem Zusammenhang zu betonen, dass der gesamte Prozess immer von mehreren Personen überwacht und begleitet wird, unter anderem von gewählten Mitgliedern des kantonalen Stimmbüros (dem bereits erwähnten *Electoral Board*). Zudem erfolgt der finale Schritt der Entschlüsselung der Stimmen nicht in der Infrastruktur der Post, sondern auf einem eigens zu diesem Zweck aufgesetzten, gesicherten Computer der Staatskanzlei.[42] Dabei besitzen die Mitglieder des *Electoral Boards* einen Teil des Schlüssels, der notwendig ist, um die elektronischen Urnen zu entschlüsseln. Damit ist sichergestellt, dass die elektronisch abgegebenen Stimmen nur entschlüsselt werden können, wenn der E-Voting-Ausschuss des Stimmbüros mit dem *Admin-Board* der Staatskanzlei zusammenkommt. Eine Entschlüsselung allein durch Vertreter des Kantons oder durch Mitarbeitende der Post ist nicht möglich.

4.5 Best practices

Während der mittlerweile mehr als 15 Jahre, in denen der Kanton St.Gallen bereits Versuche mit E-Voting durchführt, haben sich verschiedene Herangehensweisen herauskristallisiert, die sich auch in der längerfristigen Betrachtung bewährt haben. Zu den wichtigsten von ihnen gehören die beiden Grundsätze «Sicherheit durch Transparenz» und «Sicherheit vor Tempo», auf die nachfolgend im Detail eingegangen wird. Im folgenden Abschnitt 4.6 wird zudem aufgezeigt, welche Erkenntnisse und «best practices» aus dem Kontext der elektronischen Stimmabgabe auch auf andere Bereiche der politischen Rechte übertragen werden können und wo sie mit Blick auf die Entwicklung von neuen digitalen Services gewinnbringend angewendet werden können.

4.5.1 «Sicherheit durch Transparenz»

Seit dem Jahr 2021 veröffentlicht die Post im Rahmen ihres so genannten *Community-Programms* alle relevanten Komponenten des E-Voting-Systems (dazu gehören neben dem Quellcode und der Systemdokumentation auch neue Entwicklungsversionen und Releases) und lässt sie öffentlich testen. Meldungen, die zur Verbesserung des Systems beitragen, werden mit Prämien von bis zu Fr. 250'000.– honoriert und die Post informiert auf einer eigens dafür eingerichteten Webseite regelmässig über die eingegangenen Meldungen sowie die dadurch ermöglichten Verbesserungen ihres Systems.[43] Dieser Ansatz der Prüfung der eigenen Software durch Inputs von unabhängigen Expertinnen und Experten ist auch bekannt als «Bug Bounty-Programm». Die Bezeichnung kommt daher, dass jeweils nur die erste Meldung einer bislang unbekannten Schwachstelle («bug») mit einer Prämie («bounty») belohnt wird. Dies soll die Entdecker allfälliger Schwachstellen davon abgehalten, ihr Wissen für sich zu behalten (um es möglicherweise später ausnutzen zu können), da sie davon ausgehen müssen, dass ein anderer «hunter» früher oder später auf die gleiche Schwachstelle stösst und diese dann behoben wird. Das Bug-Bounty-Programm der Post hat sich bewährt und soll unbefristet weitergeführt werden, mit dem Ziel, das System und dessen Sicherheit kontinuierlich zu verbessern und das Vertrauen der Öffentlichkeit ins E-Voting zu stärken.

---

42 Die Daten ruft der Kanton verschlüsselt und signiert aus der Post-Infrastruktur ab. Die Übertragung erfolgt über eine gesicherte Verbindung. Die Bundeskanzlei hat die Technik unabhängig geprüft (siehe Abschnitt 4.3.2).

43 Alle Informationen zum *E-Voting-Community-Programm* der Post finden sich auf der dazugehörigen Webseite unter https://evoting-community.post.ch/de.

Darüber hinaus bemühen sich auch die Kantone um die Schaffung von Transparenz, indem sie auf ihren Webseiten laufend die wichtigsten Informationen und Dokumente zu E-Voting allgemein, zum Anmeldeverfahren sowie zum aktuellen Stand des Bewilligungsverfahrens veröffentlichen und relevante Informationen der Bundeskanzlei und der Post verlinken. Die Bundeskanzlei ihrerseits veröffentlicht auf ihrer Website die Berichte der unabhängigen Prüfungen (siehe auch Abschnitt 4.3.2).

