University of Zurich[UZH]

Sicherheit und Vertrauenswürdigkeit von Wahlen und Abstimmungen im digitalen Umfeld

Christian Killer
Jan von der Assen
Burkhard Stiller

Stand der Inhalte: Juli 2022
Letzte redaktionelle Überarbeitung: Juni 2025

University of Zürich UZH
Department of Informatics IfI
Binzmühlestrasse 14
CH—8050 Zürich, Switzerland

Inhaltsverzeichnis

1 Prozessüberblick Wahlen- und Abstimmungen

Die Gesamtübersicht des Abstimmungsprozesses im Kanton St. Gallen ist in der Abbildung 1 skizziert. Der gesamte Prozess wurde dabei in sieben Phasen aufgeteilt und wird von diversen Beteiligten ausgeführt, welche in den jeweiligen Unterschritten die Sicherheit und Vertrauenswürdigkeit sicherstellen (vgl. Legende in Abbildung 1).

Die erste Phase der “Vorbereitung” umfasst vor allem den Druck der Stimmrechtsausweise, der Stimmzettel und anderer Beilagen, welches somit den Druck der gesamten Wahl- und Abstimmungsunterlagen umfasst. Diese werden anschliessend verpackt (“kuvertiert”), adressiert und in der zweiten Phase “Versand” durch die Schweizerische Post transportiert und zwischengelagert.

Nachdem die Unterlagen die Stimmberechtigten auf dem postalischen Weg erhalten haben, beginnt die dritte Phase, die “Stimmabgabe”. Hierbei ist den Stimmberechtigten freigestellt, welche der drei offerierten Möglichkeiten einer Stimmabgabe gewählt werden, der Rückversand auf postalischem Wege ist jedoch die am häufigsten gewählte Option.

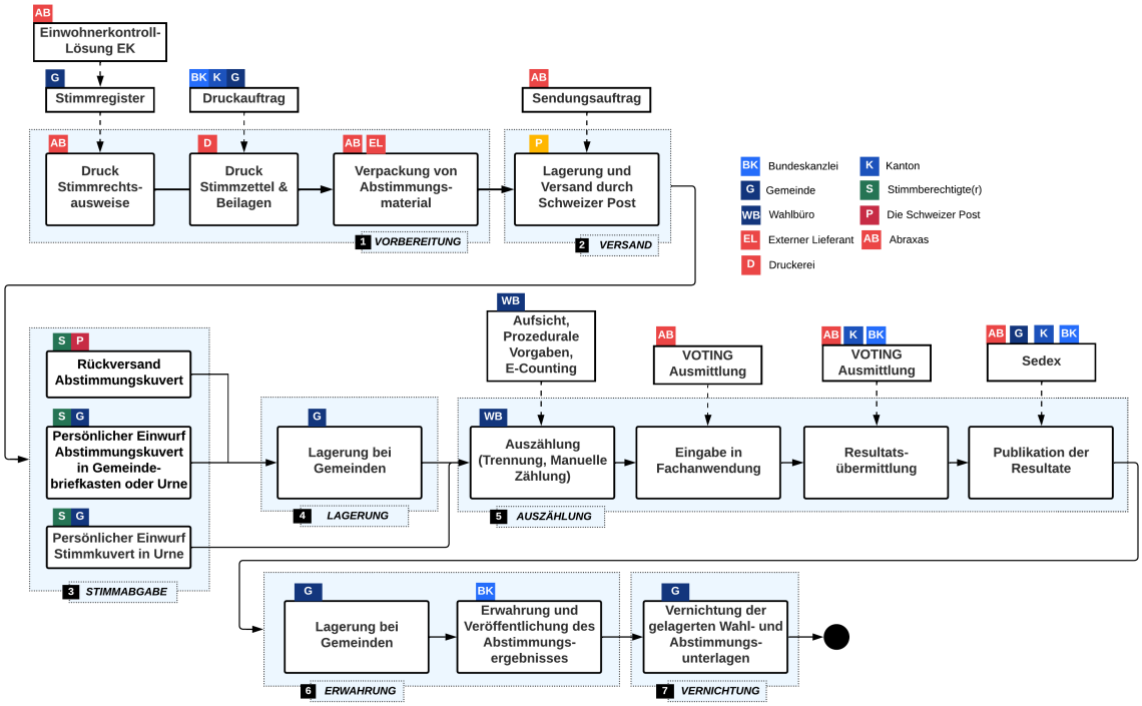

Abbildung 1: Prozessüberblick von Wahlen- und Abstimmungen Kanton SG

Nach Eingang der Stimmabgaben in der jeweiligen Gemeinde werden die Zustellkuverts sicher bis zum Abstimmungswochenende zwischengelagert, was in der Phase “Lagerung” definiert ist.

Die Phase der “Auszählung” beginnt am Abstimmungssonntag. Die Mitglieder des Stimmbüros öffnen zuerst die Zustelllkuverts, dann werden die Stimmrechtsausweise überprüft und anschliessend werden die Stimmzettelkuverts geöffnet. Die ermittelten Resultate werden neben einer papierbasierten Zusammenstellung schliesslich auch elektronisch erfasst und an die St. Galler Staatskanzlei übermittelt.

Nachdem diese Resultate publiziert wurden, werden die Wahl-, Stimmzettel und Stimmrechtsausweise bis zur “Erwahrung” durch die Bundeskanzlei, respektive die Regierung des Kantons St. Gallen, zwischengelagert.

In der letzten Phase des Prozessüberblicks, erfolgt die “Vernichtung” aller Wahl- und Abstimmungsunterlagen.

2 Bedrohungsanalyse

In der vorliegenden Bedrohungsanalyse werden die aktuell erkennbaren Bedrohungen für Wahl- und Abstimmungsprozesse des im Kanton St. Gallens relevanten Prozesse und deren Phasen zusammengefasst. Die im folgenden definierten Bedrohungen sind bewusst nicht allgemeiner Natur, sondern direkt für die analysierten Wahlen und Abstimmungen als relevant eingestuft worden, um sicherzustellen, dass messbare Gegenmassnahmen ermittelt werden können, die die betroffenen Prozessdetails bzw. Schwächen explizit adressieren. Allgemeine Bedrohungen für Informationssysteme werden kurz in Kapitel 6 summarisch behandelt.

2.1 Methodik

Der Wahl- und Abstimmungsprozess wird in sieben Phasen unterteilt, welche sich nach den vorzubereitenden und auszuführenden Aufgaben bzw. deren Ergebnissen aufteilen lassen[1]. Jede dieser Phasen findet in den nachfolgenden Unterkapiteln jeweils im Detail Beachtung, wobei jeweils neben der ausgeführten Prozessbeschreibung im Besonderen für diese Prozesse die relevanten Bedrohungen behandelt werden. Im Rahmen einer Bedrohungsanalyse werden diesen Bedrohungen die geplanten als auch die bereits umgesetzten Gegenmassnahmen gegenübergestellt. Dieses Vorgehen ermöglicht eine Bedrohungsanalyse, welche im Einzelnen auf die spezifischen Besonderheiten der jeweiligen Phasen eingeht und auf bereits existierende sowie auf geplante Gegenmassnahmen Rücksicht nimmt. Bedrohungen wurden aufgrund der prozeduralen Architektur und dem Vorhandensein von Gegenmassnahmen analysiert. Diese Betrachtung findet auf der Basis von konzeptionellen Details statt und beinhaltet keine Systemdetails (bspw. wurden keine Softwaresysteme im Detail analysiert). Deshalb werden zusätzliche, generelle Empfehlungen ausgesprochen, welche aus Sicht des Betriebs das Risiko der IT-Sicherheit weiter minimieren könnten.

Die Beschreibung der Bedrohungen verzichtet so weit wie möglich auf Begriffe der sicherheitstechnischen Fachsprache. Die wichtigsten Begriffe der folgenden Bedrohungsanalyse werden jedoch kurz wie folgt definiert: Eine (realistische) *Bedrohung* ergibt sich durch die (realistische) Möglichkeit, durch böswilliges Einwirken Schaden auf Schutzziele, wie der Vertrauenswürdigkeit, der Integrität oder der Verfügbarkeit eines digitalen Informationssystems oder eines durch Menschen behandelten Prozesses, zu erreichen. In diesem Kontext muss ein oder müssen die Angreifer einen spezifischen Angriffspfad, definiert durch den Angriffsvektor, auswählen. Unter der *Skalierbarkeit* eines Angriffs wird dann eine Einschätzung des benötigten Aufwands aus Sicht des oder der Angreifer verstanden.

Den Autoren liegen ausser den anekdotischen Sicherheitsvorfällen keine Daten vor, welche eine Erfassung der exakten Verletzlichkeiten der Systemen und Prozessen oder der Wahrscheinlichkeiten eines Angriffs ermöglichen. Deshalb wird auf eine systematische Quantifizierung der Risikoexposition im Folgenden verzichtet. Die beschriebenen Bedrohungen werden auf konzeptioneller Ebene im Bezug auf ihre Machbarkeit diskutiert und primär anhand ihres Schadenausmasses bewertet. Dafür werden als primäre Schutzziele die integre und erfolgreiche Durchführung einer Abstimmung oder Wahl und die Wahrung des Stimmgehminis definiert. Das Schadensausmass wird qualitativ beschrieben, wobei die drei Stufen («hoch», «mittel», «niedrig») die Anzahl an Stimmen beschreiben, welche realistisch von den profilierten Angreifenden gefälscht werden könnten. Während bei einem «niedrigen» Schadensausmass

[1] Killer, C., Stiller, B.: „The Swiss Postal Voting Process and Its System and Security Analysis“ In: 4th International Joint Conference on Electronic Voting (E-Vote-ID 2019), Bregenz, Austria, October 1–4, 2019, Available at: ttps://www.researchgate.net/publication/335997715_The_Swiss_Postal_Voting_Process_and_Its_System_and_Security_Analysis

einzelne Stimmen gefälscht würden, beschreibt ein «hohes» Ausmass ein Szenario, in dem der Angriff auf einen substanziellen Anteil der Wählerbasis ausgeweitet werden kann.

Diese Qualifizierung muss deshalb vorsichtig interpretiert werden, da je nach Wahlgang bereits einzelne Stimmen das Wahlergebnis beinflussen könnten. Im weiteren muss beachtet werden, dass eine Bedrohungsanalyse lediglich einen möglichen Satz an relevanten Bedrohungen beschreibt und die Existenz anderer, nicht beschriebener Bedorhungen nicht ausschliessen kann. Dies beinhaltet sowohl nicht identifizierte Bedrohungen, welche das beschriebene Schutzziel betreffen ebenso wie verwandte Bedrohungen, welche hier bewusst nicht beschrieben werden (bspw. Missbrauch von internem Wissen zum Handel auf Aktienmärkten).

