Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundeskanzlei BK

Sektion Politische Rechte

28. Juli 2023

Risikobeurteilung Vote électronique der Bundeskanzlei 2023

Management Summary

Im Rahmen der Neuausrichtung des Versuchsbetriebs erstellt neu jeder Akteur eine eigene Risikobeurteilung, mit der die mit der elektronischen Stimmabgabe verbundenen Risiken in seinem Zuständigkeitsbereich abgedeckt werden (vgl. Massnahme B.5 des Massnahmenkatalogs im Schlussbericht des Steuerungsausschusses Vote électronique vom 30. November 2020 zur Neuausrichtung und Wiederaufnahme der Versuche).[1] Mit den Risikobeurteilungen sollen die Risiken auf einem akzeptablen Niveau gehalten werden. Ausserdem dienen sie der Bundeskanzlei (BK) als Basis für die Beurteilung der Zulassungsgesuche, die von den Kantonen im Hinblick auf den Einsatz eines E-Voting-Systems bei eidgenössischen Urnengängen eingereicht werden. Im Sinne der Transparenz veröffentlicht die BK ihre Risikobeurteilung sowie das Prozessdokument, nach dem sich diese richtet.[2]

Werden keine Schutzmassnahmen ergriffen, wären die Risiken eines Einsatzes des elektronischen Stimmkanals für politische Entscheide hoch. Deshalb bildet die BK in der vorliegenden Risikobeurteilung zuerst die Situation ab, wie sie sich vor dem Ergreifen von Massnahmen präsentiert. Damit können in einem ersten Schritt die Risiken mit hoher Priorität identifiziert werden. Anschliessend wendet die BK die bereits umgesetzten rechtlichen, finanziellen, sozialen, wissenschaftlichen und organisatorischen Massnahmen auf die Risiken an, um einen aktuellen Überblick der effektiv bestehenden Risiken zu erhalten. Dabei berücksichtigt die BK auch den aktuellen Wissensstand in den Bereichen Politik, Verwaltung, Sicherheit und Technik. Die daraus resultierende Schlussfolgerung wird in der folgenden Übersicht der Restrisiken dargestellt. Diese zeigt auf, dass die grosse Mehrheit der Risiken derzeit als ausreichend gering beurteilt wird (grüne Bereiche in der Übersicht). Die Entwicklung aller Risiken muss weiterhin beobachtet werden. Es verbleiben insgesamt fünf Risiken (R2, R8, R11, R13 und R14), die gemäss den im Risikomanagementprozess Vote électronique der BK definierten Kriterien zum Umgang mit Risiken besonders beobachtet werden müssen. Die Risiken R3 und R5, die sich auf die Akzeptanz von E-Voting bzw. die Verfügbarkeit einer anonymen Plattform für den Stimmenkauf beziehen, können zwar gemäss den für den Umgang mit Risiken definierten Kriterien als akzeptabel eingestuft werden, jedoch bedürfen auch diese Risiken einer besonderen Aufmerksamkeit.

Zusätzlich zu den bereits ergriffenen Massnahmen haben die BK und die Kantone einen Massnahmenkatalog beschlossen, mit denen die Risiken weiter reduziert werden können.[2]

[1] www.bk.admin.ch > Politische Rechte > E-Voting > Berichte und Studien.

[2] www.bk.admin.ch > Politische Rechte > E-Voting > Versuche mit E-Voting.

Wahrscheinlichkeit	Auswirkungen (Risiko-Score) 32 – 49 (Hoch)	22 – 31 (Mittel)	17 – 21 (Tief)
Hoch			**R8** Systemausfall infolge Angriff durch einen politisch motivierten Akteur mit hohen Ressourcen
Mittel			**R4** Negativkampagne gegen E-Voting in (sozialen) Medien **R5** Stimmenkauf über anonyme Plattform **R7** Verletzung Stimmgeheimnis durch einen politisch motivierten Akteur mit hohen Ressourcen
Tief	**R2** Mangelnde Erkennung systematischer Fehler **R11** Einsatz eines nicht zugelassenen Systems **R13** Mangel an unabhängigen Expertinnen und Experten **R14** Neue Technologien führen zu Verletzung Stimmgeheimnis	**R3** Mangelnde Akzeptanz von E-Voting **R6** Manipulation der Stimmen durch einen politisch motivierten Akteur mit hohen Ressourcen **R9** Unzulängliche Anforderungen **R10** Zulassung eines mangelhaften Systems **R15** Systemausfall während Urnengang **R16** Wegfall Stimmkanal wegen unzureichender Zusammenarbeit **R17** Wegfall Stimmkanal wegen fehlender Ressourcen **R18** Überschreitung der Limiten im Bundesrecht	**R1** Erheblicher Sicherheitsmangel im System **R12** Gefährdung Weiterentwicklung Sicherheitsanforderungen

Tabelle 1: Übersicht der Restrisiken, die nach der Umsetzung von Minimierungsmassnahmen verbleiben.

Inhaltsverzeichnis

1 Anwendungsbereich und Zielsetzung

Das vorliegende Dokument wird von der Bundeskanzlei (BK) in Übereinstimmung mit der Massnahme B.5 des Massnahmenkatalogs des Schlussberichts des Steuerungsausschusses Vote électronique (SA VE) vom 30. November 2020 zur Neuausrichtung und Wiederaufnahme der Versuche erstellt.[3] Die Risikobeurteilung richtet sich nach dem Risikomanagementprozess Vote électronique der BK.[4] Sie bildet die Sichtweise der BK auf die mit Vote électronique in Zusammenhang stehenden Risiken ab, die in ihrem Zuständigkeitsbereich liegen. Die Risikobeurteilungen der Kantone, die Versuche mit der elektronischen Stimmabgabe durchführen, werden bei der Risikobeurteilung der BK berücksichtigt. Sie orientiert sich auch nach dem Leitfaden der BK für Risikobeurteilungen,[5] indem eine ähnliche Methode zur Identifizierung, Analyse und Evaluation der Risiken angewendet und ein Teil der im Leitfaden erwähnten Risiken in den Bereichen Politik und Verwaltung behandelt werden, wie es im Leitfaden der BK vorgesehen ist.

Die vorliegende Risikobeurteilung trägt nicht nur zur Erreichung der Ziele des Risikomanagementprozesses Vote électronique der BK bei, sondern dient auch der Beurteilung der Zulassungsgesuche, die von den Kantonen im Hinblick auf den Einsatz eines E-Voting-Systems bei einem eidgenössischen Urnengang eingereicht werden.

2 Identifizierung der Risiken

Basierend auf den im Risikomanagementprozess Vote électronique der BK definierten Ressourcen wurden die folgenden Risiken identifiziert. Einige Risiken stammen aus dem Leitfaden für Risikobeurteilungen der BK. Der Verweis auf den Leitfaden wird in der Spalte «Referenz» angegeben.

ID	Beschreibung	Ressourcen	Referenz
BK-VE-R1	Ein erheblicher Sicherheitsmangel, der das System betrifft, wird während eines Urnengangs entdeckt.	Ergebnisse eidg. Urnengänge Vertrauen der Stimmberechtigten Vertrauenswürdiger Urnengang mit elektronischer Stimmabgabe	
BK-VE-R2	In mehreren Kantonen werden falsch angezeigte Prüfcodes gemeldet, aber aufgrund einer fehlenden Koordination zwischen den Kantonen und der BK erfolgt auf nationaler Ebene keine Alarmierung.	Ergebnisse eidg. Urnengänge Vertrauenswürdiger Urnengang mit elektronischer Stimmabgabe	RPA-10
BK-VE-R3	Der elektronische Stimmkanal wird nicht ausreichend akzeptiert.	Vertrauen der Stimmberechtigten	
BK-VE-R4	In den Medien oder in sozialen Netzwerken wird eine Kampagne gegen den elektronischen Stimmkanal geführt. Diese kann auf Ereignissen rund um die elektronische Stimmabgabe im Ausland, auf angeblich fehlenden öffentlichen Kontrollmöglichkeiten, auf falschen Behauptungen über die Verifizierbarkeit oder auf einer mangelhaften Kommunikation der Behörden beruhen.	Vertrauen der Stimmberechtigten	RPA-6
BK-VE-R5	Eine Gruppe, die über eine anonyme Kaufplattform verfügt, lanciert eine grossangelegte Kampagne zum Stimmenkauf.	Vertrauen der Stimmberechtigten Vertrauenswürdiger Urnengang mit elektronischer Stimmabgabe	RPA-9

[3] www.bk.admin.ch > Politische Rechte > E-Voting > Berichte und Studien.

[4] www.bk.admin.ch > Politische Rechte > E-Voting > Versuche mit E-Voting.

[5] www.bk.admin.ch > Politische Rechte > E-Voting > Bundesrechtliche Anforderungen.