Ergänzend haben die E-Voting-Kantone mit ihrer gemeinsamen Informationsplattform eine zentrale Anlaufstelle für Fragen und Informationen zum Thema E-Voting in der Schweiz geschaffen. Unter *evoting-info.ch* finden sich umfassende Erläuterungen zum Ablauf der elektronischen Stimmabgabe, inklusive Schritt-für-Schritt-Anleitungen, einem Erklärvideo und einem FAQ mit häufig gestellten Fragen. Zudem haben Besucherinnen und Besucher die Möglichkeit, die elektronische Stimmabgabe auf einer Testplattform selbst auszuprobieren. Im Sinn der Transparenz bietet die E-Voting-Informationsplattform zudem eine fortlaufend aktualisierte Übersicht über alle sicherheitsrelevanten Vorkommnisse, Abklärungen und Meldungen in Zusammenhang mit dem E-Voting-System. Diese Massnahme dient nicht zuletzt auch der Vertrauensbildung, indem die Kantone aufzeigen, wie sie mit Hinweisen aus der Bevölkerung umgehen und welche technischen oder organisatorischen Massnahmen sie als Reaktion darauf ergriffen haben.

4.5.2 «Sicherheit vor Tempo» und kantonsübergreifende Zusammenarbeit

Seit der Wiedereinführung im Juni 2023 hat die Post das E-Voting-System in enger Zusammenarbeit mit den Kantonen und der Bundeskanzlei kontinuierlich weiterentwickelt. Dabei wird konsequent der Grundsatz «Sicherheit vor Tempo» verfolgt. Neue Funktionalitäten werden erst dann umgesetzt, wenn sämtliche sicherheitsrelevanten Anforderungen erfüllt und die entsprechenden Prüfungen abgeschlossen sind. Diese Vorgehensweise stellt sicher, dass der Schutz der Stimmabgabe, die Verifizierbarkeit des Systems sowie die Einhaltung der gesetzlichen Vorgaben jederzeit gewährleistet sind. Auch der Kanton St.Gallen misst der Sicherheit und der Vertrauenswürdigkeit die höchste Priorität bei und orientiert sich bei der Ausweitung und Weiterentwicklung der elektronischen Stimmabgabe an diesem bewährten Grundsatz.

Darüber hinaus haben die vier E-Voting-Kantone St.Gallen, Thurgau, Basel-Stadt und Graubünden seit der Wiedereinführung auch ihre Zusammenarbeit untereinander (sowie mit der Post und der Bundeskanzlei) kontinuierlich optimiert und dadurch den Betrieb erheblich professionalisiert. Die Zusammenarbeit zwischen den Kantonen ist eng und vertrauensvoll und basiert auf Transparenz, gegenseitiger Unterstützung und der bestmöglichen Nutzung von Synergien.

4.6 Anwendung der Erfahrungen mit E-Voting auf andere digitale Services im Bereich Wahlen und Abstimmungen

Wie im vorangegangenen Abschnitt aufgezeigt, unterstehen die Einführung und der Betrieb des E-Voting-Systems anspruchsvollen, gesetzlich vorgeschriebenen Sicherheitsanforderungen, deren Umsetzung von der Bundeskanzlei und Expertengremien mit grossem Aufwand überwacht werden. Mit der Erneuerung vom 30. November 2018 des Kreisschreibens zur Verwendung von technischen Hilfsmitteln bei der Ergebnisermittlung[44] hat der Bundesrat zudem den Einsatz von Scannern zur Auszählung und Auswertung von Stimm- und Wahlzetteln (E-Counting, siehe auch Abschnitt 3.6.2), sowie anderer technischer Hilfsmittel wie Präzisionswaagen oder Zählmaschinen formell reglementiert. Für den Einsatz von Ergebnisermittlungssystemen für Wahlen und Abstimmungen bestehen jedoch aktuell keine expliziten Sicherheitsanforderungen, die erfüllt sein müssen. Es ist allerdings nicht auszuschliessen, dass – nicht zuletzt auch als Folge der Debatte über die elektronische Stimmabgabe und deren Sicherheit – in

44 Vgl. BBl 2018, 7683.

den nächsten Jahren entsprechende Vorgaben auf Bundesebene erlassen und auch mit Blick auf die eingesetzten Ergebnisermittlungssysteme die Forderung nach einer Offenlegung des Quellcodes laut werden könnten.

Im Zuge der Ausschreibung ihres neuen Ergebnisermittlungssystems (siehe auch Abschnitt 3.6.1) haben die Kantone St.Gallen und Thurgau im Frühling 2020 gemeinsam entschieden, in punkto Transparenz und öffentlicher Nachvollziehbarkeit des neuen Systems sowie hinsichtlich dessen unabhängiger Überprüfung erhöhte Anforderungen zu stellen, in der Absicht einen neuen (Sicherheits-)Standard zu etablieren. So wurde von der Anbieterin des zu beschaffenden Systems ausdrücklich verlangt, dass diese sich bereit erklärt, den Quellcode des neuen Ergebnisermittlungssystems offenzulegen und dieses einem unbefristeten Bug-Bounty-Programm zu unterstellen.[45] Dabei handelte es sich um einen bewussten Paradigmenwechsel hin zu einem Verständnis von «Sicherheit durch Transparenz», wie es sich im thematisch eng verwandten E-Voting-Bereich bereits etabliert hatte.