2.2 Vorbereitung

Die "Vorbereitung" ist die einleitende Phase des Wahl- und Abstimmungsprozesses (vgl. Abb. 2). Die Vorbereitungsphase beinhaltet drei Schritte, in welchen der Druck der Stimmrechtsausweise, der Druck der Stimmzettel und Beilagen sowie deren Verpackung und Adressierung stattfinden. Die Vorbereitungsphase wird mit der Übergabe des Stimm- und Wahlmaterials an die Schweizerische Post abgeschlossen.

2.2.1 Prozessbeschreibung

Der Prozess beginnt im Schritt “Druck Stimmrechtsausweise”, wobei diverse Systeme zum Einsatz kommen. Einerseits die Einwohnerkontroll-Lösung EK für den Export des Stimmregisters und die Generierung der Stimmrechtsausweise. Zudem wird in vier Pilotgemeinden das Tool “VOTING Stimmausweis” getestet. Ende 2022 werden eine Reihe weiterer “VOTING” Tools eingeführt werden, welche eine vereinheitlichte Pflege von Stammdaten, Urnengängen und Geschäften ermöglichen. Normale Stimmrechtsausweise (nicht im E-Voting) werden über CONNECT SG an das Druck- und Verteilzentrum (DVZ) der Abraxas oder über den von der Gemeinde gewählten Connector Endpunkt übermittelt. Für die Übermittlung der E-Voting-Stimmrechtsausweise wurde ein komplexerer Prozess definiert, welcher asymmetrische Verschlüsselung und den Einsatz von Offline-Geräten kombiniert. Es wird ebenfalls CONNECT SG zur Übermittlung an das DVZ verwendet. Für den E-Voting-Stimmrechtsausweis existiert eine gesonderte Druckstrasse, welche vollständig offline arbeitet und in welcher die Druckdaten per separatem USB-Stick eingelesen werden.

Der Schritt “Druck Stimmzettel & Beilagen” umfasst den Druck der Stimmzettel und der Abstimmungsbroschüren, welche je nach Vorlage durch die Bundeskanzlei, die Staatskanzlei oder durch die jeweiligen Gemeinden in Auftrag gegeben werden. Externe Druckereien führen diese Druckaufträge aus und senden die gedruckten Stimmzettel und Beilagen für die Verpackung und den Versand an die Firma Abraxas.

Anschliessend müssen die gedruckten Stimmrechtsausweise, die Stimmzettel und die Beilagen zusammen korrekt verpackt werden. In den meisten Fällen geschieht dieses durch die Firma Abraxas, welche die verpackten Unterlagen anschliessend der Schweizerischen Post zum Versand an die Stimmberechtigten übergibt. Hierfür wird die Spezialdienstleistung "Wahl- und Abstimmungssendung"[2] der Schweizerischen Post verwendet.

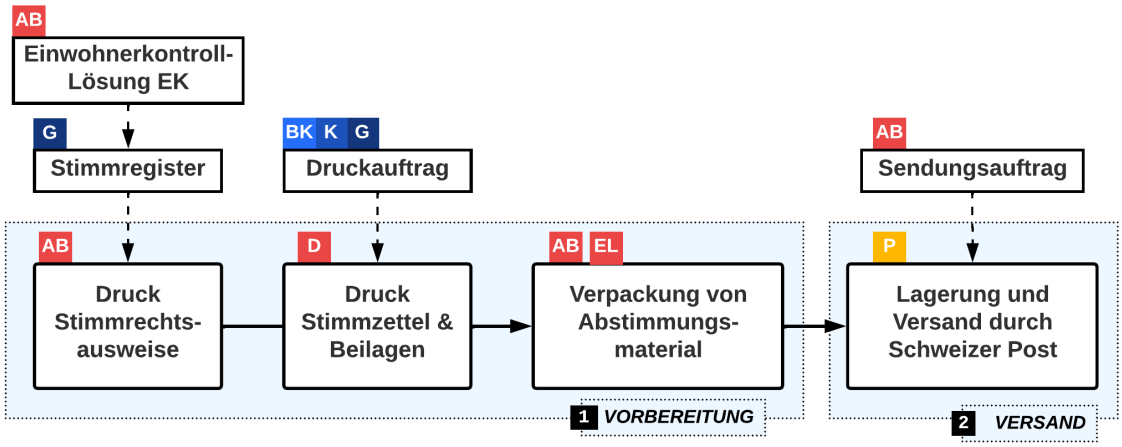

Abbildung 2: Vorbereitung und Versand des Abstimmungsmaterials

[2] Die Post, "Wahl- und Abstimmungssendung" https://www.post.ch/de/briefe-versenden/dokumenten-und-urkunden/wahl-und-abstimmungssendung

2.2.2 Bedrohungen & Gegenmassnahmen

ID	Beschreibung	Schadensausmass
B1	Diebstahl und Missbrauch von Abstimmungsmaterial, insbesondere der Stimmrechtsausweise	HOCH
B2	Fälschung von Abstimmungsmaterial, insbesondere der Stimmrechtsausweise	HOCH
B3	Verzögerung Druck Abstimmungsunterlagen (Stimmrechtsausweise, Stimmzettel und Beilagen)	NIEDRIG
B4	Manipulation des Stimmregisters (Hinzufügen, Löschen, Ändern)	MITTEL
B5	Konsistenz des Stimmregisters (bspw. bei Umzug von Bewohner und Bewohnerinnen)	NIEDRIG

Bedrohung B1: Bedrohung B1 subsumiert eine Bandbreite von Bedrohungen, welche die physische Lagerung, Verpackung und Zustellung der Abstimmungsmaterialien betreffen. Der sicherheitsrelevante Fokus liegt dabei klar auf dem Stimmrechtsausweis, da ohne gültigen Stimmrechtsausweis keine Stimmabgabe möglich ist. Die Überprüfung der Stimmrechtsausweise wird von Mitgliedern der Stimmbüros durchgeführt, was sowohl Manipulations- als auch Fehlerpotenzial mit sich bringt. Um den Aufwand eines Angriffs einzuschätzen, muss berücksichtigt werden, dass ein Angriff an verschiedenen Stellen dieses Prozesses möglich ist. Zunächst wird das Abstimmungsmaterial in der Druckerei hergestellt und zwischengelagert. Obschon dieses an einem zentralen Ort geschieht, erschweren vorhandene Prozesskontrollen den Angriff. Beispielsweise werden die Daten für Druckaufträge im Falle der E-Voting-Stimmrechtsausweise verschlüsselt übertragen und erst in der Druckerei entschlüsselt. Es können aber auch andere Abstimmungsunterlagen (beispielsweise Stimmzettel) gestohlen oder kopiert werden. Da diese Unterlagen jedoch nicht an die Identitäten von Stimmberechtigten gebunden sind, kann nur im später behandelten Schritt der “Auszählung” versucht werden, einen manipulierten, zusätzlichen Stimmzettel aktiv in den Auszählungsprozess einzubringen. Dieses führt jedoch zu fehlerhaften Stimmzettelanzahlen (siehe B14). Aus Sicht der Bedrohung B1 ist deswegen primär der Stimmrechtsausweis sicherheitsrelevant.

Bedrohung B2: Die Bedrohung B2 beschreibt Angriffsmöglichkeiten, welche eine Vervielfachung der Abstimmungsmaterialien, insbesondere des Stimmrechtsausweises, betreffen. Dadurch lassen sich Stimmen fälschen und somit das Ergebnis von Wahlen und Abstimmungen beeinflussen. Eine Erkennung und Eindämmung dieses Angriffs sind zum Stand der momentanen Umsetzung schwierig. Zunächst sind mögliche Diskrepanzen nur anhand von offensichtlichen Mehrfachstimmabgaben oder physischen Unregelmässigkeiten des Stimmrechtsausweises zu erkennen. Weiter ist es nicht möglich, einmal bemerkte Unregelmässigkeiten zu bereinigen, da zu diesem Zeitpunkt die Stimmrechtsausweise in der Regel bereits vom restlichen Abstimmungsmaterial bereits getrennt sind.

Existierende und geplante Gegenmassnahmen für B1 und B2: Beide Bedrohungen werden als zentral angesehen, da noch keine Gegenmassnahmen definiert oder umgesetzt sind. Es befinden sich jedoch mehrere Abwehrmassnahmen in Planung, um diesen Bedrohungen entgegenzuwirken. Als zentrale Gegenmassnahme ist die Einführung von zusätzlichen Sicherheitsmerkmalen auf den Stimmrechtsausweisen geplant (siehe B14). Zusätzlich ist eine Softwarelösung in Entwicklung, welche den Herstellungsprozess von Abstimmungsunterlagen digital unterstützt und damit unbewusste oder bewusste Manipulationen von beteiligten Personen minimiert. Mit dieser Lösung ist es vorgesehen, einen Abgleich zwischen der Anzahl hergestellter Abstimmungsunterlagen und dem Stimmregister vorzunehmen, um Fehlern in der Herstellung vorzubeugen. Zudem wird mit diesem Vorgehen vorgebeugt, dass keine gefälschten Stimmrechtsausweise eingeschleust

werden können. Die Behandlung von Spezialfällen, wie umziehenden Stimmberechtigten von einer Gemeinde in eine andere, bleibt hiervon unbenommen.

Bedrohung B3: Die Bedrohung B3 beschreibt eine mögliche Verzögerung im Druckprozess, welche sowohl den Druck der Stimmrechtsausweise als auch den Druck von Stimmzetteln und Beilagen betreffen kann. Durch eine Verzögerung kann der gesamte Prozess behindert werden, da theoretisch die nötigen Unterlagen nicht rechtzeitig für den Versand bereit sind und damit die gesetzlich vorgeschriebenen Fristen für die Zustellung des Wahl- und Abstimmungsmaterials an die Stimmberechtigten verletzt werden könnten.

Bedrohung B4: Die Bedrohung B4 beschreibt eine Manipulation des Stimmregisters. Zum Beispiel könnten Stimmberechtigte entfernt, hinzugefügt oder deren Daten (bspw. die Wohnadresse) verändert werden. Dadurch könnten Stimmberechtigte von der Abstimmung ausgeschlossen oder als fiktive Stimmberechtigte hinzugefügt werden. Die meisten Gemeinden verwenden zur Verwaltung der Stimmberechtigten ein System, das von der Firma Abraxas mandantenfähig betrieben wird. Ein direkter Angriff auf die Firma Abraxas wäre ebenfalls mit hohem Aufwand verbunden, da dort entsprechend prozedurale Sicherheitsmassnahmen (siehe “Geplante und umgesetzte Gegenmassnahmen für B3, B4 und B5”) bereits eingesetzt werden.