ID	Beschreibung	Ressourcen	Referenz
BK-VE-R6	Ein politisch motivierter Akteur mit hohen Ressourcen * mobilisiert seine Ressourcen und es gelingt ihm, Stimmen im System zu manipulieren.	Ergebnisse eidg. Urnengänge Vertrauen der Stimmberechtigten Vertrauenswürdiger Urnengang mit elektronischer Stimmabgabe	
BK-VE-R7	Ein politisch motivierter Akteur mit hohen Ressourcen * mobilisiert seine Ressourcen und es gelingt ihm, das Stimmgeheimnis zu brechen.	Vertrauen der Stimmberechtigten Vertrauenswürdiger Urnengang mit elektronischer Stimmabgabe	
BK-VE-R8	Ein politisch motivierter Akteur mit hohen Ressourcen * mobilisiert seine Ressourcen und es gelingt ihm, das Ergebnis des Urnengangs zu beeinflussen, indem Stimmberechtigte von der Stimmabgabe abgehalten werden.	Ergebnisse eidg. Urnengänge Vertrauen der Stimmberechtigten Vertrauenswürdiger Urnengang mit elektronischer Stimmabgabe	
BK-VE-R9	Die bundesrechtlichen Anforderungen sind unzulänglich und das gewünschte Sicherheitsniveau kann damit nicht aufrechterhalten werden.	VPR und VEleS	
BK-VE-R10	Der Bund hat ein System zugelassen, das die bundesrechtlichen Sicherheitsanforderungen nicht erfüllt.	Ergebnisse eidg. Urnengänge Vertrauen der Stimmberechtigten Vertrauenswürdiger Urnengang mit elektronischer Stimmabgabe	RPA-2
BK-VE-R11	Es wird ein System eingesetzt, das nicht dem zugelassenen System entspricht.	Ergebnisse eidg. Urnengänge Vertrauen der Stimmberechtigten Vertrauenswürdiger Urnengang mit elektronischer Stimmabgabe	
BK-VE-R12	Ein fehlendes Interesse von Expertinnen und Experten im Bereich von Vote électronique führt dazu, dass die Sicherheitsanforderungen nicht weiterentwickelt werden und sie nicht mehr den aktuellen Kenntnisstand abbilden.	Unabhängige und kompetente Expertinnen und Experten	
BK-VE-R13	Für die Durchführung von Überprüfungen mangelt es an qualifizierten unabhängigen Expertinnen und Experten.	Unabhängige und kompetente Expertinnen und Experten	
BK-VE-R14	Eine neue Technologie verbreitet sich und führt dazu, dass die Sicherheitsanforderungen für die Wahrung des Stimmgeheimnisses nicht mehr ausreichen (z.B. Quantencomputer).	Vertrauen der Stimmberechtigten VPR und VEleS Vertrauenswürdiger Urnengang mit elektronischer Stimmabgabe	
BK-VE-R15	Der Systemanbieter ist während eines Urnengangs nicht mehr in der Lage, sein System zur Verfügung zu stellen, obwohl bereits Stimmen abgegeben wurden.	Ergebnisse eidg. Urnengänge Systemanbieter Vertrauenswürdiger Urnengang mit elektronischer Stimmabgabe	

ID	Beschreibung	Ressourcen	Referenz
BK-VE-R16	Streitigkeiten zwischen den Behörden und der Post stören die Zusammenarbeit derart stark, dass der elektronische Stimmkanal nicht mehr weiterentwickelt werden kann oder unterbrochen werden muss.	Kantone mit E-Voting-Versuchen Systemanbieter	RPA-3
BK-VE-R17	Den Kantonen fehlen die Ressourcen für die Umsetzung des elektronischen Stimmkanals.	Kantone mit E-Voting-Versuchen	RPA-8
BK-VE-R18	Die tatsächliche Nutzung des elektronischen Stimmkanals übersteigt die Limitierung des zugelassenen Elektorats (30 % kantonal und 10 % national).	Vertrauen der Stimmberechtigten Kantone mit E-Voting-Versuchen Vertrauenswürdiger Urnengang mit elektronischer Stimmabgabe	

Tabelle 2: Risikokatalog.

* Es wird angenommen, dass es sich bei politisch motivierten Akteuren mit hohen Ressourcen um diejenigen Angreifer handelt, die über das höchste Mass an Mitteln und Kenntnissen verfügen. Deshalb werden hier keine Risiken abgebildet, die von anderen Kategorien von Angreifern ausgehen. Solche Angriffe würden im Vergleich zu den Massnahmen, die zur Abwehr von Angriffen von politisch motivierten Akteuren mit hohen Ressourcen ergriffen werden, keine zusätzlichen Massnahmen erfordern. Mögliche Angriffe wie etwa interne Angriffe durch Angestellte des Systemanbieters oder des Kantons oder ein direkter Angriff auf die Plattform der stimmenden Person sind durch die hier aufgeführten Risiken abgedeckt.

3 Für die Risikobeurteilung relevante Ereignisse und Erkenntnisse

3.1 Politik und Regulierung

3.1.1 Verzicht auf die Überführung in den ordentlichen Betrieb

An seiner Sitzung vom 26. Juni 2019 hat der Bundesrat entschieden, vorläufig auf die Überführung der elektronischen Stimmabgabe in den ordentlichen Betrieb zu verzichten. In der Vernehmlassung zur damals geplanten Änderung des Bundesgesetzes über die politischen Rechte hatte sich die Mehrheit der Teilnehmenden zwar grundsätzlich für E-Voting ausgesprochen. Den Übergang in den ordentlichen Betrieb erachteten aber insbesondere die meisten Parteien als verfrüht.

3.1.2 Neuausrichtung des Versuchsbetriebs

Der Bundesrat hat die BK am 26. Juni 2019 beauftragt, gemeinsam mit den Kantonen eine Neuausrichtung des Versuchsbetriebs mit der elektronischen Stimmabgabe zu konzipieren. Ziel der Neuausrichtung ist ein stabiler Versuchsbetrieb mit vollständig verifizierbaren E-Voting-Systemen. Die Neuausrichtung des Versuchsbetriebs orientiert sich an den folgenden Zielen:

- Weiterentwicklung der Systeme
- Wirksame Kontrolle und Aufsicht
- Stärkung der Transparenz und des Vertrauens
- Stärkere Vernetzung mit der Wissenschaft

Die BK und die Kantone haben einen gemeinsamen Schlussbericht zur Neuausrichtung und Wiederaufnahme der Versuche erarbeitet. Dazu haben sie einen breiten Dialog mit Expertinnen und Experten aus der Wissenschaft und Industrie geführt und anschliessend den Schlussbericht mit einem Massnahmenkatalog erarbeitet. Der Massnahmenkatalog sieht eine Etappierung der Massnahmen mit Blick auf die Wiederaufnahme der Versuche vor.

Der Bundesrat hat den Schlussbericht des SA VE am 18. Dezember 2020 zur Kenntnis genommen. Er hat die BK beauftragt, die für die Neuausrichtung erforderlichen Massnahmen schrittweise umzusetzen.

Als erste Etappe der Neuausrichtung wurden die Rechtsgrundlagen zu E-Voting revidiert. Die teilrevidierte Verordnung über die politischen Rechte (VPR; SR 161.11) und die totalrevidierte Verordnung der BK über die elektronische Stimmabgabe (VEleS; SR 161.116) sind am 1. Juli 2022 in Kraft getreten.

Mit der Revision der VPR und VEleS wird die Sicherheit der E-Voting-Systeme gestärkt, indem die Sicherheits- und Qualitätsanforderungen an die Systeme, deren Einsatz und deren Entwicklung präzisiert und erhöht werden. Neu werden nur noch vollständig verifizierbare und von unabhängigen Expertinnen und Experten im Auftrag des Bundes überprüfte Systeme zugelassen. Sie dürfen für maximal 30 % des kantonalen und 10 % des schweizweiten Elektorats eingesetzt werden.

Die neuen Rechtsgrundlagen erhöhen die Transparenzanforderungen und schreiben den Einbezug der Öffentlichkeit und von Fachkreisen vor. So wurden die Vorgaben für die Offenlegung von Informationen zum System und dessen Betrieb präzisiert und Anforderungen für den Einbezug der Öffentlichkeit – zum Beispiel die Pflicht zur Führung eines ständigen Bug-Bounty-Programms – geregelt.

Die Zusammenarbeit mit Expertinnen und Experten erfolgt nicht nur im Rahmen der unabhängigen Überprüfung der Systeme, sondern wird auch als ständige Begleitung der Versuche etabliert. Der bereits für die Ausgestaltung der Neuausrichtung des Versuchsbetriebs geführte Dialog mit der Wissenschaft wird weitergeführt und in den Rechtsgrundlagen verankert. So soll in den nächsten Jahren ein breiter Massnahmenkatalog umgesetzt werden, der zu einer kontinuierlichen Verbesserung der E-Voting-Systeme und deren Betrieb führt.[6]

3.1.3 Wiederaufnahme der Versuche

Das vollständig verifizierbare E-Voting-System der Schweizerischen Post kam anlässlich der eidgenössischen Abstimmung vom 18. Juni 2023 zum ersten Mal zum Einsatz. Die vollständige Verifizierbarkeit ermöglicht die Entdeckung von allfälligen Manipulationen. Dazu kommen unabhängige Hilfsmittel zum Einsatz (Verifizierungscodes für die Stimmenden und Verifizierungssoftware für das Stimmbüro oder die Wahlkommission). Drei Kantone (Basel-Stadt, St.Gallen und Thurgau) haben anlässlich jenes Urnengangs einen Versuch mit der elektronischen Stimmabgabe durchgeführt und dabei das System der Schweizerischen Post eingesetzt. In allen drei Kantonen konnten die Auslandschweizer Stimmberechtigten ihre Stimme elektronisch abgeben. Zwei Kantone (Basel-Stadt, St.Gallen) haben die elektronische Stimmabgabe auch einer begrenzten Zahl von Stimmberechtigten mit Schweizer Wohnsitz angeboten. Am Versuch waren 64’869 Stimmberechtigte zugelassen. Dies entspricht rund 1.2 % aller Schweizer Stimmberechtigten. Davon haben insgesamt 4’239 Stimmberechtigte ihre Stimme elektronisch abgegeben.[6] Die Kantone und die BK ziehen zum Wiedereinsatz der elektronischen Stimmabgabe eine positive Bilanz. Es gab lediglich einen Vorfall zu verzeichnen (das E-Voting-Portal war zu Beginn der Abstimmungsperiode fast eine Stunde lang nicht verfügbar). Die Ursache lag in einem technischen Problem.[7] Massnahmen, um ein Wiederauftreten dieses Vorfalls zu verhindern, wurden ergriffen.