Ein erster Hinweis dafür, dass der verstärkte Fokus auf die Sicherheit des Ergebnisermittlungssystems und damit auf den zentralen Bereich der Ausmittlung und Zusammenführung der (Gemeinde-)Ergebnisse richtig und wichtig ist, folgte bereits im Herbst 2020 in Form mehrerer kritischer Medienberichte zum Thema. So zeigte das Online-Magazin *Republik* am 25. September 2020 mit Hilfe zweier IT-Sicherheitsforscher auf, dass «mindestens 14 Kantone angreifbare und nicht mehr zeitgemässe Software» zur Ermittlung der Ergebnisse von Wahlen und Abstimmungen verwenden würden.[46] Die Befunde des Artikels der *Republik* wurden von verschiedenen anderen Medien aufgegriffen und führten zu verschiedenen Anpassungen an kantonalen Ausmittlungssystemen.[47]

Nachdem die Regierung den Zuschlag fürs neue Ergebnisermittlungssystem am 22. Dezember 2020 an die Firma Abraxas erteilt hatte, wurde der Quellcode der neu entwickelten Applikation *VOTING Ausmittlung* wie angekündigt vor deren erstem produktiven Einsatz im Rahmen eines Bug-Bounty-Programms offengelegt. Die Offenlegung erfolgte dabei in zwei Stufen: In einem ersten Schritt prüften rund 140 eingeladene Sicherheitsforscherinnen und Sicherheitsforscher das neue System, im zweiten Schritt wurde das Programm dann in ein öffentliches Bug-Bounty überführt und so einem internationalen Kreis von Sicherheitsexperten zugänglich gemacht.[48] Ein vergleichbares Vorgehen hat beispielsweise im Fall des E-Voting-System der Post aufschlussreiche Erkenntnisse zutage gefördert. Insgesamt erstreckte sich die Offenlegung über den Zeitraum von Mai 2022 bis Januar 2023. Nach dem erfolgreichen Abschluss des öffentlichen Sicherheitstests folgte im Februar 2023 dann der Entscheid zur produktiven Inbetriebnahme von *VOTING Ausmittlung.* Das Bug-Bounty-Programm läuft aber unbefristet weiter und allfällige nach wie vor vorhandene Schwachstellen können weiterhin gemeldet werden.[49]

Bis Mitte Dezember 2025 sind insgesamt 95 Meldungen über mögliche Schwachstellen eingereicht worden, die alle von den Sicherheitsspezialisten von Abraxas geprüft und bewertet wurden. Obwohl bislang erst zwei Meldungen mit der Kritikalität «hoch» eingestuft wurde, haben die Hinweise aus der Community kontinuierlich dazu beigetragen, die Sicherheit des Ergeb-

---

45 Die gleichen Anforderungen wurden 2023 auch vom Kanton Zürich und 2024 vom Kanton Basel-Stadt in die Pflichtenhefte für die Ausschreibung ihrer neuen Ergebnisermittlungssysteme übernommen.

46 Vgl. https://www.republik.ch/2020/09/25/passwort-wahlen.

47 Das vormalige System des Kantons St.Gallen (WABSTI) wurde im Artikel der *Republik* nicht thematisiert, da den beiden IT-Sicherheitsforschern gemäss eigenen Angaben zu wenig Informationen für eine Beurteilung vorlagen. Die Absicht der Kantone St.Gallen und Thurgau, den Quellcode des neu zu beschaffenden Ergebnisermittlungssystems offenzulegen, wurde hingegen explizit positiv gewürdigt.

48 Siehe auch Medienmitteilung der Staatskanzlei vom 22. August 2022 unter https://www.sg.ch/news/sgch_allgemein/2022/08/-expertinnen-und-experten-koennen-ergebnisermittlungssystem-test.html.

49 Sämtliche Informationen zum Bug-Bounty-Programm von Abraxas finden sich im Internet unter https://www.bug-bounty.ch/abraxas/; die Dokumentationen und der Quellcode unter https://github.com/abraxas-labs.

nisermittlungssystems weiter zu stärken. Aufgrund der positiven Erfahrungen mit dem Bug-Bounty-Programm zu *VOTING Ausmittlung* haben die Staatskanzlei und Abraxas zudem gemeinsam entschieden, nach und nach auch sämtliche anderen Applikationen im Bereich der politischen Rechte ins Bug-Bounty-Programm aufzunehmen und deren Quellcodes auf diese Weise einer öffentlichen Überprüfung zugänglich zu machen.[50]