Bedrohung B5: Die Bedrohung B5 betrifft die Daten der Einwohnerregister, welche in jeder Gemeinde verteilt geführt werden. Inkonsistenzen könnten beispielsweise als Folge von Mutationen (Zu- oder Wegzug von Stimmberechtigten) nach dem Versand des Stimmmaterials für einen Urnengang entstehen. Die Skalierbarkeit eines Angriffs gestaltet sich hier schwierig, weil grosse Differenzen im Stimmregister auffallen würden. Ausserdem ist gesetzlich geregelt, dass Neuzuzüger nur im Austausch gegen den Stimmrechtsausweis, welcher in der alten Gemeinde bereits ausgestellt wurde, einen neuen Stimmrechtsausweis erhalten. Somit sind Angriffe, welche kleine Differenzen im Endresultat zur Folge haben, zwar denkbar, eine Veränderung des Ergebnisses mit einer grossen Zahl von Stimmen erscheint jedoch sehr unwahrscheinlich.

Existierende und geplante Gegenmassnahmen für B3, B4 und B5: Als existierende Gegenmassnahme für B3 sind die gesetzlich vorgeschriebenen Fristen zum Versand der Wahl- und Abstimmungsunterlagen massgebend. Für die Zustellungen von Wahl- und Abstimmungsmaterialien ist der zeitliche Rahmen gesetzlich geregelt. So gilt, dass die Wahl- und Abstimmungsunterlagen bei eidgenössischen Geschäften frühestens 28 Tage und spätestens 21 Tage vor der Abstimmung zugestellt sein müssen. Im Falle einer Verzögerung gewähren diese Fristen der Regierung genügend Zeit, um einen erneuten Druck und Versand einzuleiten.

Um B4 entgegenzuwirken, steht die Informationssicherheit der Firma Abraxas im Vordergrund. Die Firma Abraxas ist ISO 27001 zertifiziert, was bedeutet, dass organisatorische Risiken regelmässig überprüft und mit entsprechenden Sicherheitsmassnahmen implementiert werden. Die Einhaltung dieses Sicherheitsmanagements auf Seiten der Firma Abraxas wird von einem unabhängigen Auditor geprüft.

Als existierende Gegenmassnahme für B5 besteht die Vorgabe, dass Neuzuzüger nur gegen Vorweisen des alten Stimmrechtsausweises einen von der neuen Wohngemeinde ausgestellt bekommen. Eine Einführung des zurzeit geplanten und in Entwicklung befindendem “stehenden Stimmregisters” erlaubt in der Zukunft, weitere Gegenmassnahmen zu realisieren (vgl. Umgesetzte und Geplante Gegenmassnahmen B1 und B2). Solch ein stets aktuelles und abfragbares Stimmregister erlaubt, Gewissheit über die Datenbestände und Identitäten zu erlangen, was für den Druck der Stimmrechtsausweise (aber auch später für die Auszählung) relevant ist.

2.3 Versand

Der “Versand" definiert die zweite Phase des Abstimmungsprozesses (vgl. Abb. 2). Die Versandphase beinhaltet im Besonderen die Lagerung bei der Post und den Versand der Abstimmungsunterlagen.

2.3.1 Prozessbeschreibung

Nach der Produktion der Abstimmungsunterlagen wird die Schweizerische Post AG mit dem Versand der Abstimmungsunterlagen beauftragt. Die Post holt diese ab und lagert die Unterlagen, wenn nötig, zwischen, bevor der Versand erfolgt. Gemäss Art. 11 Abs. 3, Art. 33 Abs. 2 und Art. 48 des Bundesgesetzes über die politischen Rechte (BPR) lassen die Kantone den Stimmberechtigten mindestens drei sowie frühestens vier Wochen vor dem Wahltag einen vollständigen Satz aller Wahlzettel zustellen.

2.3.2 Bedrohungen & Gegenmassnahmen

ID	Beschreibung	Schadensausmass
B6	Diebstahl von Abstimmungsmaterial während Lagerung bei der Schweizerischen Post	MITTEL
B7	Zerstörung von Abstimmungsmaterial während Lagerung bei der Schweizerischen Post	NIEDRIG
B8	Diebstahl von Abstimmungsmaterial nach Versand an Stimmberechtigte (bspw. aus dem Briefkasten)	MITTEL
B9	Zerstörung von Abstimmungsunterlagen nach Versand an die Stimmberechtigten	NIEDRIG

Bedrohung B6: Die Bedrohung B6 umfasst den Diebstahl der Abstimmungsunterlagen während der Lagerung bei der Schweizerischen Post. Der Aufwand für einen solchen Diebstahl ist, aufgrund der vorhandenen Sicherheitsmechanismen der Schweizerischen Post, als hoch einzuschätzen. Hier muss angemerkt werden, dass diese Einschätzung auf der Annahme beruht, dass die Schweizerische Post Sicherheitsmassnahmen in ihre Prozesse einbindet. Bliebe ein Diebstahl unbemerkt und würden die gestohlenen Abstimmungsunterlagen vom Angreifer ausgefüllt und abgesandt, wäre es schwierig, legitime von missbräuchlich verwendeten Unterlagen zu unterscheiden. Bei einer substanziellen Anzahl gestohlener Unterlagen kann jedoch davon ausgegangen werden, dass eine genügend grosse Anzahl von Stimmberechtigten bemerkt, dass die Abstimmungsunterlagen nicht angekommen sind und dies der Gemeinde meldet.

Bedrohung B7: Die Bedrohung B7 betrifft die Zerstörung der Abstimmungsunterlagen während der Lagerung bei der Schweizerischen Post. Da es wahrscheinlich ist, dass ein Nichterhalt von den Stimmberechtigten bemerkt würde, könnte durch einen solchen Angriff primär eine Verzögerung der Zustellung erreicht werden.

Existierende oder geplante Gegenmassnahmen für B6 und B7: Für die Bedrohungen B6 und B7 ist die physische Sicherheit der Schweizerischen Post massgebend. Die genauen Massnahmen – ausserhalb der geprüften Führung eines Informationssicherheits-Management-Systems nach ISO 27001:2022[3] – der Schweizerischen Post sind nicht öffentlich bekannt, jedoch ist es wahrscheinlich, dass ein unbemerkter Diebstahl oder eine unbemerkte Zerstörung durch Externe erfolgen könnten. Wahrscheinlich hätte ein interner Angreifer höhere Chancen, den Angriff erfolgreich umzusetzen. Ferner wird das Risiko für B6 und B7 minimiert, indem durch einen Hinweis auf dem Stimmrechtsausweis auf die Konsequenzen einer missbräuchlichen Stimmabgabe hingewiesen wird: “Die unbefugte oder mehrmalige Teilnahme an einer Wahl oder Abstimmung ist als Wahlfälschung strafbar (Art. 282 StGB)”.

[3] https://www.post.ch/de/ueber-uns/verantwortung/zertifikate#iso-27001

Für die Zustellungen von Wahl- und Abstimmungsmaterialien ist der zeitliche Rahmen gesetzlich geregelt (Siehe existierende Massnahmen zu B3, B4 und B5). Dieses ermöglicht eine potenzielle Erkennung eines grossangelegten Angriffs. Es muss jedoch betont werden, dass eine Trennung von missbräuchlich verwendeten Stimmrechtsausweisen von korrekt verwendeten Stimmrechtsausweisen nicht direkt möglich ist (siehe Bedrohung B1), obwohl bei erkannten Unregelmässigkeiten die leitende Behörde verpflichtet ist, die notwendigen Massnahmen anzuordnen[4].

Bedrohungen B8 und B9: Während die Bedrohung B8 den Diebstahl der Abstimmungsunterlagen nach dem Versand an die Wähler betrifft (beispielsweise aus einem Briefkasten), beschreibt die Bedrohung B9 die Zerstörung dieses Materials. Diese Bedrohungen sind weitgehend mit den Bedrohungen B6 und B7 vergleichbar, jedoch weichen aus Sicht eines potenziellen Angreifers in zwei Details ab: Zunächst ist der Aufwand für einen internen Angreifer (bspw. einer Mitarbeiterin oder einem Mitarbeiter der Schweizerischen Post) als höher zu bewerten, da an dieser Stelle das Abstimmungsmaterial bereits deutlich stärker dezentralisiert ist, sich die Wahl- und Abstimmungsunterlagen jedoch bereits in den entsprechenden Haushalten befinden. Andererseits entfallen jedoch allfällige Prozesskontrollen, die in der Logistik der Schweizerischen Post standardmässig vorzufinden sind (beispielsweise per Videoüberwachung oder Geo-Lokalisierung der Mitarbeitenden). Die Auswirkungen dieser beiden Bedrohungen sind damit mit den Bedrohungen B6 und B7 vergleichbar.

Existierende oder geplante Gegenmassnahmen gegen B8 und B9: Diese beiden Bedrohungen sind von den individuellen Gegebenheiten der Briefkästen der Stimmberechtigten abhängig. Daher existieren keine speziellen Gegenmassnahmen, auch sind solche bis anhin nicht geplant oder könnten nicht umgesetzt werden. Auch ist festzuhalten, dass ein solcher Angriff schwierig zu skalieren ist, da der physische Zugriff zu verschiedenen Briefkästen notwendig wäre. Weiterhin helfen wiederum die bereits oben erwähnten Gegenmassnahmen, welche einen zeitlichen Puffer zwischen Zustellung und Verwendung der Unterlagen vorsehen und die Warnung bezüglich des Missbrauchs auf dem Stimmrechtsausweis beinhalten.

2.4 Stimmabgabe

Die Phase der "Stimmabgabe" umfasst die dritte Phase des Abstimmungsprozesses (vgl. Abb. 3) und behandelt primär die alternativen Möglichkeiten der Stimmabgabe durch die Stimmberechtigten.

2.4.1 Prozessbeschreibung

Es gibt drei formal zulässige Alternativen, wie eine Stimme abgegeben werden kann. Am häufigsten wird das Abstimmungscouvert via der Schweizerischen Post zurück an die Gemeinde gesandt. Alternativ können Stimmberechtigte die Abstimmungscouverts auch direkt in den teilweise speziell bezeichneten Gemeindebriefkasten einwerfen. Und schliesslich besteht als dritte Option die Möglichkeit der persönlichen Stimmabgabe an der Urne, typischerweise nur während eines bestimmten Zeitfensters am Sonntag des Urnengangs.