3.2 Sicherheit

3.2.1 Offenlegung des Quellcodes und öffentlicher Intrusionstest 2019

Im Februar 2019 legte die Schweizerischen Post den Quellcode ihres neuen Systems mit vollständiger Verifizierbarkeit sowie die entsprechende Dokumentation offen. Ausserdem unterstand das System vom 25. Februar bis am 24. März 2019 einem öffentlichen Intrusionstest. Im Quellcode des neuen Post-Systems wurden zwei erhebliche Mängel entdeckt. Ein weiterer Mangel betraf auch die individuelle Verifizierbarkeit und damit das damals bereits eingesetzte E-Voting-System der Post. In der Folge hat die Post ihr individuell verifizierbares System zurückgezogen.

---

[6] www.bk.admin.ch > Politische Rechte > E-Voting > Versuche mit E-Voting.

[7] https://www.evoting-info.ch/themen/sicherheit-technik/protokoll.html

3.2.2 Unabhängige Überprüfungen seit 2021

Die BK hat am 5. Juli 2021 eine unabhängige Überprüfung des vollständig verifizierbaren E-Voting-Systems der Post und dessen Betriebs gestartet. Mit der Überprüfung wurden Expertinnen und Experten aus Wissenschaft und Industrie beauftragt. Die Überprüfung wurde im Grundsatz im Januar 2023 für die Wiederaufnahme der Versuche bei der Abstimmung vom 18. Juni 2023 abgeschlossen. Anpassungen am System oder an seinem Betrieb werden gegebenenfalls erneut überprüft.

Die ersten Ergebnisse zeigten, dass das E-Voting-System der Post seit 2019 wesentlich verbessert wurde.[8] Wichtige Mängel konnten identifiziert und behoben werden. Aus den Berichten ging jedoch hervor, dass weitere Massnahmen ergriffen werden mussten. Im Sinne des kontinuierlichen Verbesserungsprozesses haben sich Bund und Kantone auf die Umsetzung dieser Massnahmen geeinigt und sie im gemeinsamen Massnahmenkatalog festgehalten.

Die Massnahem, die bis zu den Nationalratswahlen 2023 umgesetzt werden mussten, wurden umgesetzt und zusammen mit den anderen Änderungen überprüft. Diese Überprüfung wurde Ende Juli 2023 abgeschlossen. Gestützt auf die Ergebnisse dieser Überprüfung kommt die BK zum Schluss, dass das Sicherheitsniveau trotz bestehendem Handlungsbedarf ausreichend ist Der Handlungsbedarf muss mittel- bis langfristig angegangen werden. Dementsprechend haben Bund und Kantone haben den Massnahmenkatalog ergänzt.

Die Ergebnisse der unabhängigen Überprüfung bilden Teil der Entscheidungsgrundlagen im Hinblick auf die Beurteilung der kantonalen Gesuche um die Erteilung der Grundbewilligungen durch den Bundesrat.

3.2.3 Offenlegung des Quellcodes und der Dokumentation zum System der Post und dessen Betrieb sowie Bug-Bounty-Programm seit 2021

Gemäss Artikel 13 der revidierten VEleS hat die Post ihr gesamtes E-Voting-System mit vollständiger Verifizierbarkeit dauerhaft offengelegt. Sie führt zudem ein ständiges Bug-Bounty-Programm. In diesem Rahmen kann die Öffentlichkeit Hinweise einreichen, die einen Bezug zur Sicherheit haben und die zu Verbesserungen des Systems beitragen. Entsprechende Hinweise werden finanziell entschädigt. So können Expertinnen und Experten die Dokumente analysieren und den Quellcode überprüfen. Ziel dieser Massnahmen ist es, mögliche Schwachstellen im System aufgrund von entsprechenden Hinweisen zu erkennen und zu beheben.

Mit Stand vom Dezember 2022 hält die Post fest, dass über 180 Meldungen eingegangen sind, davon vier mit dem Schweregrad «hoch». Insgesamt wurden rund 120’000 Euro für die Meldungen ausbezahlt.[9] Im Juli 2023 sind 74 neue Meldungen eingegangenen. Sämtliche lagen unter dem Schweregrad «hoch». Die Post hat insgesamt 28.500 Euro für die neuen Meldungen ausbezahlt.[10,11]

Darüber hinaus fand vom 8. August bis 2. September 2022 ein erster öffentlicher Intrusionstest (PIT) statt. Die Post dokumentierte die Teilnahme von rund 3’400 Teilnehmenden sowie den Eingang von zwei Befunden. Ein Befund wurde mit Schweregrad «tief» bestätigt und mit 500 CHF belohnt. Ein Eindringen in die Infrastruktur oder in die elektronische Urne ist nicht gelungen. Die Post hat einen Abschlussbericht über den PIT veröffentlicht.[12] Der PIT wurde im Juli 2023 zum zweiten Mal durchgeführt. Das Bug-Bounty-Programm wird in Übereinstimmung mit den rechtlichen Anforderungen fortgesetzt.

3.2.4 Zunehmend bedrohendes Umfeld in der digitalen Welt

Angriffe auf IT-Systeme existieren zwar schon lange, aber in den letzten Monaten und Jahren konnte eine starke Zunahme beobachtet werden.[13] Die Angriffe beschränken sich nicht mehr auf grosse Unternehmen, sondern betreffen auch Behörden. Zwar scheint der Hauptgrund für solche Angriffe vor allem finanzieller Natur zu sein, aber auch ideologische oder politische Motive spielen eine Rolle. Ausserdem

---

[8] www.bk.admin.ch > Politische Rechte > E-Voting > Überprüfung von Systemen

[9] https://evoting-community.post.ch/de

[10] https://gitlab.com/swisspost-evoting/e-voting/e-voting-documentation/-/issues/46

[11] https://gitlab.com/swisspost-evoting/e-voting/e-voting-documentation/-/issues/48

[12] https://gitlab.com/swisspost-evoting/e-voting/e-voting-documentation/-/tree/master/Reports/PublicIntrusionTest

[13] www.ncsc.admin.ch > Dokumentation > Berichte > Lageberichte > Halbjahresbericht 2022/1

trägt die zunehmende Verfügbarkeit von Malware-as-a-Service-Plattformen dazu bei, dass die für einen Cyberangriff erforderlichen Instrumente immer leichter zugänglich sind und dass für die Durchführung eines Angriffs weniger Kenntnisse notwendig sind.

Cyberkriminalität ist nach wie vor die unmittelbarste Bedrohung für kritische Infrastrukturen. Sie geht sowohl von privaten Akteuren aus finanziellen Gründen als auch von staatlichen Akteuren oder Hacktivisten zur Destabilisierung von Systemen aus. Unmittelbar vor und auch während des russischen Krieges gegen die Ukraine erfolgten Cyberangriffe auf kritische ukrainische Infrastrukturen. Wenn die Schweiz aus politischen Gründen ins Visier von staatlichen oder nichtstaatlichen Akteuren gerät, die über die notwendigen Kapazitäten verfügen, steigt die Wahrscheinlichkeit von Cyberangriffen. Laut Lagebericht des Nachrichtendienstes des Bundes sind speziell gegen die Schweiz gerichtete Sabotage sehr unwahrscheinlich und «Hacktivismus» gegen die Schweiz eher wahrscheinlich, während Angriffe im Bereich der Desinformation als wahrscheinlich angenommen werden. Cyberspionage gegen die Schweiz hingegen ist sehr wahrscheinlich.[14] Das Ergreifen von Massnahmen durch die Schweiz gegen bestimmte russische Interessen könnte auch Auswirkungen auf die Gefährdung durch Cyberangriffe auf kritische IT-Infrastrukturen haben.[13] Ein konkretes Beispiel sind die Denial-of-Service-Angriffe, die im Juni 2023 gegen die Websites des Parlaments und der Bundesverwaltung durchgeführt wurden und zu denen sich eine sich selbst als pro-russisch bezeichnende Gruppe namens "NoName" bekannte. Ausserdem sind derzeit Ransomware-Angriffe im Trend.[15] Auch wenn diese nun hauptsächlich auf die Erpressung zur Herausgabe der gesammelten Daten abzielen, haben sie dennoch ein hohes Störungspotenzial, indem sie die betroffenen IT-Systeme lahmlegen können. Die Gruppe "Play" hat sich in diesem Bereich besonders hervorgetan. Sie verfügt über ein Arsenal an Werkzeugen, mit denen sie gut geschützte Ziele angreifen kann.[16]

Die Verifizierbarkeit gemäss VEleS ist so ausgestaltet, dass sie auch gegen ein besonders bedrohendes Umfeld einen angemessenen Schutz bietet. Darüber hinaus gehören die mit E-Voting verbundene Infrastruktur und Software zu den kritischen Infrastrukturen, die im Falle eines Angriffs von den zuständigen Bundesstellen unterstützt werden können.[17]