In Ergänzung zu den bereits besprochenen Bestrebungen zur Erhöhung der Transparenz gegen aussen wurden im neuen Ergebnisermittlungssystem auch verschiedenen Massnahmen umgesetzt, welche die Nachvollziehbarkeit der Handlungen innerhalb des Systems – also der Eingaben, Korrekturen und Löschungen durch die Mitarbeitenden der Gemeinden und der Staatkanzlei – deutlich verbessern. So kann *VOTING Ausmittlung* nur noch mit persönlichen Logins und einer zusätzlichen Authentifizierung durch einen zweiten Faktor (*SG-Login-App*) benutzt werden. Zudem werden sämtliche Mutationen im System in Transaktions-Logs aufgezeichnet, die bei Bedarf eingesehen werden können, und kritische Prozessschritte (wie beispielsweise die Freigabe des fertig ausgezählten Gemeindeergebnisses zuhanden der Staatskanzlei) müssen von der verantwortlichen Person mittels Eingabe des zweiten Faktors bestätigt werden. Diese Massnahmen dienen nicht zuletzt auch dem Schutz der Mitarbeitenden.[51] Denn damit lässt sich im Fall einer Unregelmässigkeit exakt nachvollziehen, wer wann was eingegeben hat (wie der Fall der Wahlfälschung bei den Thurgauer Grossratswahlen 2020 gezeigt hat, kann das Fehlen einer Möglichkeit, eine Handlung einer einzelnen Person oder einem eng definierten Personenkreis zuzuschreiben, zur Folge haben, dass eine grössere Anzahl an Personen während längerer Zeit unter Verdacht steht, siehe Abschnitt 5.1).

Auch der Grundsatz «Sicherheit vor Tempo» kommt nicht mehr nur im Kontext von E-Voting zur Anwendung, sondern ist in vielen Gemeinden und Kantonen das prozessleitende Prinzip, wenn es um die Auszählung der Stimmen bei Wahlen und Abstimmungen geht.[52] Gerade im Spannungsverhältnis mit dem insbesondere an Wahltagen oftmals verspürten Druck, die Ergebnisse möglichst früh zu kommunizieren, kommt ihm eine besondere Bedeutung zu. Darüber hinaus dient der Grundsatz als wichtige Leitlinie für die Erschliessung neuer Themengebiete im Bereich der politischen Rechte und insbesondere für die Entwicklung der damit zusammenhängenden technischen Lösungen (wie z.B. E-Collecting).

5 Fokus Organisatorische Herausforderungen

Wie an verschiedenen Stellen im vorliegenden Bericht bereits erwähnt, hängt das Vertrauen der Bevölkerung in die korrekte Durchführung von Wahlen und Abstimmungen nicht nur vom Umgang der beteiligten Personen und Behörden mit den Risiken ab, die sich aus dem Einsatz von Computern und digitalen Services ergeben. Auch organisatorische Herausforderungen und insbesondere Pannen oder öffentlich gewordene Versäumnisse haben das Potenzial, dieses Vertrauen zu beeinträchtigen. Anhand zweier Beispiele aus der jüngeren Vergangenheit – der Wahlfälschung bei den Thurgauer Grossratswahlen im März 2020 («Fall Frauenfeld») und der Auszählungspanne bei der Wahl des St.Galler Stadtparlamentes am 22. September 2024 – soll

50 Aktuell umfasst das Bug-Bounty-Programm neben *VOTING Ausmittlung* auch die Applikationen *VOTING Stimmunterlagen Online*, *VOTING Stimmunterlagen Offline*, *VOTING Stimmregister* sowie *VOTING Wahlvorschlag*. Ende August wurde zudem die neue E-Collecting-Plattform des Kantons St.Gallen ins Programm aufgenommen und 2026 wird, wie in Abschnitt 3.2.3 erwähnt, die neue Einwohnerkontroll-Lösung der Gemeinden (*DME*) dazu kommen.

51 Nach anfänglichen Reklamationen einzelner Gemeinden aufgrund der aufwändigeren initialen Einrichtung der benötigten Benutzerkonten sind die persönlichen Logins und die 2-Faktor-Authentifizierung seit längerem kein Thema von Rückmeldungen mehr und deren Vorteile werden seitens der Gemeinden nicht mehr angezweifelt.

52 Entsprechende Referenzen finden sich beispielsweise im Schlussbericht des Instituts für Politikwissenschaft der Universität Zürich zur externen Untersuchung der Wahl- und Abstimmungsprozesse der Stadt St.Gallen (siehe Abschnitt 5.2) oder auch im Bericht der Thurgauer Staatskanzlei zur Wahlfälschung in der Stadt Frauenfeld bei den Grossratswahlen vom 15. März 2021 (siehe Abschnitt 5.1).

deshalb aufgezeigt werden, welche (für alle Gemeinden gleichermassen gültigen) Schlüsse im Hinblick auf zentrale organisatorische und prozedurale Erfordernisse wie die sichere Lagerung des Stimmmaterials, die Aufbewahrung und Protokollierung des Reservematerials oder die Einhaltung der etablierten Prozesse gezogen werden können.