[4] https://www.gesetzessammlung.sg.ch/app/de/texts_of_law/125.3/versions/2500

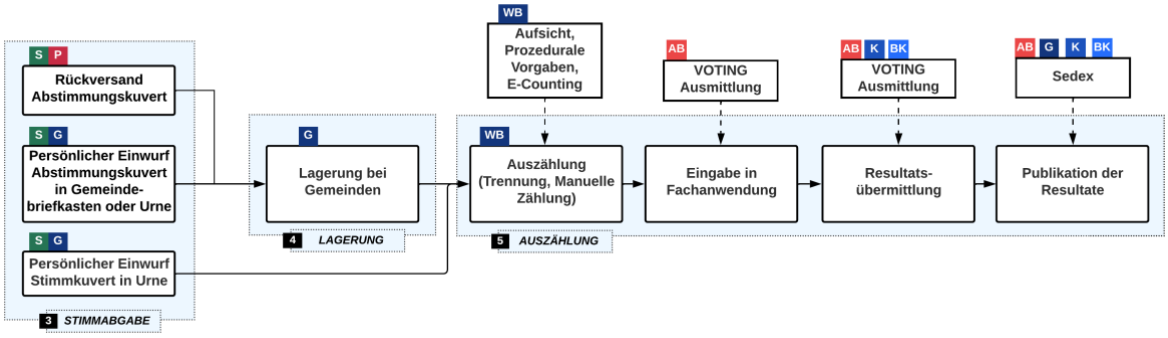

Abbildung 3: Stimmabgabe, Lagerung und Auszählung

2.4.2 Bedrohungen & Gegenmassnahmen

ID	Beschreibung	Schadensausmass
B10	Diebstahl oder Zerstörung von Abstimmungsmaterial aus Gemeindebriefkasten	MITTEL
B11	Überlastung der postalischen Services durch ‘Flooding’ von Briefpost	NIEDRIG
B12	Überlastung der postalischen Services durch Cyberangriffe auf die Informationssysteme der Schweizerischen Post	MITTEL
B13	Überlastung der Briefverarbeitung beim Empfänger (Wahllokal, Gemeinde) durch Abgabe oder Versand von gefälschtem Abstimmungsmaterial	NIEDRIG
B14	Abgabe von gefälschtem Abstimmungsmaterial	HOCH

Bedrohung B10: Die Bedrohung B10 beschreibt das Szenario, in welchem Abstimmungscouverts aus dem Gemeindebriefkasten entwendet und/oder zerstört werden. Dieser Angriff könnte relativ einfach umgesetzt werden, da lediglich der physische Zugriff zu einem Briefkasten erlangt werden muss, jedoch ist dieser Angriff schnell erkannt (typischerweise durch Einbruchsspuren). Allerdings kann das nächtliche "Fischen" von Couverts aus einem Briefkasten ohne externe Sicherheitsmassnahmen am oder um den Briefkasten herum nicht ausgeschlossen werden. Die entsprechenden Auswirkungen halten sich sehr wahrscheinlich dennoch im kleinen Rahmen, da eine Skalierbarkeit des Angriffs durch die physische Dezentralisierung der Gemeinden erschwert wird und es als unwahrscheinlich angesehen wird, dass sehr viele Couverts gleichzeitig im Gemeindebriefkasten enthalten sind (u.a. durch ein tägliches Leeren erreichbar). Da das unbemerkte Verändern (hier im Sinne der Zerstörung) einer eher kleineren Anzahl von Stimmen in diesem Fall schon den gravierendsten Fall darstellen, wird das Schadensausmass als “mittel” bewertet.

Existierende und geplante Gegenmassnahmen für B10: Da jede Gemeinde selbst für die Sicherheit der Gemeindebriefkästen zuständig ist, lässt sich keine allgemeingültige Aussage über geplante oder existierende Gegenmassnahmen formulieren. Eine verstärkte Sicherung der physischen Infrastruktur (bspw. durch das Anbringen eines Entnahmeschutzes, eines tieferliegenden Faches für die eingeworfenen Couverts oder durch eine Überwachung) erhöht die Sicherheit, allerdings ist es schwierig, den Einwurf von brennbarem Material in einen Gemeindebriefkasten grundsätzlich zu verhindern.

Bedrohungen B11, B12 und B13: Angriffsszenarien, die eine Sabotage der Diensterbringung ("Denial-of-Service") des Postzustelldienstes anstreben, werden in den Bedrohungen B11, B12 und B13 beschrieben. Das Ziel eines solchen Angriffs ist es stets, eine Verzögerung der Diensterbringung oder gar einen Ausfall dieses Prozessschrittes zu erwirken. Diese Bedrohungen sind für die sichere Durchführung der Wahlen und Abstimmungen von Bedeutung, da die zeitnahe Verarbeitung des abgegebenen Abstimmungsmaterials für eine erfolgreiche und vollständige Wahl oder Abstimmung als Ganzes entscheidend ist.

Bei der postalischen Stimmabgabe sind mehrere Szenarien einer Sabotage bzw. einer künstlich herbeigeführten Überlastung denkbar. So könnte ein grosses Aufkommen von brieflichen Sendungen (B11) zu einer Verzögerung in der Zustellung führen. Ähnlich könnten Angreifer die internen Kapazitäten der Schweizerischen Post AG ausspionieren und die Zustellung der per B-Post transportierten Wahlcouverts verzögern (B11). Hier könnten die Angriffe u.a. auf Ressourcen wie die involvierten Informationssysteme (B12) oder Mitarbeitende gezielt werden. Besonders wenn ein solcher Angriff im grossen Stil angewandt würde, also bspw. durch das Bestechen von Postmitarbeitenden in einem Verteilzentrum, wäre eine sofortige Erkennung eines derartigen Angriffs nicht als realistisch einzuschätzen. Schlussendlich könnte eine Überlastung auch direkt beim Empfänger erreicht werden, indem eine grosse Anzahl an Briefen eingesandt würde. Je nach

verfügbaren personellen Ressourcen könnte das Sortieren von Stimmcouverts zu einer verzögerten Stimmverarbeitung führen (B13).

Das Schadensausmass der Bedrohungen B11 und B13 wird jedoch als niedrig eingeschätzt, da ein grossangelegter Angriff grosse physische Ressourcen (zum Beispiel das Vorbereiten einer grossen Anzahl von Briefen) benötigen würde. Ferner bleibt ohne dezidierte Analyse der Infrastruktur unklar, ob ein solcher Angriff tatsächlich zu einer Verzögerung führen würde. Das Schadensausmass der Bedrohung B12 wird als “mittel” bewertet, da ein grossangelegter Angriff hypothetisch mit weniger Aufwand verbunden wäre, als wenn eine Überlastung physisch angestrebt würde. Die Verletzlichkeit der effektiv eingesetzten IT-Systemen ist schwierig im Generellen zu evaluieren und kann daher nur anhand konkreter Szenarien und einer technischen Analyse evaluiert werden. Mit der zunehmenden Professionalisierung von Cyberangriffen, wie u.a. Ransomware-Angriffen[5], wäre jedoch ein schwerwiegendes Szenario denkbar, in welchem auch von der Schweizerischen Post verwendete IT-Systeme von einem derartigen Angriff betroffen sein könnten und zu einem (teilweisen) Versagen der korrekten Zustellung von Briefen führen könnte.

Existierende und geplante Gegenmassnahmen für B11, B12 und B13: Bestehende Massnahmen gegen eine Überlastung der Infrastruktur der Schweizerischen Post, wie in B11 beschrieben, sind nicht bekannt. Da die Schweizerische Post auch im täglichen Geschäft stark fluktuierende Lasten bewältigen kann (zum Beispiel ein Anstieg der Brief- und Paketpost während der Weihnachtszeit), wird angenommen, dass die Schweizerische Post über genügend grosse Kapazitäten verfügt, um einem solchen Angriff standzuhalten.

Die Verletzlichkeit und die damit verbundenen existierenden oder geplanten Gegenmassnahmen der IT-Sicherheit (B12) der Schweizerischen Post sind ebenfalls nicht bekannt. Da mit einem Angriff primär eine Verzögerung oder der (teilweise) Ausfall der regulären Briefpost erreicht werden könnte, könnten im Ernstfall die persönliche Abgabe an der Urne als mögliche Gegenmassnahme verwendet werden.

Auch in Bezug auf die Bedrohung B13 sind keine spezifischen Gegenmassnahmen geplant, da das Schadensausmass eines erfolgreichen Angriffs als “niedrig” eingestuft wird. Im unwahrscheinlichen Fall, dass ein solcher Angriff erfolgreich ist, könnten die Gemeinden durch das Aufbieten von Helfenden, analog zum Aufgebot von Wahlhelfenden, den Angriff abschwächen oder gar vollständig abwenden.

Bedrohung B14: Bei der brieflichen oder persönlichen Stimmabgabe wird die Authentizität des Stimmrechtsausweises geprüft und anschliessend der Stimmrechtsausweis vom Rest des Abstimmungsmaterials getrennt, um das Stimmgeheimnis zu wahren. Gelingt es einem Angreifer jedoch, den physischen Stimmrechtsausweis zu fälschen, würde dieses zu einer Situation führen, in welcher Mehrfachstimmen möglich sind oder die Wahl oder Abstimmung nicht eindeutig ausgezählt werden kann (siehe Kapitel 3.5 Auszählung).

Existierende und geplante Gegenmassnahmen für B14: Die Erkennung von gefälschtem Abstimmungsmaterial wäre im Rahmen einer Plausibilitätsprüfung des Gesamtergebnisses realistisch (zum Beispiel durch die auffallend hohe Stimmbeteiligung in einer Gemeinde), eine Erkennung eines Einzelfalles ist jedoch sehr unwahrscheinlich. Um diesen Angriff auf individueller Basis erkennen zu können, ist die Einführung eines QR-Codes geplant, mit welchem sichergestellt wird, dass es sich um einen echten Stimmrechtsausweis hält. So kann mit diesem QR-Code ein direkter Stimmregisterabgleich vollzogen werden, womit die Echtheit und Validität sichergestellt wird, und Mehrfachstimmen oder gefälschte Stimmen verunmöglicht werden. Für diese Gegenmassnahme werden sowohl Prozessänderungen beim Druck von Wahlunterlagen als auch bei der Auszählung (beispielsweise über die Einführung einer Scanning-Lösung) nötig.

[5] Massnahmen gegen Ransomware-Angriffe:
https://www.newsd.admin.ch/newsd/message/attachments/90430.pdf

2.5 Lagerung in der Gemeinde

In der Schweiz verwendet der Grossteil der Abstimmenden den brieflichen Stimmkanal. Der prozentuale Anteil an Urnenstimmen nimmt stetig ab. Im Jahr 2020 wurde ermittelt, dass über 90% der Abstimmungscouverts bereits “verfrüht” in den jeweiligen Gemeinden eintreffen (d.h. sie erreichen die Gemeinde vor dem Wahltag) und damit bis zum Abstimmungstag zwischengelagert werden müssen.[6] Die vierte Phase behandelt deshalb die "Lagerung" der Abstimmungscouverts in den Gemeinden.