3.3 Technologie

3.3.1 Quantencomputer

Quantencomputer könnten insbesondere für asymmetrische Verschlüsselungsmechanismen (RSA, El Gamal, Diffie-Hellman) ein Problem darstellen, da es bereits einen Quantenalgorithmus (Faktorisierungsalgorithmus Shor[18]) gibt, mit dem diese Probleme effizient gelöst und somit die mit diesen Mechanismen verschlüsselten Daten entschlüsselt werden können. Doch obwohl sich dieses Gebiet rasch entwickelt und viel investiert wird, ist eine konkrete Anwendung noch weit entfernt. Quantencomputer benötigen eine sehr spezifische Umgebung, um richtig funktionieren zu können, und sie sind sehr anfällig für Störungen.[19] Derzeit wird davon ausgegangen, dass bei einer Anwendung des oben erwähnten Shor-Algorithmus auf einem perfekten Quantencomputer mindestens doppelt so viele Qubits[20] benötigt würden wie die Anzahl der Bits, mit denen die zu erratende Zahl codiert wird.[21] Zum Knacken eines RSA-Schlüssels von 2048 Bit würde man somit mehr als 4’000 Qubits benötigen. IBM plant, dies im Jahr 2025 zu erreichen.[22]

---

[14] https://www.vbs.admin.ch/ > Über uns > Organisation > Verwaltungseinheiten > Nachrichtendienst > Dokumente > Sicherheit Schweiz 2023 - Lagebericht des Nachrichtendienstes des Bundes

[15] Jährliche Beurteilung der Bedrohungslage - Bericht des Bundesrates an die eidgenössischen Räte

[16] www.ncsc.ch > Dokumentation > Berichte > Lageberichte > Halbjahresbericht 2022/2

[17] www.babs.admin.ch > Weitere Aufgabenfelder > Schutz kritischer Infrastrukturen.

[18] Shor-Algorithmus – Wikipedia

[19] Present landscape of quantum computing - Hassija - 2020 - IET Quantum Communication - Wiley Online Library

[20] Qubits sind eine Masseinheit für die Leistung von Quantencomputern. Vereinfacht gesagt: Je mehr Qubits ein Quantencomputer hat, desto grösser sind die Zahlen, die er manipulieren kann. Allerdings können nicht alle Qubits für Berechnungen verwendet werden, da je nach verwendeter Technologie ein Teil der Qubits für die Korrektur von Fehlern eingesetzt werden muss. IBM hat daher eine neue Masseinheit eingeführt, das Quantenvolumen, das nur die Qubits berücksichtigt, die tatsächlich und zuverlässig genutzt werden können.

[21] Quantum Attack Resource Estimate: Using Shor’s Algorithm to Break RSA vs DH/DSA VS ECC – Kudelski Security Research

[22] https://www.ibm.com/quantum/roadmap

Das National Institute of Standards and Technology (NIST)[23] hat 2016 einen Prozess zur Auswahl und Standardisierung von Verfahren der Post-Quanten-Kryptografie eingeleitet.[24] Die dritte Auswahlrunde wurde 2020 abgeschlossen und die Entwürfe der Standards sollten bis 2024 verfügbar sein.

Bis Post-Quanten-Standardalgorithmen zur Verfügung stehen, ist es immer noch möglich, die Auswirkungen der Entwicklung von Quantencomputern auf aktuelle Verschlüsselungsmechanismen zu verhindern und zu minimieren, indem die Schlüssel für die Verschlüsselung verlängert werden. Das System der Post verwendet derzeit Schlüssel mit einer Länge von 3072 Bit. Ebenso können informationstheoretisch sichere Verschlüsselungsverfahren den erfolgreichen Einsatz von Quantencomputern erschweren.

4 Analyse und Evaluation der Risiken

Zahlreiche Massnahmen werden umgesetzt, um die Risiken bei E-Voting zu minimieren. Die folgende Tabelle umfasst eine Zusammenfassung der Beurteilung der Risiken, wie sie sich vor dem Ergreifen von Minimierungsmassnahmen präsentieren. Die detaillierte Beurteilung der einzelnen Risiken befindet sich im Anhang. Zu beachten ist, dass sich der Risiko-Score auf die Auswirkungen des Eintretens eines Risikos bezieht, während sich die Wahrscheinlichkeit des Risikos auf das in der Beschreibung genannte Ereignis beschränkt. Die hier angegebene Wahrscheinlichkeit bezieht sich somit nicht auf das im Anhang beschriebene worst-case-Szenario, das in der Regel mit einer geringeren Wahrscheinlichkeit eintritt als ein optimistischeres Szenario. Die Evaluation zum Zustand nach dem Ergreifen von Minimierungsmassnahmen wird in Kapitel 6 zu den Restrisiken dargestellt.

ID	Beschreibung	Score	Wahrscheinlichkeit
BK-VE-R1	Ein erheblicher Sicherheitsmangel, der das System betrifft, wird während eines Urnengangs entdeckt.	40	Mittel
BK-VE-R2	In mehreren Kantonen werden falsch angezeigte Prüfcodes gemeldet, aber aufgrund einer fehlenden Koordination zwischen den Kantonen und der BK erfolgt auf nationaler Ebene keine Alarmierung.	44	Mittel
BK-VE-R3	Der elektronische Stimmkanal wird nicht ausreichend akzeptiert.	33	Mittel
BK-VE-R4	In den Medien oder in sozialen Netzwerken wird eine Kampagne gegen den elektronischen Stimmkanal geführt. Diese kann auf Ereignissen rund um die elektronische Stimmabgabe im Ausland, auf angeblich fehlenden öffentlichen Kontrollmöglichkeiten, auf falschen Behauptungen über die Verifizierbarkeit oder auf einer mangelhaften Kommunikation der Behörden beruhen.	29	Hoch
BK-VE-R5	Eine Gruppe, die über eine anonyme Kaufplattform verfügt, lanciert eine grossangelegte Kampagne zum Stimmenkauf.	43	Mittel
BK-VE-R6	Einen politisch motivierten Akteur mit hohen Ressourcenmobilisiert seine Ressourcen und es gelingt ihm, Stimmen im System zu manipulieren.	43	Mittel
BK-VE-R7	Einen politisch motivierten Akteur mit hohen Ressourcenmobilisiert seine Ressourcen und es gelingt ihm, das Stimmgeheimnis zu brechen.	38	Mittel
BK-VE-R8	Einen politisch motivierten Akteur mit hohen Ressourcenmobilisiert seine Ressourcen und es gelingt ihm, das Ergebnis des Urnengangs zu beeinflussen, indem Stimmberechtigte von der Stimmabgabe abgehalten werden.	31	Hoch

[23] Das National Institute of Standards and Technology ist eine Behörde des Handelsministeriums der USA. Es verfolgt das Ziel, die Wirtschaft durch die Entwicklung von Technologien, Messverfahren und Normen in Zusammenarbeit mit der Industrie zu fördern.

[24] https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization

ID	Beschreibung	Score	Wahrscheinlichkeit
BK-VE-R9	Die bundesrechtlichen Anforderungen sind unzulänglich und das gewünschte Sicherheitsniveau kann damit nicht aufrechterhalten werden.	40	Tief
BK-VE-R10	Der Bund hat ein System zugelassen, das die bundesrechtlichen Sicherheitsanforderungen nicht erfüllt.	47	Mittel
BK-VE-R11	Es wird ein System eingesetzt, das nicht dem zugelassenen System entspricht.	44	Mittel
BK-VE-R12	Ein fehlendes Interesse von Expertinnen und Experten im Bereich von Vote électronique führt dazu, dass die Sicherheitsanforderungen nicht weiterentwickelt werden und sie nicht mehr den aktuellen Kenntnisstand abbilden.	40	Mittel
BK-VE-R13	Für die Durchführung von Überprüfungen mangelt es an qualifizierten unabhängigen Expertinnen und Experten.	32	Mittel
BK-VE-R14	Eine neue Technologie verbreitet sich und führt dazu, dass die Sicherheitsanforderungen für die Wahrung des Stimmgeheimnisses nicht mehr ausreichen (z.B. Quantencomputer).	35	Tief
BK-VE-R15	Der Systemanbieter ist während eines Urnengangs nicht mehr in der Lage, sein System zur Verfügung zu stellen, obwohl bereits Stimmen abgegeben wurden.	40	Tief
BK-VE-R16	Streitigkeiten zwischen den Behörden und der Post stören die Zusammenarbeit derart stark, dass der elektronische Stimmkanal nicht mehr weiterentwickelt werden kann oder unterbrochen werden muss.	23	Mittel
BK-VE-R17	Den Kantonen fehlen die Ressourcen für die Umsetzung des elektronischen Stimmkanals.	28	Mittel
BK-VE-R18	Die tatsächliche Nutzung des elektronischen Stimmkanals übersteigt die Limitierung des zugelassenen Elektorats (30 % kantonal und 10 % national).	39	Tief

Tabelle 3: Zusammenfassung der Risikoanalyse und -evaluation vor der Umsetzung von Minimierungsmassnahmen.