5.1 Erkenntnisse aus dem «Fall Frauenfeld»

Die in den Medien als «Fall Frauenfeld» bekannt gewordene Wahlfälschung ereignete sich im Nachgang zu den Thurgauer Grossratswahlen vom 15. März 2020. In der Einleitung zu ihrem am 8. November 2021 veröffentlichten Untersuchungsbericht[53] (S. 1) fasst die Staatskanzlei des Kantons Thurgau die Ereignisse folgendermassen zusammen:

> *Im Nachgang zu den Grossratswahlen vom 15. März 2020 wurden in der Stadt Frauenfeld Unregelmässigkeiten festgestellt. Zwei Tage nach der Wahl meldete die Stadt Frauenfeld, nachdem sie [durch die Staatskanzlei] aufgefordert worden war, die unveränderten Wahlzettel zu kontrollieren, es seien fälschlicherweise 100 unveränderte Wahlzettel [...] der Liste Nr. 06 (glp) bei der Liste Nr. 09 (SVP) abgelegt und gezählt worden. In der Folge überprüfte die Staatskanzlei die Ergebnisse der Stadt Frauenfeld. Die Überprüfung ergab, dass die Zahl und die Zuordnung der physisch vorhandenen unveränderten Wahlzettel nicht stimmen konnten. Es bestand der Verdacht auf eine Wahlfälschung. Die Staatskanzlei erstattete deshalb bei der Staatsanwaltschaft Anzeige gegen unbekannt.*

Wie die Untersuchungen der Staatskanzlei und später auch der Staatsanwaltschaft ergeben haben, stimmte die Zahl der physisch vorhandenen unveränderten Wahlzettel auch nach der Korrektur durch die Stadt Frauenfeld nicht mit der Zahl der Wahlzettel überein, die sich aufgrund der Auswertung der Laufzettel (im Kanton St.Gallen sind diese auch als Bundblätter bekannt) hätte ergeben müssen. Vielmehr erhärtete sich der Verdacht, dass «minimal 86 und maximal 99 unveränderte [Wahlzettel] der Liste 06 (glp) vernichtet und durch unveränderte Wahlzettel der Liste 09 (SVP) ersetzt worden» sind (Untersuchungsbericht, S. 7). Dies wurde auch durch die kriminaltechnischen Ermittlungen der Staatsanwaltschaft bestätigt. Letztere ergaben, dass es sich im Fall von mindestens 86 der unveränderten Wahlzettel der Liste 09 (SVP) nicht um gültig abgegebene Stimmen handeln konnte, sondern vielmehr um nachträglich hinzugefügte Wahlzettel aus dem Reservematerial der Stadt Frauenfeld handeln musste, die den Auszählungsprozess nie durchlaufen hatten.[54]

In der Konsequenz führte dieser Befund zu einer nachträglichen Sitzverschiebung zu Gunsten der Grünliberalen, während die SVP den ihr im Nachgang zur Grossratswahl zu Unrecht zugesprochenen Sitz verlor. Darüber hinaus erhob die Staatsanwaltschaft Anklage wegen qualifizierter Wahlfälschung gegen den ehemaligen Stadtschreiber von Frauenfeld.[55] Das Bezirksgericht Frauenfeld sah es im Rahmen der Hauptverhandlung vom 6. Juli 2021 als erwiesen an, dass eine Manipulation der Wahlzettel stattgefunden hatte und dass der ehemalige Stadtschreiber diese vorgenommen haben muss. Es verurteilte ihn deshalb zu 12 Monaten Gefängnis bedingt. Das Urteil wurde im nachfolgenden Berufungsverfahren sowohl vom Thurgauer Obergericht als auch vom Bundesgericht in allen zentralen Punkten gestützt.[56]

---

53 Der vollständige Bericht der Staatskanzlei des Kantons Thurgau zur Wahlfälschung in der Stadt Frauenfeld bei den Grossratswahlen vom 15. März 2021 findet sich im Internet unter https://rechtsdienst.tg.ch/public/upload/assets/165904/211108_SK_Bericht_Wahlf%C3%A4lschung_Frauenfeld_GRW_2020.pdf?fp=1726466698833.

54 Diese Einschätzung beruhte unter anderem auf der Tatsache, dass die fraglichen Wahlzettel im Vergleich deutlich weniger Gebrauchsspuren (Fingerabdrücke, Verwischungen etc.) sowie keine oder nur sehr schwach ausgeprägte Faltungen aufwiesen.

55 Qualifiziert bedeutet in diesen Zusammenhang, dass der Angeklagte die ihm vorgeworfene Wahlfälschung in seiner amtlichen Eigenschaft als Stadtschreiber begangen hatte.