2.5.1 Prozessbeschreibung

Der Prozess der "Lagerung" kennt keine separierbaren Teilschritte. In der praktischen Umsetzung entstehen jedoch entscheidende Bedrohungslagen, wenn der physische Zugriff auf die gelagerten Unterlagen durch einzelne Personen möglich ist, d.h., wenn das Vieraugenprinzip nicht angewendet wird.

2.5.2 Bedrohungen & Gegenmassnahmen

ID	Beschreibung	Schadensausmass
B15	Zugriff auf gelagerte Abstimmungscouvert	HOCH
B16	Einspeisung von gefälschten Abstimmungsunterlagen	NIEDRIG

Bedrohung B15 und B16: Die Bedrohung B15 betrifft primär den Zugriff auf die zwischengelagerten Abstimmungscouverts. Je nach vorhandenen Sicherheitsmassnahmen müsste hier physische Gewalt angewandt werden, um den Zugriff auf Abstimmungscouverts zu erhalten, bspw. durch den Aufbruch eines Safes (sofern Abstimmungscouverts dort drin gelagert sind) oder eines spezifischen Raumes. Ein vollständig unbemerkter Zugriff ist somit sehr schwierig zu erreichen, ausser wenn eine bereits mit dem in der Gemeinde angewendeten Verfahren vertraute Person den Angriff ausführt (interner Angriff). Sobald ein Angreifer Zugriff auf die Abstimmungscouverts hat, müssen verschiedene Szenarien betrachtet werden: (a) der Diebstahl von Abstimmungscouverts und/oder deren Zerstörung, (b) die Manipulation von brieflichen Stimmabgaben und (c) die Einspeisung von gefälschten Stimmabgaben (gemäss Bedrohung B16). Ein interner Angreifer könnte nach der Trennung von Stimmrechtsausweisen und Stimmzettelcouverts am Abstimmungssonntag gefälschte Stimmzettel einschleusen oder austauschen. Eine forensische Analyse zur Abgrenzung und Erkennung des Angriffs wäre deutlich erschwert, da potenziell mehrere (autorisierte) Personen mit den Abstimmungscouverts und den Wahlzetteln in Kontakt waren. Eine nachträgliche Auflösung dieses Angriffs ist mit hohem Aufwand verbunden.

Existierende und geplante Gegenmassnahmen für B15 und B16: Beide Bedrohungen zielen auf die sichere Lagerung der Zustellkuverts ab, welche in den Gemeinden einen besonders kritischen Punkt im Abstimmungsprozess darstellen. Gleiches gilt im Kern auch für die Zwischenlagerung der übrigen Abstimmungsunterlagen (beispielsweise der überschüssigen Stimmzettel). Die korrekte Lagerung ist im geltenden Recht nur rudimentär reguliert (Art. 61 des Gesetzes über Wahlen und Abstimmungen [abgekürzt WAG]), und die Lagerung erfolgt je nach Gemeinde gemäss den eigens dafür verwendeten oder definierten organisatorischen Sicherheitsvorkehrungen. Beispielsweise ist in Bezug auf die physische Zugriffskontrolle kaum

[6] Domhnall O'Sullivan: "Die Schweiz wird zum Briefwahl-Paradies", Swissinfo, 06.10.2020, URL: https://www.swissinfo.ch/ger/direkte-demokratie_die-schweiz-wird-zum-briefwahl-paradies/46073018

geregelt, dass immer nur zwei Gemeindeangestellte gleichzeitig Zugang zu dem Tresor oder Raum mit den Abstimmungscouverts haben. Stattdessen wird die Überwachung typischerweise auf vertrauensvolle Einzelpersonen abgestellt. Damit sind derartige Angriffe entsprechender Einzelpersonen faktisch nicht zu verhindern und in der Regel wohl auch nicht erkennbar.

Aus praktischer Sicht ist ein derartiger Angriff auf die Lagerung schwierig auf kantonale oder gar schweizweite Abstimmungen auszuweiten, da eine grössere, gemeinsame Absprache von mehreren (einzelnen) Vertrauensträgern in verschiedenen Gemeinden gleichzeitig erfolgen müsste. Jedoch sind Eingriffe möglich und gerade bei Einzelpersonen nicht grundsätzlich auszuschliessen, was bei Wahlen und Abstimmungen von lokaler Bedeutung sein kann (vgl. mediale Berichterstattung zum "Fall Frauenfeld"). Für den Zugriff auf Wahl- oder Abstimmungsmaterial sollte das Vieraugenprinzip angewendet werden, so dass immer mehrere Vertrauensträger für einen Zugang notwendig sind.

2.6 Auszählung

Die "Auszählung" stellt die fünfte Phase des Abstimmungsprozesses dar (vgl. Abb. 3) und behandelt die Auszählung der abgegebenen Stimmen.

2.6.1 Prozessbeschreibung

Die Auszählung zählt zu den komplexesten Prozessschritten, mit insgesamt vier Hauptschritten, welche wiederum diverse Unterprozesse beinhalten. Der erste Schritt ist der Beginn der Auszählung, wobei zuerst die Zustellkuverts geöffnet und die einliegenden Stimmrechtsausweise auf ihre Gültigkeit überprüft werden. Wenn der Stimmrechtsausweis korrekt unterschrieben wurde, wird er zuerst zum “Stapel” der gültigen Stimmrechtsausweise hinzugefügt und danach das Stimmzettelcouvert zur Weiterverarbeitung getrennt zwischengelagert.

Die Details der Zählmethoden variieren je nach Kanton und Gemeinde und danach, ob es sich um eine Wahl oder Abstimmung handelt. Grundsätzlich werden im Kanton St. Gallen jedoch nach der Prüfung der Stimmrechtsausweise die Stimmzettelcouverts geöffnet und die Stimmzettel geprüft und ausgezählt. Anschliessend werden die Ergebnisse im Ergebnisermittlungssystem (aktuell "WABSTI", ab dem Frühjahr 2023 "VOTING Ausmittlung", als Neuentwicklung der Firma Abraxas) erfasst.

Nachdem der Zähl- und Erfassungsprozess in einer Gemeinde abgeschlossen ist, werden in einem dritten Schritt die Ergebnisse im Ergebnisermittlungssystem für die Plausibilisierung durch die Staatskanzlei freigegeben. Fördert diese Plausibilitätsprüfung keine Auffälligkeiten zutage, werden die Ergebnisse im letzten Schritt der Auszählung publiziert, was eine nachfolgende Überprüfung durch die Öffentlichkeit ermöglicht.

2.6.2 Bedrohungen & Gegenmassnahmen

ID	Beschreibung	Schadensausmass
B17	Manipulation der Zählung durch Insider	HOCH
B18	Manipulation oder Überlastung der Online-Infrastruktur von Ergebnisermittlungssystem	HOCH
B19	Manipulation oder Überlastung der Ergebnispublikation	MITTEL
B20	Manipulation oder Überlastung der E-Counting Software	HOCH

Bedrohung B17: Diese Bedrohung beschreibt einen Angriff von innen, wobei bei den Stimmzählung ein oder mehrere Vertrauensträger kolludieren. Eine Manipulation (vgl. mediale Berichterstattung zum “Fall Frauenfeld”) ist somit durch Personen mit erhöhten Berechtigungen (bspw. einen Stimmbüroleiter) einfacher umsetzbar. Jedoch wäre es auch denkbar, dass kleinere Gruppen von Zählenden absichtlich Wahl- oder Stimmzettel manipulieren oder als ungültig deklarieren. Weiter könnte eine Vertrauensperson mit erhöhten Berechtigungen bestochen werden, was die Erkennung dieses Angriffs schwieriger machen würde. So könnte beispielsweise die verantwortliche Person ermittelte Ergebnisse falsch im Ergebnisermittlungssystem erfassen. Die Auswirkungen durch eine direkte Manipulation begrenzen sich auf die betroffene Gemeinde, da eine lokale Manipulation bei einer schweizweiten Abstimmung höchstwahrscheinlich statistisch nicht relevant ins Gewicht fallen würde. Handelt es sich jedoch um lokale (Gemeinde-)Wahlen, können die Auswirkungen statistische Signifikanz erreichen und das Ergebnis messbar verfälschen.

Existierende und geplante Gegenmassnahmen für B17: Für diese Bedrohung erscheint der Fall zentral, wo eine einzelne Person allein Zugang zu den Abstimmungsunterlagen oder zum Ergebnisermittlungssystem hat. Ein solcher Angriff kann durch das sogenannte “Vieraugenprinzip” während der Zählung erschwert werden. Daher sollten alle kritischen Prozessschritte in Zweierteams durchgeführt werden. Im Idealfall sind solche Zweierteams zufällig bestimmt oder aus Personen mit unterschiedlichen politischen Interessen zusammengesetzt (bspw. Personen aus unterschiedlichen Parteien) und müssen entsprechende Unterlagen auch zu zweit unterschreiben. Da diese Prozesskontrollen von den Gemeinden auf freiwilliger Basis umgesetzt werden, ist nicht bekannt, wie ganzheitlich solche Kontrollen umgesetzt werden.
Neben den zuvor beschriebenen, rein prozeduralen Kontrollen kann die Sicherheit der Ergebnisermittlung durch den Einsatz von personalisierter Authentifizierung und dem Protokollieren von Operationen (Transaktions-Logs) erhöht werden. Das aktuell eingesetzte System WABSTI, in welchem eine derartige Protokollierung nicht ausreichend enthalten ist, wird von dem neuen System “VOTING Ausmittlung” abgelöst werden, welches eine solche Protokollierung personalisiert ermöglichen soll.

Neben bösartigen Manipulationen müssen bei der Ergebnisermittlung auch Fehler beim Erfassen von Wahl- und Abstimmungsergebnissen betrachtet werden. Die momentan eingesetzte Software WABSTI erlaubt eine automatische mathematische Validierung der erfassten Werte für sämtliche Arten von Geschäften. Dieses ist nicht mit der Plausibilisierung der Ergebnisse zu verwechseln, was in WABSTI nicht möglich ist, sie wird jedoch in der zukünftig eingesetzten VOTING Ausmittlung teilweise integriert. Der Quellcode dieser Software wird veröffentlicht, was helfen soll, das öffentliche Vertrauen in die neue Software zu verbessern. Die neue VOTING Ausmittlung Software wurde bereits durch die Firma Abraxas intern auf Sicherheit geprüft und wird durch die geplante Veröffentlichung einem internationalen Publikum von Sicherheitsexperten zugänglich gemacht, was beispielsweise bei dem E-Voting System der Schweizerischen Post aufschlussreiche Erkenntnisse erbrachte.