Wahrscheinlichkeit	Auswirkungen (Risiko-Score) 32 – 49 (Hoch)	22 – 31 (Mittel)	17 – 21 (Tief)
Hoch		**R4** Negativkampagne gegen E-Voting in (sozialen) Medien **R8** Systemausfall infolge Angriff durch einen politisch motivierten Akteur mit hohen Ressourcen	
Mittel	**R1** Erheblicher Sicherheitsmangel im System **R2** Mangelnde Erkennung systematischer Fehler **R5** Stimmenkauf über anonyme Plattform **R6** Manipulation der Stimmen durch einen politisch motivierten Akteur mit hohen Ressourcen **R7** Verletzung Stimmgeheimnis durch einen politisch motivierten Akteur mit hohen Ressourcen **R10** Zulassung eines mangelhaften Systems **R11** Einsatz eines nicht zugelassenen Systems **R12** Gefährdung Weiterentwicklung Sicherheitsanforderungen **R13** Mangel an unabhängigen Expertinnen und Experten	**R3** Mangelnde Akzeptanz von E-Voting **R16** Wegfall Stimmkanal wegen unzureichender Zusammenarbeit **R17** Wegfall Stimmkanal wegen fehlender Ressourcen	
Tief	**R9** Unzulängliche Anforderungen **R14** Neue Technologien führen zu Verletzung Stimmgeheimnis **R15** Systemausfall während Urnengang **R18** Überschreitung der Limiten im Bundesrecht		

Tabelle 4: Übersicht der Risiken vor der Umsetzung von Minimierungsmassnahmen.

5 Risikobehandlung (Umgang)

Ein Grossteil der Massnahmen zur Risikominimierung ist in den Rechtsgrundlagen geregelt (VPR und VEleS). Diese Massnahmen reichen jedoch nicht aus und es müssen weitere Massnahmen ergriffen werden, um die Risiken auf ein akzeptables Niveau zu minimieren. Die folgende Tabelle zum Umgang mit den Risiken zeigt die sogenannten aktuellen Massnahmen, die bereits umgesetzt werden, und die künftigen Massnahmen, deren Umsetzung geplant ist, auf. Die künftigen Massnahmen umfassen insbesondere die mittel- bis langfristigen Massnahmen aus dem Massnahmenkatalog von Bund und Kantonen.[25] Die künftigen Massnahmen werden laufend und je nach Bedarf im Sinne des kontinuierlichen Verbesserungsprozesses der Versuche ergänzt.

[25] www.bk.admin.ch > Politische Rechte > E-Voting > Versuche mit E-Voting.

Score	Wahrsch.	Umgang	Aktuelle Massnahmen	Künftige Massnahmen
BK-VE-R1 Erheblicher Sicherheitsmangel im System				

40	Mittel	Minimieren	- Rechtliche Anforderungen:
			  - Unabhängige Überprüfung der Systeme und Betriebsmodalitäten (Art. 27*l* VPR, Art. 10 VEleS)
			  - Limitierung auf 30 % des kantonalen und 10 % des nationalen Elektorats (Art. 27*f* VPR)
			  - Öffentlichkeit der Informationen zum System und dessen Betrieb (Art. 27*l*^{bis} VPR)
			  - Einbezug der Öffentlichkeit (Art. 27*l*^{ter} VPR)
			  - Plausibilisierung (Art. 27*i* Abs. 2 VPR)
			  - Beizug unabhängiger Fachpersonen und wissenschaftliche Begleitung (Art. 27*o* VPR)
			  - Grundvoraussetzungen für die Zulassung der elektronischen Stimmabgabe pro Urnengang (Art. 3 VEleS)
			  - Risikobeurteilungen (Art. 4 VEleS)
			  - Anforderungen an die vollständige Verifizierbarkeit (Art. 5 VEleS)
			  - Offenlegung des Quellcodes und der Dokumentation zum System und dessen Betrieb (Art. 11 und 12 VEleS)
			  - Anforderungen an vertrauenswürdige Komponenten nach Ziffer 2 und an deren Betrieb (Ziff. 3 Anhang VEleS)
			  - Stimmabgabe an der Urne oder briefliche Stimmabgabe sind vor der Bestätigung der definitiven Stimmabgabe weiterhin möglich (Ziff. 4.4 und 4.11 Anhang VEleS)
			  - Feststellung und Meldung von Sicherheitsereignissen und -schwächen; Handhabung von Sicherheitsereignissen und -verbesserungen (Ziff. 14 Anhang VEleS)
			- Führen eines gemeinsamen Massnahmenplans von Bund und Kantonen
			- Krisenvereinbarung
			- Krisenübungen
				- Weiterentwicklung der Plausibilisierung der E-Voting-Ergebnisse (Massnahme B.8 Massnahmenkatalog)
				- Stärkung der Verifizierbarkeit (Massnahmen A.4, A.5, A.6, A.19 und A.22 Massnahmenkatalog)
				- Stärkere Vernetzung mit der Wissenschaft und wissenschaftliche Begleitung der Versuche (Massnahmen D.1, D.2 und D.3 Massnahmenkatalog)
				- Weiterentwicklung des Systems und der Dokumentation (Massnahmen A.10, A.12, A.13, A.14, A.15, A.16, A.18, A.21, A.23, A.24 und A.25 Massnahmenkatalog)
				- Erweiterung der Elemente, deren Quellcode offengelegt wird (Massnahme A.11 Massnahmenkatalog)
				- Verbesserung der Dokumentation, die offengelegt wird (Massnahmen A.17, A.20 und C.7 Massnahmenkatalog)
				- Verbesserung der Möglichkeiten zur Untersuchung von Vorfällen (Massnahme B.13 Massnahmenkatalog)
				- Verbesserung der Risikodokumentation (Massnahmen B.11 und B.12 Massnahmenkatalog)

BK-VE-R2 Mangelnde Erkennung systematischer Fehler				

44	Mittel	Minimieren	- Rechtliche Anforderungen:
			  - Informationen für die Stimmberechtigen (Ziff. 8 Anhang VEleS)
			  - Feststellung und Meldung von Sicherheitsereignissen und -schwächen; Handhabung von Sicherheitsereignissen und -verbesserungen (Ziff. 14 Anhang VEleS)
			- Krisenvereinbarung
			- Krisenübungen
				- Verbesserung der Möglichkeiten zur Untersuchung von Vorfällen (Massnahme B.13 Massnahmenkatalog)

Score	Wahrsch.	Umgang	Aktuelle Massnahmen	Künftige Massnahmen
BK-VE-R3 Mangelnde Akzeptanz von E-Voting				

33	Mittel	Minimieren	- Rechtliche Anforderungen:
			  - Limitierung auf 30 % des kantonalen und 10 % des nationalen Elektorats (Art. 27*f* VPR)
			  - Öffentlichkeit der Informationen zum System und dessen Betrieb (Art. 27*l*^{bis} VPR)
			  - Einbezug der Öffentlichkeit (Art. 27*l*^{ter} VPR)
			  - Information der Stimmberechtigten und Veröffentlichung der Ergebnisse der elektronischen Stimmabgabe (Art. 27*m* VPR)
			  - Plausibilisierung (Art. 27*i* Abs. 2 VPR)
			  - Beizug unabhängiger Fachpersonen und wissenschaftliche Begleitung (Art. 27*o* VPR)
			  - Grundvoraussetzungen für die Zulassung der elektronischen Stimmabgabe pro Urnengang (Art. 3 VEleS)
			  - Risikobeurteilungen (Art. 4 VEleS)
			  - Anforderungen an die vollständige Verifizierbarkeit (Art. 5 VEleS)
			  - Offenlegung des Quellcodes und der Dokumentation zum System und dessen Betrieb (Art. 11 und 12 VEleS)
			  - Verantwortung und Zuständigkeiten für den korrekten Ablauf des Urnengangs mit der elektronischen Stimmabgabe (Art. 14 VEleS)
			- Organisation/Teilnahme an öffentlichen Anlässen
			- Zurverfügungstellen von Informationsmaterial über die Sicherheit von E-Voting
			- Führen eines gemeinsamen Massnahmenplans von Bund und Kantonen
			- Sachliche und transparente Kommunikation
			- Kontinuierlicher Verbesserungsprozess für die Versuchsphase
				- Stärkung der Verifizierbarkeit (Massnahmen A.4, A.5, A.6, A.19 und A.22 Massnahmenkatalog)
				- Weiterentwicklung der Plausibilisierung der E-Voting-Ergebnisse (Massnahme B.8 Massnahmenkatalog)
				- Stärkere Vernetzung mit der Wissenschaft und wissenschaftliche Begleitung der Versuche (Massnahmen D.1, D.2 und D.3 Massnahmenkatalog)
				- Weiterentwicklung des Systems und der Dokumentation (Massnahmen A.10, A.12, A.13, A.14, A.15, A.16, A.18, A.21, A.23, A.24 und A.25 Massnahmenkatalog)
				- Erweiterung der Elemente, deren Quellcode offengelegt wird (Massnahme A.11 Massnahmenkatalog)
				- Verbesserung der Dokumentation, die offengelegt wird (Massnahmen A.17, A.20 und C.7 Massnahmenkatalog)
				- Verbesserung der Möglichkeiten zur Untersuchung von Vorfällen (Massnahme B.13 Massnahmenkatalog)
				- Verbesserung der Risikodokumentation (Massnahmen B.11 und B.12 Massnahmenkatalog)

Score	Wahrsch.	Umgang	Aktuelle Massnahmen	Künftige Massnahmen
BK-VE-R4 Negativkampagne gegen E-Voting in (sozialen) Medien				