56 Vgl. Urteil OGer TG SBR.2021.80 vom 1. Juni 2022 sowie Urteil BGer 6B_1437/2022 vom 2. August 2023.

Mit Blick auf die Sicherheit und Vertrauenswürdigkeit von Wahlen und Abstimmungen lassen sich aus dem «Fall Frauenfeld» vier Erkenntnisse ableiten:

– Da die unveränderten Wahlzettel im Fall von Proporzwahlen nicht einzeln im Ergebnisermittlungssystem erfasst werden, ist es wichtig, dass deren Anzahl auf verschiedene Weisen erhoben wird (z.B. Zählung mit Präzisionswaage plus Auswertung der Bundblätter) und dass die ermittelten Zahlen anschliessend miteinander verglichen werden (siehe auch Abschnitt 3.6.3).

– Die sichere Lagerung des Stimmmaterials an einem Ort, zu dem möglichst wenige Personen Zugang haben, ist absolut zentral. Wie aus dem Bericht der Thurgauer Staatskanzlei hervorgeht, wurden die ausgezählten Wahlzettel in Frauenfeld in einem Kellerabteil gelagert, zu dem sich insgesamt 19 Personen hätten Zugang verschaffen können (Untersuchungsbericht, S. 11). Entsprechend lange hat es gedauert, bis alle diese Personen (mit Ausnahme des letztlich verurteilten ehemaligen Stadtschreibers) als Verdächtige ausgeschlossen werden konnten. Wie in Abschnitt 3.5.3 bereits erläutert, sollten die bestehenden Vorgaben dahingehend präzisiert werden, dass das Stimmmaterial zwingend in einem Safe gelagert werden muss, der lediglich von einer überschaubaren Anzahl an Personen geöffnet werden kann – im Idealfall nur von zwei Personen gemeinsam. Dadurch würde eine unerkannte Entnahme von Stimmmaterial nahezu verunmöglicht.

– Sämtliche Handlungen, die in Zusammenhang mit der Ermittlung der Ergebnisse einer Wahl oder einer Abstimmung stehen, dürfen nur im Vieraugenprinzip vorgenommen werden. Dazu gehören auch Handlungen im Nachgang zur eigentlichen Auszählung wie beispielsweise Nachzählungen. Zudem empfiehlt es sich, entsprechende Handlungen zu protokollieren. Diese Praxis dient nicht nur dem Schutz des Stimmmaterials, sondern auch dem Selbstschutz der involvierten Mitglieder des Stimmbüros.

– Die Gemeinden müssen jederzeit wissen, über wie viel Reservematerial sie noch verfügen. Im Rahmen der Ermittlungen zur Wahlfälschung in Frauenfeld waren umfangreiche Abklärungen nötig – unter anderem auch bei der mit der Verpackung beauftragten Firma Abraxas –, um eingrenzen zu können, über wie viele Wahlzettelsets die Stadt Frauenfeld noch verfügte (und damit letztlich auch, um bestimmen zu können, ob genug Wahlzettel für den oben geschilderten Austausch der unveränderten Listen der glp durch solche der SVP vorhanden waren). Wie in Abschnitt 3.5.3 ebenfalls bereits diskutiert, sollten die bestehenden Vorgaben daher dahingehend erweitert werden, dass sie auch mit Blick auf die Lagerung des Reserve-Stimmmaterials Anwendung finden und der aktuelle Bestand an Reservematerial von den Gemeinden fortlaufend protokoliert werden muss. Zudem sollte geprüft werden, ob auch das Reservematerial erst zum Zeitpunkt der Erwahrung vernichtet werden darf, da es im Fall einer Nachzählung unter Umständen Erkenntnisse erlaubt, die auf anderem Wege nicht zu erhalten sind.

5.2 Erkenntnisse aus der Wahlpanne in der Stadt St.Gallen

Am 22. September 2024 kam es im Rahmen der kommunalen Gesamterneuerungswahlen in der Stadt St.Gallen zu einem Fehler bei der Auszählung der Stimmen für das Stadtparlament. Dieser wurde am darauffolgenden Tag vom Präsidenten und der Sekretärin des Stimmbüros festgestellt und die Öffentlichkeit wurde noch gleichentags über die nötig gewordene Korrektur der Ergebnisse informiert.[57] Wie die Stadt in ihrer Medienmitteilung ausführte, passierte der Fehler bei der manuellen Erfassung der unveränderten Wahlzettel und ist auf menschliches

[57] Die Medienmitteilung der Stadt St.Gallen vom 23. September 2024 findet sich im Internet unter https://www.stadt.sg.ch/news/stsg_medienmitteilungen/2024/09/erneuerungswahlen-stadtparlament-2024--korrektur-der-ergebnisse.html.