Bereits heute werden zudem alle Ergebnisse nach einer ersten Plausibilisierung durch die Staatskanzlei St. Gallen veröffentlicht. Sie können also auch durch unabhängige Beobachter jederzeit nachvollzogen und überprüft werden.

Bedrohung B18: Die Bedrohung B18 kennzeichnet einen Angriff auf den Betrieb des Ergebnisermittlungssystems (bis anhin “WABSTI” und neu “VOTING Ausmittlung”. Diese Software ist vor allem bei Wahlen ein wichtiges Werkzeug, da es im Vergleich zu einer manuellen Auszählung, effizientere Wahlauszählungen ermöglicht. Wenn die Datenbank des Ergebnisermittlungssystems manipuliert werden könnte, dann könnte ein Angreifer beispielsweise die Sitzvergabe beeinflussen. Eine Überlastung der Infrastruktur, etwa durch die oben erwähnten “Denial-of-Service"-Angriffe, könnte zudem zu Verzögerungen der Ausmittlung führen.

Existierende und geplante Gegenmassnahmen für B18: Die Erkennung eines derartigen Angriffs wird jedoch durch die (existierende) Bundkontrolle (manuelle Stichproben von

identifizierbaren “Bündeln” an Wahlzetteln) erhöht und die unerkannte Durchführung dieses Angriffs dadurch erschwert. Die Bedrohung durch “Denial-of-Service”-Angriffe kann durch operative Vorkehrungen (bspw. einen Härtetest der Software durch “Penetration Testing” oder den Einsatz von "Scrubbing-Diensten") bei Herstellung und Betrieb der Software minimiert werden. Das neu entwickelte Ergebnisermittlungssystem Software VOTING Ausmittlung wurde von der Firma Abraxas bereits mit solchen Härtetests getestet. Zudem werden alle VOTING Applikationen von einer vorgeschalteten Web Application Firewall vor verteilten “Denial-of-Service”-Angriffe geschützt. Um volumetrische Netzwerkangriffe abzuwehren, wurden Vereinbarungen mit den Internetbetreibern getroffen, welche eine solche Attacke abwenden könnten.

Bedrohung B19: Die Bedrohung B19 betrifft eine Manipulation der Ergebnisübermittlung. In einem wissenschaftlichen Papier[7] wurde dieses Szenario beschrieben und schweizweit erfasst. So ist die Übermittlung von vorläufigen Resultaten potenziell für Manipulationen anfällig. Spezifisch könnte auf Gemeindeebene die zentralisierte Ergebniserfassung oder auf kantonaler Ebene die Übertragung der Resultate über den SEDEX-Service das Ziel eines Angriffs sein. Eine Erkennung eines solchen Angriffs könnte durch Abgleiche von publizierten Resultaten und vorhandenen Protokollen in den jeweiligen Gemeinden und durch Plausibilitätsprüfungen ermöglicht werden.

Existierende und geplante Gegenmassnahmen für B19: Die Manipulation von publizierten Resultaten kann durch digital signierte Resultate erschwert werden. Im neuen Ergebnisermittlungssystem “VOTING Ausmittlung” werden ebenfalls die Protokolle elektronisch signiert. Neben dem Erreichen dieser höheren Fälschungssicherheit kann die Verfügbarkeit im Falle eines Überlastungsangriffs durch redundante Kapazitäten oder den Einsatz kommerzieller “Denial-of-Service”-Schutzdienste gesichert werden.

Bedrohung B20: Die Bedrohung B20 bezieht sich auf einen Spezialfall der Auszählung: das E-Counting (Optisches Scanning von Stimmzetteln). B20 umfasst allfällige Verfälschungen des Resultats oder Behinderungen bei der Resultatsermittlung durch eine Manipulation der eingesetzten Scan-Software. E-Counting wird aktuell in drei Gemeinden des Kantons (Stadt St. Gallen, Rapperswil-Jona und Auslandsschweizer) verwendet. Der Computer, auf dem die Scan-Software betrieben wird, könnte dabei über das Kommunikationsnetzwerk, an das er angeschlossen ist, angegriffen werden. Gleichzeitig ergibt sich bezüglich der Vertrauenswürdigkeit der ermittelten Ergebnisse eine Abhängigkeit zur Herstellerfirma. Für einen externen Angreifer wäre die Durchführung eines solchen Angriffs mit hohem Aufwand verbunden, da die Resultate grundsätzlich unabhängigen Plausibilitätsprüfungen unterzogen werden müssen (Anforderung der Bundeskanzlei[8]). Gemäss diesen Anforderungen ist die korrekte Funktionsweise anhand der erhobenen Daten zu plausibilisieren, wofür eine Stichprobe von manuell ausgezählten Stimmzetteln hinzugezogen wird. Die Kantone bestimmen die Grösse der Stichprobe, welche dann mit der digitalen Repräsentation (des E-Countings) verglichen wird.

Existierende und geplante Gegenmassnahmen B20: Die Korrektheit des E-Counting wird aktuell primär durch die Plausibilitätsprüfungen gesichert. Sind die notwendigen Parameter, wie unter anderem die Stichprobengrösse, gegeben, so gelten die Plausibilitätsprüfungen als vertrauenswürdig. Die Sicherheit dieses Prozesses könnte zusätzlich verbessert werden, indem die Sicherheit der verwendeten Computer-Systeme “gehärtet” wird. So könnte beispielsweise der Zugang zum Scan-Computer absolut beschränkt werden, indem der Rechner grundsätzlich ohne Netzzugang betrieben würde und ausschliesslich – neben dem technisch gehärteten Betriebssystem – die Scan-Software betreibt. Für das Einlesen der gezählten Resultate kann temporär ein gesicherter Netzzugang gewährt oder eine USB-Schnittstelle geöffnet werden. Es sind aktuell keine geplanten Gegenmassnahmen bekannt.

[7] David M. Sommer, Moritz Schneider, Jannik Gut, Srdjan Capkun: "Cyber-Risks in Paper Voting", https://arxiv.org/abs/1906.07532

[8] Kreisschreiben des Bundesrates an die Kantonsregierungen über die Ermittlung der Ergebnisse eidgenössischer Volksabstimmungen mit technischen Mitteln vom 30. November 2018, https://www.zh.ch/content/dam/zhweb/bilder-dokumente/themen/politik-staat/wahlen-abstimmungen/logistik/Kreisschreiben_Bundesrat_tech_Hilfsmittel.pdf

2.7 Erwahrung

Die Phase der "Erwahrung" folgt auf diejenige der Auszählung der Stimmen, daher ist eine erneute Lagerung der nun bereits ausgewerteten und gezählten Wahl- und Abstimmungsunterlagen nötig (vgl. Abb. 4). Die sichere Lagerung ist auch hier entscheidend, da eine potenzielle Nachzählung solange möglich sein muss, bis die offizielle Erwahrung durch den Bundesrat, respektive die Regierung des Kantons St. Gallen erfolgt und die Stimm- und Wahlunterlagen in der Folge vernichtet werden können.

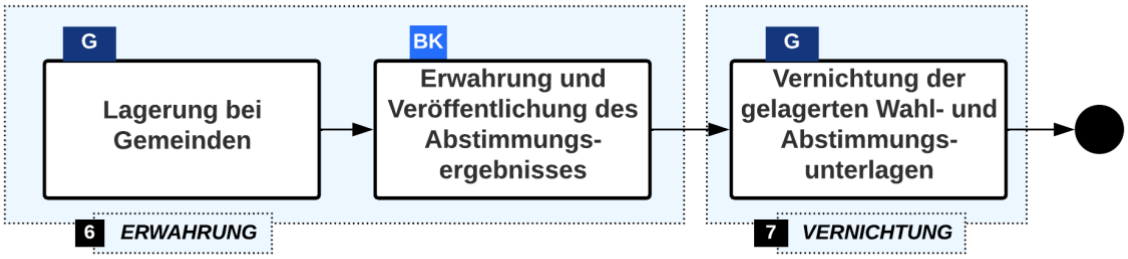

Abbildung 4: Erwahrung und Vernichtung

2.7.1 Prozessbeschreibung

Zuerst werden in der Erwahrungsphase die bereits ausgewerteten und gezählten Wahl- und Abstimmungsunterlagen sicher gelagert. Formal gilt: “Der Bundesrat stellt das Abstimmungsergebnis verbindlich fest (Erwahrung), sobald feststeht, dass beim Bundesgericht keine Abstimmungsbeschwerden eingegangen sind, oder so bald über diese entschieden worden ist.”[9] Das gleiche gilt analog für die Regierung des Kantons St. Gallen im Fall von kantonalen Wahlen und Abstimmungen.

2.7.2 Bedrohungen & Gegenmassnahmen

ID	Beschreibung	Schadensausmass
B21	Manipulation gelagerter Abstimmungsunterlagen	MITTEL
B22	Verfrühte Vernichtung durch gefälschte Erwahrungsnachricht forcieren	NIEDRIG

Bedrohung B21: Die Bedrohung B21 ähnelt der Bedrohung B15, da sich beide auf die Lagerung der Abstimmungsunterlagen und in dieser Phase ebenfalls auf die Protokolle und damit die (lokalen) Zwischenergebnisse der Auszählung beziehen. Unter der Voraussetzung, dass jemand eine Nachzählung einleiten kann, kommen höchstens kombinierte Angriffe bei dieser Bedrohung in Frage. Einerseits können so durch Zugriff auf die Abstimmungsunterlagen (a) diese entfernt und/oder zerstört werden oder (b) zusätzliche Unterlagen hinzugefügt werden (siehe Kapitel 7). In beiden Fällen ist eine exakte Nachzählung zwar möglich, das Resultat dieser Auszählung wäre jedoch bereits verfälscht. Die Lagerung der Wahl- und Stimmzettel, sowie Stimmrechtsausweise wird je nach Gemeinde sehr unterschiedlich umgesetzt (vgl. Kapitel 4.4.2). Weiterhin müssten die Gegebenheiten für eine Nachzählung zuerst festgestellt sein. Allerdings sind die Hürden für die

[9] 161.1 Bundesgesetz über die politischen Rechte (BPR) Artikel 15
https://www.fedlex.admin.ch/eli/cc/1978/688_688_688/de#art_15

Anordnung einer Nachzählung hoch (vgl. Art 13 Abs. 3 BPR sowie Art. 83 WAG) und diese dementsprechend sehr selten.

Existierende und geplante Gegenmassnahmen für B21: Analog zu den Gegenmassnahmen zu B17 sollten Prozesskontrollen wie das Vieraugenprinzip in Bezug auf den Umgang mit dem Abstimmungsmaterial berücksichtigt werden. Eine mögliche Umsetzung müsste jedoch von den einzelnen Gemeinden vollzogen werden.