29	Hoch	Minimieren	- Rechtliche Anforderungen:
			  - Öffentlichkeit der Informationen zum System und dessen Betrieb (Art. 27*l*bis VPR)
			  - Einbezug der Öffentlichkeit (Art. 27*l*ter VPR, Art. 13 VEleS)
			  - Information der Stimmberechtigten und Veröffentlichung der Ergebnisse der elektronischen Stimmabgabe (Art. 27*m* VPR)
			  - Beizug unabhängiger Fachpersonen und wissenschaftliche Begleitung (Art. 27*o* VPR)
			  - Plausibilisierung (Art. 27*i* Abs. 2 VPR)
			  - Anforderungen an die vollständige Verifizierbarkeit (Art. 5 VEleS)
			  - Unabhängige Überprüfung der Systeme und Betriebsmodalitäten (Art. 27*l* VPR, Art. 10 VEleS)
			  - Unterbreiten von Hinweisen an die Prüferinnen und Prüfer (Ziff. 11.10 Anhang VEleS)
			  - Erstellung eines Notfallplans (Ziff. 11.11 Anhang VEleS)
			- Sachliche und transparente Kommunikation
			- Führen eines gemeinsamen Massnahmenplans von Bund und Kantonen
			- Krisenvereinbarung
			- Krisenübungen
				- Stärkere Vernetzung mit der Wissenschaft und wissenschaftliche Begleitung der Versuche (Massnahmen D.1, D.2 und D.3 Massnahmenkatalog)
				- Weiterentwicklung des Systems und der Dokumentation (Massnahmen A.10, A.12, A.13, A.14, A.15, A.16, A.18, A.21, A.23, A.24 und A.25 Massnahmenkatalog)
				- Erweiterung der Elemente, deren Quellcode offengelegt wird (Massnahme A.11 Massnahmenkatalog)
				- Verbesserung der Dokumentation, die offengelegt wird (Massnahmen A.17, A.20 und C.7 Massnahmenkatalog)
				- Verbesserung der Möglichkeiten zur Untersuchung von Vorfällen (Massnahme B.13 Massnahmenkatalog)

BK-VE-R5 Stimmenkauf über anonyme Plattform				

43	Mittel	Minimieren	- Rechtliche Anforderungen:
			  - Limitierung auf 30 % des kantonalen und 10 % des nationalen Elektorats (Art. 27*f* VPR)
			  - Risikobeurteilungen (Art. 4 VEleS)
			- Strafrechtliche Verfolgung von Wahlbestechung, die auch auf E-Voting anwendbar ist (Art. 281 Schweizerisches Strafgesetzbuch)	

Score	Wahrsch.	Umgang	Aktuelle Massnahmen	Künftige Massnahmen
BK-VE-R6 Manipulation der Stimmen durch einen politisch motivierten Akteur mit hohen Ressourcen				

43	Mittel	Minimieren	- Rechtliche Anforderungen:
			  - Limitierung auf 30 % des kantonalen und 10 % des nationalen Elektorats (Art. 27*f* VPR)
			  - Öffentlichkeit der Informationen zum System und dessen Betrieb (Art. 27*l*^{bis} VPR)
			  - Einbezug der Öffentlichkeit (Art. 27*l*^{ter} VPR)
			  - Plausibilisierung (Art. 27*i* Abs. 2 VPR)
			  - Beizug unabhängiger Fachpersonen und wissenschaftliche Begleitung (Art. 27*o* VPR)
			  - Grundvoraussetzungen für die Zulassung der elektronischen Stimmabgabe pro Urnengang (Art. 3 VEleS)
			  - Risikobeurteilungen (Art. 4 VEleS)
			  - Anforderungen an die vollständige Verifizierbarkeit (Art. 5 VEleS und Ziff. 2 Anhang VEleS)
			  - Offenlegung des Quellcodes und der Dokumentation zum System und dessen Betrieb (Art. 11 und 12 VEleS)
			  - Anforderungen an vertrauenswürdige Komponenten nach Ziffer 2 und an deren Betrieb (Ziff. 3 Anhang VEleS)
			  - Stimmabgabe an der Urne oder briefliche Stimmabgabe sind vor der Bestätigung der definitiven Stimmabgabe weiterhin möglich (Ziff. 4.4 und 4.11 Anhang VEleS)
			  - Anforderungen an die Druckereien (Ziff. 7 Anhang VEleS)
			  - Informationen und Anleitungen (Ziff. 8 Anhang VEleS)
			  - Feststellung und Meldung von Sicherheitsereignissen und -schwächen; Handhabung von Sicherheitsereignissen und -verbesserungen (Ziff. 14 Anhang VEleS)
			  - Vertrauenswürdigkeit des Personals (Ziff. 20 Anhang VEleS)
			  - Management der Kommunikation und des Betriebs (Ziff. 22 Anhang VEleS)
			- Führen eines gemeinsamen Massnahmenplans von Bund und Kantonen
			- Beobachten von Entwicklungen im Bereich von Bedrohungen
			- Krisenvereinbarung
			- Krisenübungen
				- Stärkung der Verifizierbarkeit (Massnahmen A.4, A.5, A.6, A.19 und A.22 Massnahmenkatalog)
				- Weiterentwicklung der Plausibilisierung der E-Voting-Ergebnisse (Massnahme B.8 Massnahmenkatalog)
				- Weiterentwicklung des Systems und der Dokumentation (Massnahmen A.10, A.12, A.13, A.14, A.15, A.16, A.18, A.21, A.23, A.24 und A.25 Massnahmenkatalog)
				- Verbesserung der Möglichkeiten zur Untersuchung von Vorfällen (Massnahme B.13 Massnahmenkatalog)
				- Verbesserung der Risikodokumentation (Massnahmen B.11 und B.12 Massnahmenkatalog)

Score	Wahrsch.	Umgang	Aktuelle Massnahmen	Künftige Massnahmen
BK-VE-R7 Verletzung Stimmgeheimnis durch einen politisch motivierten Akteur mit hohen Ressourcen				

38	Mittel	Minimieren	- Rechtliche Anforderungen:
			  - Limitierung auf 30 % des kantonalen und 10 % des nationalen Elektorats (Art. 27*f* VPR)
			  - Risikobeurteilungen (Art. 4 VEleS)
			  - Anforderungen an die vollständige Verifizierbarkeit (Art. 5 VEleS und Ziff. 2 Anhang VEleS)
			  - Anforderungen an vertrauenswürdige Komponenten nach Ziffer 2 und an deren Betrieb (Ziff. 3 Anhang VEleS)
			  - Anforderungen an die Druckereien (Ziff. 7 Anhang VEleS)
			  - Informationen und Anleitungen (Ziff. 8 Anhang VEleS)
			  - Umgang mit vertraulichen Daten (Ziff. 12 VEleS)
			  - Feststellung und Meldung von Sicherheitsereignissen und -schwächen; Handhabung von Sicherheitsereignissen und -verbesserungen (Ziff. 14 Anhang VEleS)
			  - Vertrauenswürdigkeit des Personals (Ziff. 20 Anhang VEleS)
			- Führen eines gemeinsamen Massnahmenplans von Bund und Kantonen
			- Beobachten von Entwicklungen im Bereich von Bedrohungen
			- Krisenvereinbarung
			- Krisenübungen
				- Weiterentwicklung des Systems und der Dokumentation (Massnahmen A.10, A.12, A.13, A.14, A.15, A.16, A.18, A.21, A.23, A.24 und A.25 Massnahmenkatalog)
				- Verbesserung der Möglichkeiten zur Untersuchung von Vorfällen (Massnahme B.13 Massnahmenkatalog)
				- Verbesserung der Risikodokumentation (Massnahmen B.11 und B.12 Massnahmenkatalog)

Score	Wahrsch.	Umgang	Aktuelle Massnahmen	Künftige Massnahmen
BK-VE-R8 Systemausfall infolge Angriff durch einen politisch motivierten Akteur mit hohen Ressourcen				

31	Hoch	Minimieren	- Rechtliche Anforderungen:
			  - Periode zur Stimmabgabe dauert 3 bis 4 Wochen (Art. 11 Abs. 3 und Art. 33 Abs. 2 Bundesgesetz über die politischen Rechte)
			  - Risikobeurteilungen (Art. 4 VEleS)
			  - Anforderungen an die vollständige Verifizierbarkeit (Art. 5 VEleS und Ziff. 2 Anhang VEleS)
			  - Anforderungen an vertrauenswürdige Komponenten nach Ziffer 2 und an deren Betrieb (Ziff. 3 Anhang VEleS)
			  - Stimmabgabe an der Urne oder briefliche Stimmabgabe sind vor der Bestätigung der definitiven Stimmabgabe weiterhin möglich (Ziff. 4.4 und 4.11 Anhang VEleS)
			  - Feststellung und Meldung von Sicherheitsereignissen und -schwächen; Handhabung von Sicherheitsereignissen und -verbesserungen (Ziff. 14 Anhang VEleS)
			  - Vertrauenswürdigkeit des Personals (Ziff. 20 Anhang VEleS)
			  - Management der Kommunikation und des Betriebs (Ziff. 22 Anhang VEleS)
			- Führen eines gemeinsamen Massnahmenplans von Bund und Kantonen
			- Beobachten von Entwicklungen im Bereich von Bedrohungen
			- Krisenvereinbarung
			- Krisenübungen
				- Weiterentwicklung der Plausibilisierung der E-Voting-Ergebnisse (Massnahme B.8 Massnahmenkatalog)
				- Mögliche Massnahmen zum Schutz des Netzwerks prüfen
				- Verbesserung der Möglichkeiten zur Untersuchung von Vorfällen (Massnahme B.13 Massnahmenkatalog)