Versagen zurückzuführen. Konkret wurde in der Excel-Datei, die zur Summierung der am Samstag und am Sonntag je separat ausgezählten, unveränderten Wahlzettel verwendet wird, aus Versehen eine falsche Formel hinterlegt. In der Folge wurde für die Liste «02a FDP.Die Liberalen» eine zu hohe Anzahl an Parteistimmen errechnet, die anschliessend im Ergebnisermittlungssystem erfasst wurde. Dieser Fehler hatte zur Konsequenz, dass bei der Berechnung der Sitze gestützt auf die Parteistimmen sämtlicher Listen der Liste «02a» – im Vergleich zu den korrekten Ergebnissen – fünf Sitze zu viel, der Liste «01a» hingegen zwei Sitze zu wenig und den Listen «03», «04» sowie «05a» je ein Sitz zu wenig zugeteilt wurden.

Die Auszählungspanne löste im Nachgang zum Wahlsonntag eine intensive Medienberichterstattung und teilweise negative Reaktionen in der Politik und bei der Bevölkerung aus.[58] In der Folge trat der Präsident des Stimmbüros von dieser Funktion zurück. Zudem beauftragte der Stadtrat am 5. Dezember 2024 das Institut für Politikwissenschaft der Universität Zürich (IPZ) mit einer externen Untersuchung der Wahl- und Abstimmungsprozesse in der Stadt St.Gallen.[59]

Im Rahmen des vorliegenden Berichts soll nicht im Detail auf die Erkenntnisse und Empfehlungen des IPZ eingegangen werden, da der Fokus der Untersuchung schwergewichtig auf der Frage lag, wie die Organisation, die Instrumente und die Abläufe im Stimmbüro der Stadt St.Gallen angepasst werden können, so dass Auszählungspannen wie am 22. September 2024 in Zukunft vermieden werden können. Eine zentrale Feststellung mit Blick auf die Faktoren, die den Auszählungsfehler begünstigt haben – bzw. den Fakt, dass der Fehler nicht bereits vor der Veröffentlichung der Ergebnisse bemerkt wurde –, ist aber detaillierter zu beleuchten. So hält der Bericht des IPZ fest, dass «[zu] Beginn der Auszählung die Anzahl der für die Stadtparlamentswahl eingegangenen Wahlzettel nicht ermittelt wurde (S. 11)». Stattdessen wurde sogleich mit der Sortierung, Bereinigung und Erfassung der Wahlzettel in *VOTING Ausmittlung* begonnen.

Dieses Versäumnis hat zu zweierlei Problemen geführt: Zum einen wurde dadurch verunmöglicht, dass die Zahl der (vorgängig gezählten) eingegangenen Wahlzettel mit dem Total der im Ergebnisermittlungssystem erfassten veränderten, unveränderten, leeren und ungültigen Wahlzettel verglichen werden konnte. Aus diesem Vergleich «wäre ersichtlich geworden, dass nach Abschluss der Ergebnisermittlung 1'337 Wahlzettel zu viel ausgewiesen wurden (IPZ, S. 11)». Zum anderen wurde mit dem Verzicht auf eine vorgängige Zählung (und die Erfassung der in deren Zuge ermittelten Werte) auch die in *VOTING Ausmittlung* integrierte Validierungsprüfung ausgehebelt (siehe auch Abschnitt 3.6.3), die ebenfalls auf das inkorrekte Ergebnis hingewiesen bzw. den Abschluss der Ergebniserfassung im Fall der Wahl des Stadtparlamentes verhindert hätte.

Zusammenfassend kann deshalb festgehalten werden, dass die vorgegebenen und etablierten Prozesse mit Blick auf die korrekte Durchführung von Wahlen und Abstimmungen zwingend eingehalten werden müssen und nicht «abgekürzt» werden dürfen. Nur dann ist sichergestellt, dass die vorhandenen Sicherheitsmassnahmen auch ihre volle Wirkung entfalten können.

---

58 Vgl. beispielsweise https://www.tagblatt.ch/ostschweiz/stgallen/reaktionen-peinlicher-lapsus-schluderei-und-ganz-viel-zynismus-auszaehlungs-fiasko-sorgt-weit-ueber-stgallen-hinaus-fuer-wirbel-ld.2676350.

59 Der Schlussbericht zur externen Untersuchung der Wahl- und Abstimmungsprozesse der Stadt St.Gallen, den das Institut für Politikwissenschaft der Universität Zürich (IPZ) in Zusammenarbeit mit Stephan Ziegler, Leiter Wahlen und Abstimmungen des Kantons Zürich, erarbeitet hat, kann im Internet heruntergeladen werden unter https://stadtsg.ch/bericht-wahlen.