Bedrohung B22: Die aufgeführte Bedrohung B22 behandelt den Fall, bei dem eine gefälschte Mitteilung (bspw. in Form einer E-Mail, einem Brief oder eines Anrufs) zu einer verfrühten Vernichtung der Abstimmungsunterlagen einer Gemeinde führen könnte. Da die Gemeinden in der Durchführung von Abstimmungen und Wahlen jedoch erfahren sind, würde eine verfrühte oder auf einem unerwarteten Weg eintreffende Aufforderung zur Vernichtung der Unterlagen sehr wahrscheinlich auffallen. Rechtlich betrachtet wäre es jedoch problematisch, wenn auch nur eine einzige Gemeinde die Unterlagen verfrüht zerstören würde, da dieser Fall bereits ausreichen würde, um eine umfassende Nachzählung zu verunmöglichen.

Existierende und geplante Gegenmassnahmen für B22: Prozedurale Kontrollen schwächen das Risiko der Bedrohung B22 ab. Zum einen ist gesetzlich vorgeschrieben, wie lange das Abstimmungsmaterial nach einem Urnengang auf jeden Fall aufbewahrt werden muss (vgl. Art. 87 WAG). Zudem ist der aktuelle Stand der Erwahrungen jederzeit über eine eigene Seite im kantonseigenen Intranet ersichtlich, was es den Gemeinden erlaubt, sich im Falle einer “zweifelhaften” Aufforderung zur Vernichtung der Abstimmungsunterlagen rückzuversichern, respektive eine solche zu verifizieren

2.8 Vernichtung

Die letzte Phase befasst sich mit der finalen Vernichtung der Wahl- und Abstimmungsunterlagen.

2.8.1 Prozessbeschreibung

Nach der Erwahrung der Ergebnisse können alle relevanten Unterlagen zu dieser Wahl bzw. Abstimmung physisch zerstört werden.

2.8.2 Bedrohungen & Gegenmassnahmen

In dieser Phase wurden keine Bedrohungen identifiziert, welche für die abgeschlossene Wahl- oder Abstimmung an sich relevant wären, weil (a) das Ergebnis der Wahl bzw. Abstimmung bereits offiziell festgestellt wurde, (b) keine Details der Stimmzettel datenschutzrechtlichen Belangen genügen müssen, sondern (c) nur die Vernichtung der Stimmrechtsausweise einen Umgang mit personenbezogenen Daten beinhaltet. Damit stellt die mögliche Privatsphärenverletzung der Stimmenden die einzige Bedrohung dar. Da Stimmrechtsausweise bereits von den Stimmzetteln getrennt sind, ist das Stimmgeheimnis jedoch auch bei einem hier möglicherweise erfolgreichen Angriff gewährleistet.

3 E-Voting

Nebst einem sicheren Betrieb der Software des E-Voting Systems selbst sowie einer sicheren Herstellung der initialen Parameter für die Stimmenden (bspw. in einer zertifizierten Druckerei für die Herstellung der Identifikationscodes), ist beim E-Voting die Sicherheit des Endgeräts, von welchem die Stimmberechtigten ihre Stimme abgeben können, von zentraler Bedeutung. Hier ist das Augenmerk im Besonderen auf die Heterogenität der Endsysteme aber auch auf die sich im Einsatz befindlichen Software-Versionen und -Systeme (beispielsweise verschiedene Betriebssysteme oder Browser für den Zugang zum E-Voting) des Betriebssystems des verwendeten Endgeräts zu richten.

Dennoch treffen im Falle des E-Votings viele Bedrohungen wie im oben geschilderten traditionellen Wahl- und Abstimmungsprozess in ähnlicher Weise zu. Potenziell könnten einige Bedrohungen einfacher zu skalieren sein (d.h. es können mehrere oder grössere Anzahlen von Stimmenden, Wahl- und Abstimmungsunterlagen oder Gemeinden unterschiedlich stark betroffen sein), da durch den Einsatz von IT-Systemen gewisse Phasen oder Schritte der Prozesse der Wahlen und Abstimmungen deutlich stärker zentralisiert sind. Ein Beispiel für diese Zentralisierung (vollständig mit dem papierbasierten Wahl- und Abstimmungsverfahren vergleichbar) ist die im E-Voting relevante Vertrauensannahme, dass eine Druckerei, welche die initialen Identifikationscodes für alle Wähler druckt, zuverlässig, sicher und typischerweise “offline”, also ohne aktiven Netzwerkzugang von aussen, zum Zeitpunkt der Code-Herstellung arbeitet.

Ein zentraler Punkt, welcher sich von den zuvor beschriebenen Prozessen unterscheidet, ist die Auszählung. Je nach Entwurf des Gesamtsystems kann im Falle des E-Votings nicht in jeder Gemeinde separat gezählt und veröffentlicht werden, sondern es wird das Sammeln und Zusammenzählen zentral in der Infrastruktur eines Dienstleistungsanbieters stattfinden müssen. Jedoch ist klar anzumerken, dass der finale Entschlüsselungsschritt der Stimmen (bspw. im Falle des E-Voting Systems der Post) nicht beim Dienstleistungsanbieter geschieht, sondern beispielsweise durch das kantonale Stimmbüro des Kantons, für welche eine speziell dafür aufgesetzte und gesicherte Maschine (Computer) eingesetzt wird.

Grundsätzlich sind sowohl die prozeduralen als auch organisatorischen und teilweise die technischen Sicherheitsvorkehrungen im E-Voting stärker zu gewichten als dieses im traditionellen brieflichen Abstimmungssystem der Fall ist. Diese liegt im Besonderen an der Tatsache, dass es beim E-Voting kritische Funktionalitäten geben muss, welche zentralisiert organisiert und betrieben werden müssen, wenn denn die ökonomischen und betrieblichen Kosten nicht die Vorteile eines E-Voting-Ansatzes absorbieren sollen. Das betrifft vor allen Dingen (a) die Herstellung der kryptographischen Parameter und Schlüssel für die Stimmenden (Identifikationscodes), (b) die Verteilung dieser Parameter und Schlüssel an die Stimmenden und (c) die zuverlässige und sichere Handhabung der kryptographischen Schlüssel zur Entschlüsselung je Kanton. Eine detaillierte Bedrohungsanalyse des E-Votings oder seiner Verfahren ist an dieser Stelle nicht möglich, da sie nur auf der Basis eines genau definierten Systems, seiner Komponenten (Hard- und Software-bezogen) und seiner Beteiligten (den Stimmenden, den Gemeinden, Kantonen, Staatskanzleien und dem Bund) sowie deren Interaktionslinien sinnvoll wäre (siehe beispielsweise “Die Analyse des E-Voting System der Schweizerischen Post”[10]).

4 Allgemeine Sicherheitsbedenken

Die voranschreitende Digitalisierung in der öffentlichen Verwaltung führt zu einer messbaren Abhängigkeit von Informationstechnologien (bspw. E-Mail-Systemen, Share Points, Cloud-basierter Datenhaltung, dem Internet und Intranet sowie den heterogenen Servern und Endgeräten). In den letzten Jahren hat sich im Besonderen die Bedrohungslandschaft für alle Informationssysteme gewandelt, weshalb im Folgenden die aktuell bedeutenden Bedrohungen für allgemeine Informationssysteme nur umrissen werden. Diese Abhandlung ersetzt keine notwendige und detaillierte Bedrohungs- und Vulnerabilitätsanalyse einer kantonalen oder gemeindespezifischen IT-Infrastruktur, soll aber anhand weniger Beispiele aufzeigen, dass relevanten Sicherheitsbedenken klar Rechnung getragen werden muss, auch und im Besonderen über IT-Systemgrenzen hinweg und unter Beachtung von Interaktionen und Interaktionsmuster aller Beteiligten.

Die Frequenz erfolgreicher Ransomware-Angriffe hat sich seit 2013 vervielfacht. In einem Ransomware-Angriff werden die Daten der angegriffenen Systeme verschlüsselt und typischerweise mit einer Lösegeldforderung (ransom) der Besitzer dieser Daten aufgefordert, eine Zahlung auszulösen, um den Schlüssel für die Entschlüsselung zu erhalten. In vielen Fällen führten

[10] SCRT SA: "Examination of the Swiss Internet voting system"Version: 1.0 / Audit scope: Infrastructure and operations (3) – Measures of the system provider 26.03.2022, Verfügbar auf: https://www.newsd.admin.ch/newsd/message/attachments/71144.pdf

diese Lösegeldforderungen jedoch nicht zum Erhalt der Schlüssel für eine Entschlüsselung der Daten. Zu Beginn der Ransomware-Angriffe wurden u.a. gezielt Krankenhäuser angegriffen[11], da diese aufgrund des grossen Zeitdrucks und der betroffenen privaten Patientendaten oft den Lösegeldforderungen nachkamen. Mittlerweile sind im Besonderen auch relativ viele kleine und mittelgrosse Unternehmen betroffen[12], ergänzt durch Behörden. Es kann damit leider aktuell nicht ausgeschlossen werden, dass kritische Informationssysteme (als auch die bereits oben genannten und heute für die existierenden Wahlen und Abstimmungen eingesetzten IT-Unterstützungen), die für Wahl- und Abstimmungsprozesse relevant sind, auch durch einen Ransomware-Angriff betroffen sein könnten. Obwohl sicherheitsrelevante Gegenmassnahmen, wie Netzwerksegmentierungen, Desaster Recovery Funktionen oder regelmässige Härte- und Sicherheitstests, nicht Teil dieser Kurzabhandlung hier sind, muss eine Umsetzung von allgemeinen Sicherheitsmassnahmen für die IT-Infrastruktur und spezieller Sicherheitsfunktionalität grundsätzlich immer erwähnt und im Betrieb gewährleistet werden.

Weitere Angriffe, wie beispielsweise das Phishing durch E-Mails oder das Social Engineering (der Versuch, persönliche Daten eines Computernutzers durch Täuschung der Identität des Anfragenden zu erhalten, oft auch über das Internet[13]), sind ebenso von praktischer Relevanz[14], und müssen dazu führen, dass Informationssysteme und Mitarbeitende vor Bedrohungen geschützt werden. Der Einsatz von veralteter Technologie kann ein weiteres, teilweise signifikantes Problem darstellen, da Sicherheitslücken ohne Software-Aktualisierungen (seltener Hardware-Aktualisierungen betreffend) weiterhin bestehen bleiben und somit die potenzielle Angriffsfläche messbar erhöhen, anstatt diese zu minimieren.