BK-VE-R9 Unzulängliche Anforderungen				
40	Tief	Minimieren	- Rechtliche Anforderungen: - Beizug unabhängiger Fachpersonen und wissenschaftliche Begleitung (Art. 27*o* VPR) - Organisation/Teilnahme an öffentlichen Anlässen - Technische Anforderungen werden in einer Verordnung der BK geregelt, um Anpassungen rasch umsetzen zu können - Beobachten der technologischen, soziologischen und rechtlichen Entwicklungen im Bereich von Vote électronique - Beobachten von Entwicklungen im Bereich der Informationssicherheit - Zusammenarbeit mit der Wissenschaft	- Stärkere Vernetzung mit der Wissenschaft und wissenschaftliche Begleitung der Versuche (Massnahmen D.1, D.2 und D.3 Massnahmenkatalog)

Score	Wahrsch.	Umgang	Aktuelle Massnahmen	Künftige Massnahmen
BK-VE-R10 Zulassung eines mangelhaften Systems				

47	Mittel	Minimieren	- Rechtliche Anforderungen:
			  - Limitierung auf 30 % des kantonalen und 10 % des nationalen Elektorats (Art. 27*f* VPR)
			  - Unabhängige Überprüfung der Systeme und Betriebsmodalitäten (Art. 27*l* VPR, Art. 10 VEleS)
			  - Offenlegung des Quellcodes und der Dokumentation zum System und dessen Betrieb (Art. 11 und 12 VEleS)
			  - Einbezug der Öffentlichkeit (Art. 13 VEleS)
			  - Feststellung und Meldung von Sicherheitsereignissen und -schwächen; Handhabung von Sicherheitsereignissen und -verbesserungen (Ziff. 14 Anhang VEleS)
			  - Entwicklung und Wartung von Informationssystemen (Ziff. 24 Anhang VEleS)
			  - Qualität Quellcode und Dokumentation (Ziff. 25 Anhang VEleS)
			- Führen eines gemeinsamen Massnahmenplans von Bund und Kantonen
				- Stärkere Vernetzung mit der Wissenschaft und wissenschaftliche Begleitung der Versuche (Massnahmen D.1, D.2 und D.3 Massnahmenkatalog)
				- Weiterentwicklung der Plausibilisierung der E-Voting-Ergebnisse (Massnahme B.8 Massnahmenkatalog)
				- Weiterentwicklung des Systems und der Dokumentation (Massnahmen A.10, A.12, A.13, A.14, A.15, A.16, A.18, A.21, A.23, A.24 und A.25 Massnahmenkatalog)
				- Verbesserung der Möglichkeiten zur Untersuchung von Vorfällen (Massnahme B.13 Massnahmenkatalog)

BK-VE-R11 Einsatz eines nicht zugelassenen Systems				

44	Mittel	Minimieren	- Rechtliche Anforderungen:
			  - Offenlegung Nachweis, dass die maschinenlesbaren Programme aus dem publizierten Quellcode der Software erstellt worden sind (Art. 27*l*^{bis} Abs. 2 Bst. d VPR, Art. 11 Abs. 1 Bst. b VEleS)
			  - Definition und Genehmigung von Rollen und Zugriffen (Ziff. 18, 21 und 23 Anhang VEleS)
			  - Zuverlässige und nachvollziehbare Kompilierung und zuverlässiges und nachvollziehbares Deployment (Ziff. 24.3 Anhang VEleS)	

BK-VE-R12 Gefährdung Weiterentwicklung Sicherheitsanforderungen				
40	Mittel	Minimieren	- Rechtliche Anforderungen: - Beizug unabhängiger Fachpersonen und wissenschaftliche Begleitung (Art. 27*o* VPR) - Organisation/Teilnahme an öffentlichen Anlässen - Beobachten der technologischen, soziologischen und rechtlichen Entwicklungen im Bereich von Vote électronique - Beobachten von Entwicklungen im Bereich der Informationssicherheit - Zusammenarbeit mit der Wissenschaft	- Stärkere Vernetzung mit der Wissenschaft und wissenschaftliche Begleitung der Versuche (Massnahmen D.1, D.2 und D.3 Massnahmenkatalog)

Score	Wahrsch.	Umgang	Aktuelle Massnahmen	Künftige Massnahmen
BK-VE-R13 Mangel an unabhängigen Expertinnen und Experten				
32	Mittel	Minimieren	- Rechtliche Anforderungen: - Beizug unabhängiger Fachpersonen und wissenschaftliche Begleitung (Art. 27*o* VPR) - Organisation/Teilnahme an öffentlichen Anlässen - Zusammenarbeit mit der Wissenschaft	- Stärkere Vernetzung mit der Wissenschaft und wissenschaftliche Begleitung der Versuche (Massnahmen D.1, D.2 und D.3 Massnahmenkatalog)
BK-VE-R14 Neue Technologien führen zu Verletzung Stimmgeheimnis				
35	Tief	Beobachten	- Beobachten der technologischen, soziologischen und rechtlichen Entwicklungen im Bereich von Vote électronique - Beobachten von Entwicklungen im Bereich der Informationssicherheit - Zusammenarbeit mit der Wissenschaft	- Stärkere Vernetzung mit der Wissenschaft und wissenschaftliche Begleitung der Versuche (Massnahmen D.1, D.2 und D.3 Massnahmenkatalog) - Weiterentwicklung des Systems und der Dokumentation (Massnahmen A.10, A.12, A.13, A.14, A.15, A.16, A.18, A.21, A.23, A.24 und A.25 Massnahmenkatalog)
BK-VE-R15 Systemausfall während Urnengang				

40	Tief	Minimieren	- Rechtliche Anforderungen:
			  - Periode zur Stimmabgabe dauert 3 bis 4 Wochen (Art. 11 Abs. 3 und Art. 33 Abs. 2 Bundesgesetz über die politischen Rechte)
			  - Limitierung auf 30 % des kantonalen und 10 % des nationalen Elektorats (Art. 27*f* VPR)
			- Stimmabgabe an der Urne oder briefliche Stimmabgabe
			- Krisenvereinbarung
			- Krisenübungen	

BK-VE-R16 Wegfall Stimmkanal wegen unzureichender Zusammenarbeit				
23	Mittel	Minimieren	- Führen eines gemeinsamen Massnahmenplans von Bund und Kantonen - Kurzfristig: Mitfinanzierung von Massnahmen, deren Kosten hauptsächlich von den (wenigen) betroffenen Kantonen getragen werden müssen, über die bestehenden Instrumente des Bundes (z.B. Digitale Verwaltung Schweiz DVS) - Mittel- bis langfristig: Sicherstellen der langfristigen Finanzierung - Koordination der Arbeiten über die bestehenden Projektgremien	- Langfristige Überprüfung der Prozesse, Rollen und Aufgaben (Massnahme B.10 Massnahmenkatalog)
BK-VE-R17 Wegfall Stimmkanal wegen fehlender Ressourcen				
28	Mittel	Minimieren	- Kurzfristig: Mitfinanzierung von Massnahmen, deren Kosten hauptsächlich von den (wenigen) betroffenen Kantonen getragen werden müssen, über die bestehenden Instrumente des Bundes (z.B. DVS) - Mittel- bis langfristig: Sicherstellen der langfristigen Finanzierung - Führen eines gemeinsamen Massnahmenplans von Bund und Kantonen	- Langfristige Überprüfung der Prozesse, Rollen und Aufgaben (Massnahme B.10 Massnahmenkatalog)

Score	Wahrsch.	Umgang	Aktuelle Massnahmen	Künftige Massnahmen
BK-VE-R18 Überschreitung der Limiten im Bundesrecht				
39	Tief	Minimieren	- Rechtliche Anforderungen: - Grundbewilligung des Bundesrates (Art. 27*a* und 27*c* VPR) - Ständiger Austausch mit den Kantonen - Begleitung der Versuche durch die BK	

Tabelle 5: Aktuelle und künftige Massnahmen, die für den Umgang mit den Risiken ergriffen werden.

6 Restrisiken

Restrisiken sind diejenigen Risiken, die nach der Umsetzung der in Kapitel 5 beschriebenen Massnahmen zur Risikominimierung verbleiben. Diese Risiken müssen explizit akzeptiert werden oder es müssen zusätzliche Beobachtungsmassnahmen umgesetzt werden, wenn sie aufgrund ihres Niveaus nicht akzeptiert werden können. Die folgende Tabelle enthält eine Zusammenfassung der Restrisiken.