6 Fazit und weiterführende Massnahmen

In den vorangegangenen Abschnitten wurden die Sicherheit und die Vertrauenswürdigkeit des gesamten Prozesses der Vorbereitung und Durchführung von Wahlen und Abstimmungen analysiert, unter Berücksichtigung der verschiedenen digitalen Services, die in den einzelnen Phasen zum Einsatz kommen, sowie organisatorischer Herausforderungen. Dabei konnte nicht nur eine ganze Reihe an potenziellen Bedrohungen identifiziert werden, die das Potenzial haben, die ordnungsgemässe Durchführung einer Wahl oder Abstimmung zu beeinträchtigen, es wurde auch aufgezeigt, dass zur Eindämmung vieler dieser Bedrohungen bereits wirkungsvolle Gegenmassnahmen bestehen. So konnten insbesondere im Zuge der Entwicklung und Einführung des neuen Ergebnisermittlungssystems (*VOTING Ausmittlung*) zahlreiche Empfehlungen aus der Bedrohungsanalyse der Universität Zürich ebenso wie einige «best practices» aus den Erfahrungen mit der elektronischen Stimmabgabe direkt umgesetzt werden. Des Weiteren halten die Experten der UZH in ihrer Analyse fest, dass die Verantwortlichen an den involvierten Stellen – bzw. für die verschiedenen Prozessschritte – «für die Relevanz von Sicherheitsfragen innerhalb ihres Zuständigkeitsbereichs sensibilisiert sind» (UZH, S. 21). Insgesamt kann deshalb festgehalten werden, dass die Sicherheit und Vertrauenswürdigkeit der Wahlen und Abstimmungen im Kanton St.Gallen bereits auf einem sehr guten Stand sind.

Allerdings gibt es keine hundertprozentige Sicherheit, weder mit Blick auf den Einsatz von digitalen Services noch im Fall der papierbasierten Verfahrensschritte und organisatorischen Prozesse im Rahmen der Vorbereitung und Durchführung von Wahlen und Abstimmungen. In den Abschnitten 3 bis 5 wurden denn auch verschiedene mögliche Massnahmen erläutert, mit denen Sicherheit und Vertrauenswürdigkeit weiter gestärkt werden könnten. Diese betreffen hauptsächlich die beiden Bereiche, die aus einer risikobasierten Perspektive betrachtet als besonders sensitiv gelten müssen: die Manipulationssicherheit der Stimmrechtsausweise (da ohne diese keine gültigen Stimmen abgegeben werden können) sowie die sichere Lagerung des Stimmmaterials, namentlich bei den Gemeinden.

Die Regierung nimmt deshalb Folgendes in Aussicht:

– Vertiefte Prüfung der technischen und organisatorischen Umsetzbarkeit sowie der zu erwartenden Kosten eines Abgleichs der eingelangten Stimmabgaben mit dem stehenden Stimmregister durch das Einscannen eines zusätzlichen Datamatrix-Codes auf dem Stimmrechtsausweis (Massnahme M2, siehe auch Abschnitt 3.4.3). Im Rahmen der Prüfung sind auch die jeweiligen Bedürfnisse und Prozesse von Gemeinden unterschiedlicher Grösse sowie verschiedene technische Umsetzungsvarianten zu berücksichtigen. Sollte die Prüfung ergeben, dass die Massnahme sinnvoll und mit verhältnismässigen Kosten umsetzbar ist, sieht die Regierung vor, die entsprechenden Kosten zulasten des Kantons ins Budget bzw. in den Aufgaben- und Finanzplan einzustellen.

– Konkretisierung der bestehenden Vorgaben betreffend die Ermittlung der Zahl der unveränderten Wahlzettel im Fall von Proporzwahlen, die sichere Lagerung des Stimmmaterials und die Anwendung des Vieraugenprinzips sowie Erweiterung um zusätzliche Vorgaben zur Lagerung, Protokollierung und Vernichtung des Reservematerials (Massnahmen M12 und M13, siehe auch Abschnitt 3.5.3 sowie Ausführungen zum «Fall Frauenfeld» in Abschnitt 5.1). Die genaue Umsetzung ist mit den Gemeinden zu klären. Denkbar ist dabei z.B. der Erlass einer Verordnung der Regierung oder auch ein gemeinsamer Leitfaden von Kanton und Gemeinden.

– Definition der kritischen Prozessschritte im Rahmen der Auszählung von Wahlen und Abstimmungen und Erarbeitung einer Checkliste zuhanden der Stimmbüros der Gemeinden (siehe auch Abschnitt 3.6.3).

– Konsequentes Weiterverfolgen des bereits eingeschlagenen Wegs der schrittweisen Offenlegung der Quellcodes aller von der Staatskanzlei im Zuge der Vorbereitung und Durchführung von Wahlen und Abstimmungen eingesetzten Applikationen im Rahmen des Bug-Bounty-Programms von Abraxas (siehe auch Abschnitt 4.6).

7 Antrag

Wir beantragen Ihnen, Herr Präsident, sehr geehrte Damen und Herren, auf den vorliegenden Bericht einzutreten.

Im Namen der Regierung

Beat Tinner
Präsident

Dr. Benedikt van Spyk
Staatssekretär

Anhang: Analyse der Universität Zürich

[gemäss separatem Dokument]