Schliesslich wird bei den erwähnten DDoS-Angriffen (Distributed Denial-of-Service) versucht, die Verfügbarkeit eines produktiven IT-Systems mittels Überflutung von scheinbar legitimen Anfragen von hunderten, wenn nicht gar tausenden von verschiedenen, böswilligen Systemen so zu beeinträchtigen, dass die tatsächlich korrekten Anfragen bzw. Aufträge nicht mehr beantwortet werden können, weil sie in der Datenflut untergehen oder aber nicht mehr als real und legitim klassifiziert werden können. Da eine Vielzahl von potenziell kompromittierten Geräten für derartige Angriffe verwendet werden kann, ist die Erkennung eines DDoS-Angriffs und eine Verteidigung dagegen alles andere als trivial. In der Praxis werden heutzutage häufig kommerzielle Services verwendet, welche über hohe Kapazitäten zur Bereinigung von Netzwerkverkehr verfügen und damit zeitlich relativ schnell legitimen von illegitimem Verkehr zu trennen versuchen. Da es im europäischen Raum je nach Grösse des Angriffs bis anhin keine relevanten Anbieter für geeignete Verteidigungsdienste gibt, könnte sich durch deren Nutzung eine Abhängigkeit ergeben, welche im Rahmen eines Dienstes, bspw. eines Wahl- und Abstimmungssystems, welches im und für den öffentlichen Sektor betrieben wird, als problematisch anzusehen ist[15].

Nebst den digitalen Angriffsvektoren sind und blieben physische Sicherheitsbedenken von zentraler Bedeutung. Die Sicherheit in Lagerung und Transport von Unterlagen, insbesondere der Stimmrechtsausweise, sind für den gesamten Abstimmungsprozess essenziell. Wie der Fall Frauenfeld (vgl. Kapitel 7) exemplarisch zeigt, ist der Zugriff auf die gelagerten Unterlagen verschiedener Natur nicht nur nicht zu vernachlässigen, sondern benötigt umgehend umfassende, aber ökonomisch ausgewogene Sicherheitsmassnahmen und Zugriffskontrollen.

5 Fazit: Diskussion und Gegenmassnahmen

Die oben ausgeführte Analyse der Bedrohungsszenarien im papierbasierten Wahl- und Abstimmungsprozess haben aufgezeigt, dass es sowohl einige messbare Bedrohungen als auch teilweise Gegenmassnahmen gibt. Dennoch ist es wichtig, für Gegenmassnahmen eine

[11] Swiss Government Computer Emergency Response Team, Cyber Security for the Healthcare Sector During Covid19 https://www.govcert.ch/blog/cyber-security-for-the-healthcare-sector-during-covid19/
[12] Swiss Government Computer Emergency Response Team, Severe Ransomware Attacks Against Swiss SMEs https://www.govcert.ch/blog/severe-ransomware-attacks-against-swiss-smes/
[13] https://de.pons.com/%C3%BCbersetzung/englisch-deutsch/social+engineering#dict
[14] Swiss Government Computer Emergency Response Team, Phishing Statistics https://www.govcert.admin.ch/statistics/phishing/
[15] https://www.concordia-h2020.eu/wp-content/uploads/2021/10/roadmaps-04-Reseach-and-Innovation.pdf

aufwandsbezogene Position einzunehmen, die aus ökonomischer Sicht Abwägungen vornimmt, welche Bedrohungen als wesentlich und welche anderen Bedrohungen als sekundär angesehen werden. Dieses ist schon rein aus praktischer Sicht relevant, weil kein System hundertprozentige Sicherheit und Vertrauenswürdigkeit bieten kann, und deswegen diese Güterabwägung vornehmen muss.

Damit erscheinen aus einer risikobasierten Perspektive zwei Bedrohungsgruppen des Wahl- und Abstimmungsprozesses als zentral: Herstellung des Abstimmungsmaterials und Auszählung der Stimmen. Der Fokus auf diese beiden Bedrohungsgruppen ergibt sich hier aus der eingeschätzten Risikosensitivität und Verletzlichkeit der betrachteten Prozesse. Damit erscheinen die Manipulationssicherheit der Stimmrechtsausweise vor der Stimmabgabe und die Manipulationssicherheit gelagerter Stimmen als zentrale Zielvorgabe.

Demnach kommen den diskutierten Gegenmassnahmen, welche im Besonderen in den Kapiteln bezüglich der Bedrohungen B1, B2 und B14 sowie B15, B17 und B18 hervorgehoben werden, grosse Bedeutung zu. In diesem Sinne muss für die dort erwähnten und teilweise bereits geplanten Massnahmen eine klare Empfehlung mit hoher Priorisierung ausgesprochen werden.

Aus der Gesamtsicht, welche den allgemeinen Umgang mit Risiken in Betracht zieht, zeigt sich, dass an verschiedenen Stellen die Verantwortlichen für die Relevanz von Sicherheitsfragen innerhalb ihres Zuständigkeitsbereichs sensibilisiert sind; aber es ist wesentlich, dass das Vieraugenprinzip im Umgang mit sensitivem Material, gerade in Bezug auf die Zwischenlagerung, die Lagerung und die Behandlung des Papiers, auch Einzug in die notwendigen Empfehlungen, wenn nicht gar neue Ausführungsbestimmungen findet. Diese Empfehlungen lassen sich relativ einfach, auch ohne IT-Systeme, aber mit hoher Priorisierung umsetzen.

Aufgrund des föderalen Systems der Schweiz gibt es jedoch kein ganzheitliches Risiko- und Informationssicherheits-Management, welches eine vollständige Übersicht über die technischen, prozessrelevanten oder organisatorischen Bedrohungen (inklusive deren Wahrscheinlichkeiten und potenzieller Schadenswirkungen) umfasst. Damit ist die Verletzlichkeit der betroffenen Systeme oder der behandelten Prozesse bis auf die Gemeindeebenen hinein nicht eindeutig erkennbar. So sind beispielsweise die Kontrollprozesse, wie in den einzelnen Gemeinden Stimmen gelagert werden, nicht vereinheitlicht und werden nicht regelmässig anhand einer übergreifenden Vorgabe geprüft. Auch wenn durch die in der Vergangenheit häufig eingesetzten Freiwilligen in Wahlen und Abstimmungen und deren äusserst zuverlässigen Arbeitsweise erkennbar ist, auch wenn weiterhin Gemeinden in diesem föderalen System wie gehabt anhand ihrer Zuständigkeiten operieren, könnte ein ganzheitliches Risiko- und Informationssicherheits-Management, welches über alle Gemeinden und Drittanbieter hinweg Risiken und Schwachstellen regelmässig auf der Basis von detailliert auszuarbeitenden Empfehlungen prüft, im organisatorischem Prozess zu einer messbaren Bedrohungsminimierung führen und dazu beitragen, dass das Vertrauen in die Sicherheit von Wahlen und Abstimmungen auch in Zukunft gewährleistet ist.

6 Anhang

Glossar

Das folgende Glossar enthält diejenigen Begrifflichkeiten, welche in der Bedrohungsanalyse häufiger verwendet werden und nicht notwendigerweise im täglichen Sprachgebrauch zu finden sind.

- **Abraxas Informatik AG (kurz "Firma Abraxas"):** Systemdienstleister, u.a. verantwortlich für den Druck und die Verpackung der Wahl- und Abstimmungsunterlagen, sowie den Betrieb der Software “VOTING Ausmittlung”.
- **Aufwand**: betrifft den effektiven Aufwand – der sich typischerweise in Hinblick auf die anfallenden Kosten beziffern lässt – im Kontext eines grossangelegten Angriffes auf den Wahl- oder Abstimmungsprozess und kann in verschiedenen untergeordneten technischen Metriken gemessen bzw. bestimmt werden.
- **Auswirkung**: beschreibt den potenziellen Schaden auf die angegriffene Wahl oder Abstimmung.
- **Denial-of-Service**: Ein Angriff, der bei einer erzwungenen Überlastung des einlaufenden Netzwerkverkehrs bzw. der Anfragen an ein IT-System zu einer Nichterbringung des produktiv offerierten Dienstes führt. Hierbei sind auch Distributed Denial-of-Service Angriffe relevant, da diese durch eine grosse Anzahl von infizierten Geräten “verteilt” ausgeführt werden, was die Identifizierung und Unterscheidung von legitimen Netzwerkteilnehmern und Angreifern erschwert.
- **Erkennung**: Unter der Erkennung wird der organisatorische und technische Aufwand beschrieben, welcher nötig ist, um einen Angriff zu solchen vom Normalbetrieb zu unterschieden und damit zu identifizieren.
- **E-Counting:** Die Möglichkeit der elektronischen oder elektronisch unterstützen Stimmauszählung von papierbasierten Stimmzetteln im Wahllokal
- **E-Voting:** Die Möglichkeit der elektronischen Stimmabgabe, typischerweise über das Internet.
- **Kaiser Data AG**: Anbieter der E-Counting Lösung
- **Penetration Testing (sicherheitstechnischer Härtetest):** Beschreibt umfassende Sicherheitstests von Systemen und Computernetzwerken jeglicher Grösse. Während eines Härtetests wird die Prüfung der Sicherheit möglichst aller Systembestandteile und Anwendungen eines Netzwerks oder der beteiligten Softwaresysteme mit Mitteln und Methoden, die ein Angreifer verwenden würde oder könnte, getestet.
- **Red Teaming:** beschreibt eine vollumfängliche Angriffssimulation, mit dem Ziel Schwachstellen und Sicherheitslücken in kritischen Systemen zu identifizieren. Red Teaming geht über klassisches Penetration Testing hinaus, da auch menschliche Faktoren inkludiert werden.
- **Scrubbing-Dienst**: Dienstleistung welche Netzwerkverkehr säubert und lediglich den gutartigen an den Betreiber des IT-Service weiterleitet.
- **Skalierbarkeit:** Die Skalierbarkeit beschreibt die Einfachheit einer Grössenveränderung, mit welcher beispielsweise ein Angriff ohne grossen Aufwand auf mehrere, viele Ziele ausgeweitet werden kann. Zum Beispiel wurde beschrieben, dass es möglich ist, ein Stimmcouvert (im Zustellungsprozess oder im Gemeindebriefkasten) zu entwenden, um damit abzustimmen bzw. die Stimmzettel zu manipulieren. Ein solcher Angriff lässt sich im Falle einer einzelnen Stimme relativ einfach anwenden. Deren Skalierbarkeit ist jedoch erschwert, da es recht schwierig (wenn nicht gar unmöglich) ist, diesen Angriff im grossen Stil, beispielsweise auf 20% aller möglichen Stimmen anzuwenden.
- **VOTING Ausmittlung**: Web-basierte Software der Firma Abraxas, die bei der Auszählung und Ausmittlung während Wahlen und Abstimmungen Verwendung findet.
- **Die Schweizerische Post AG:** In staatlichem Besitz befindliche Aktiengesellschaft, zur Beförderung von Briefen und Paketen, sie besitzt offiziell das staatliche Monopol über den Briefversand bis 50 Gramm.