Umgang	Restrisiko und Begründung	Score	Wahrsch.	Entscheid
BK-VE-R1 Erheblicher Sicherheitsmangel im System				
Minimieren	Zahlreiche Massnahmen werden ergriffen, um schwerwiegende Mängel nach Inbetriebnahme des Systems zu vermeiden. Ein Nullrisiko gibt es jedoch nicht. Die (kryptografischen, technischen und organisatorischen) Schutzmassnahmen bilden Schichten, die sich überlappen. Damit kann sichergestellt werden, dass ein Mangel in einer der Massnahmen nicht zwangsläufig dazu führt, dass Angriffe erfolgreich sind.	17	Tief	Wird akzeptiert
BK-VE-R2 Mangelnde Erkennung systematischer Fehler				
Minimieren	Die Kantone haben Rückmeldungen von Stimmberechtigten in ihre Prozesse integriert und verfügen über einen Vorgehensplan für den Fall eines solchen Vorfalls. Zudem sind der Abschluss einer Krisenvereinbarung und die Durchführung von Krisenübungen gute Instrumente zur entsprechenden Sensibilisierung. Es ist immer möglich, dass einzelne Kantone die Meldung von Ereignissen vergessen. Je mehr Kantone involviert sind, desto tiefer ist dieses Risiko. Die Stimmberechtigten werden in den ihnen zugestellten Informationen explizit aufgefordert, ihre Codes zu prüfen. Ausserdem werden sie aufgefordert, Fälle von falsch angezeigten Codes über einen zu diesem Zweck zur Verfügung gestellten Kanal zu melden. Damit kann verstärkt sichergestellt werden, dass allfällige Manipulationen aufgedeckt würden und dass betroffene Stimmberechtigte das Problem entdecken, bevor sie ihre Stimme definitiv abgeben. In diesem Fall können sie einen anderen Stimmkanal verwenden.	34	Tief	Wird beobachtet
BK-VE-R3 Mangelnde Akzeptanz von E-Voting				
Minimieren	Die Faktoren, die die Akzeptanz eines neuen Stimmkanals beeinflussen, sind ein eigenes Forschungsgebiet. Der jetzt vorgesehene, limitierte Versuchsbetrieb ermöglicht diese Forschung. Die Durchführung von limitierten Versuchen wird sowohl im Hinblick auf den Nutzen als auch auf die Auswirkungen auf die Urnengänge als sinnvoll erachtet. Die Versuche werden mit einem begrenzten Teil der Stimmberechtigten durchgeführt, was eine kontinuierliche Verbesserung der Prozesse und der Instrumente mit wissenschaftlicher Begleitung ermöglicht. Ausserdem sollte mit einer sachlichen Kommunikation ermöglicht werden, dass sich interessierte Personen ein objektives Bild der Situation machen können. Die Verifizierbarkeit trägt zudem wesentlich dazu bei, dass das Stimmgeheimnis gewahrt und zuverlässige Ergebnisse ermittelt werden können. Auch wenn entsprechende Massnahmen getroffen werden, kann es sein, dass die Digitalisierung des Prozesses zur Stimmabgabe für einen Teil der Stimmberechtigten unzumutbar ist. Jüngste Studien zeigen jedoch, dass	28	Tief	Wird beobachtet

Umgang	Restrisiko und Begründung	Score	Wahrsch.	Entscheid
	die Einführung eines elektronischen Stimmkanals durchaus gewünscht wird.[26]			
BK-VE-R4 Negativkampagne gegen E-Voting in (sozialen) Medien				
Minimieren	Mit einer kontinuierlichen, sachlichen und transparenten Kommunikation kann einer voreingenommenen Kommunikation am besten entgegengewirkt werden. Damit können zwar nicht bereits voreingenommene Personen überzeugt werden, aber es sollte ermöglicht werden, dass sich interessierte Personen ein objektives Bild der Situation machen können. In der Krisenvereinbarung werden verschiedene Aspekte der Kommunikation geregelt. Die Durchführung von Krisenübungen soll sicherstellen, dass im Krisenfall gemäss Vereinbarung vorgegangen wird.	17	Mittel	Wird akzeptiert
BK-VE-R5 Stimmenkauf über anonyme Plattform				
Minimieren	Das E-Voting-System stellt der stimmenden Person keinen Nachweis über ihre Stimmabgabe aus. So kann sie einem Käufer, der keinen (direkten oder indirekten [z.B. über Angestellte]) Zugang zum System hat, keinen Beweis für die gewünschte Stimmabgabe liefern. Der Käufer hat in einem solchen Fall also keine Garantie, dass die Stimme gemäss Kauf abgegeben wurde. Dies sollte ihn vom Stimmenkauf abhalten. Zusätzlich gibt es auch den Fall, dass eine stimmberechtigte Person direkt ihr zur Stimmabgabe notwendiges Material verkauft. Mit der Limitierung des zu E-Voting zugelassenen Elektorats sollte jedoch das Interesse an dieser Art von Angriffen verringert und auf jeden Fall die Tragweite eines solchen Angriffs eingeschränkt werden. Eine strafrechtliche Verfolgung von Wahlfälschung und -bestechung ist in jedem Fall möglich.	17	Mittel	Wird beobachtet
BK-VE-R6 Manipulation der Stimmen durch einen politisch motivierten Akteur mit hohen Ressourcen				
Minimieren	Um dieses Risiko zu vermeiden, werden verschiedene Massnahmen ergriffen. Insbesondere die Verifizierbarkeit verhindert, dass eine solche Manipulation unerkannt durchgeführt werden kann. Obwohl die Kryptografie, mit der die Verifizierbarkeit sichergestellt wird, von der Öffentlichkeit und von Expertinnen und Experten eingehend geprüft wird, besteht immer noch das Risiko eines Fehlers in der Konzeption oder in der Umsetzung der Kryptografie. Die Ausnutzung einer solchen Schwachstelle würde jedoch einen unverhältnismässig hohen Aufwand erfordern und, vor allem aufgrund der Limitierung des zugelassenen Elektorats, nur einen geringen Gewinn bringen. Darüber hinaus ist geplant, die Verifizierbarkeit und die Zusammenarbeit mit der Wissenschaft während der Versuchsphase zu stärken. Ausserdem werden die Druckereien aufgefordert, während und nach dem Druck Massnahmen zum Schutz der Codes	30	Tief	Wird akzeptiert

[26] Nationale E-Government-Studie 2022: Kurzbericht (https://www.digitale-verwaltung-schweiz.ch/application/files/6316/5216/3440/Nationale_E-Government-Studie_2022_Kurzbericht.pdf)

Deloitte Studie 2021 zur digitalen Verwaltung in der Schweiz: Die Treiber und Hürden von E-Government-Diensten (https://www2.deloitte.com/ch/de/pages/public-sector/articles/digital-government-study.html)

Schlussbericht zur Befragung «Digitalisierung und Politik Kanton Basel-Stadt» von 2020 (https://www.bs.ch/dam/jcr:96cfb1f0-96f8-4ec0-bbf1-3f566daa1247/2020-Bevoelkerungsbefragung-Digitalisierung-und-Politik-Kanton-Basel-Stadt.pdf)

Nationale E-Government-Studie 2019: Kurzbericht (https://www.digitale-verwaltung-schweiz.ch/application/files/8816/3895/8799/Nationale-E-Gov-Studie-2019-Kurzbericht.pdf)

Umgang	Restrisiko und Begründung	Score	Wahrsch.	Entscheid
	zu ergreifen, um einen Diebstahl der Codes zu verhindern. Zusammenfassend lässt sich festhalten, dass mit den umgesetzten Massnahmen – einschliesslich der Limitierung des zugelassenen Elektorats – erreicht werden kann, dass E-Voting zu einem wenig interessanten Angriffsziel für Angreifer wird, die die Ergebnisse manipulieren möchten. Der Aufwand für einen Angriff steht in keinem Verhältnis zur möglichen Wirkung. Hinzu kommt das Risiko des Angreifers, entdeckt zu werden.			
BK-VE-R7 Verletzung Stimmgeheimnis durch einen politisch motivierten Akteur mit hohen Ressourcen				
Minimieren	Es werden alle möglichen und zumutbaren Massnahmen ergriffen, um zu verhindern, dass eine einzige Person alle Informationen beschaffen kann, um das Stimmgeheimnis in grossem Ausmass zu brechen. Die Stimme könnte zwar immer noch mit einem direkten Angriff auf den Computer der stimmenden Person aufgedeckt werden (indem das Klickverhalten ausspioniert wird), aber das Bewusstsein der Bevölkerung für die Verwendung von elektronischen Geräten für sensible Vorgänge wird zunehmend geschärft. Es kann deshalb von den Benutzenden des elektronischen Stimmkanals erwartet werden, dass sie die Verantwortung dafür übernehmen, dass das von ihnen verwendete Gerät den gängigen Sicherheitsvorkehrungen entspricht. Je nachdem wie die Stimmberechtigten andere Mittel nutzen (z.B. soziale Medien), können diese zudem viel leichter Rückschlüsse darauf zulassen, ob und wie jemand abstimmt oder wählt. Die Limitierung des zugelassenen Elektorats dürfte das Interesse an dieser Art von Angriffen zusätzlich verringern.	20	Mittel	Wird akzeptiert
BK-VE-R8 Systemausfall infolge Angriff durch einen politisch motivierten Akteur mit hohen Ressourcen				
Minimieren	Die Infrastruktur des Systems muss gegen Denial-of-Service-Angriffe geschützt werden; die Infrastruktur der stimmenden Personen hingegen ist es nicht. Somit kann ein individueller Angriff nicht ausgeschlossen werden. Die Stimmabgabe an der Urne bleibt immer möglich. Die Möglichkeiten für Beeinflussungsaktionen durch politisch motivierten Akteuren beschränken sich nicht auf E-Voting und sind bereits Gegenstand von umfassenderen Überlegungen und Massnahmen.	17	Hoch	Wird beobachtet
BK-VE-R9 Unzulängliche Anforderungen				
Minimieren	Ein ständiger Dialog mit der Wissenschaft und Fachpersonen sowie die Teilnahme an Veranstaltungen zum Thema E-Voting sollten dazu beitragen, die Fachkenntnisse auf dem neusten Stand zu halten oder zumindest zu erkennen, sofern sie nicht angemessen sind. Auch die Beobachtung der Entwicklungen in verschiedenen Bereichen trägt zu diesem Ziel bei. Die technischen Anforderungen sind wohl am ehesten Gegenstand von Veränderungen. Indem diese Anforderungen in einer Verordnung der BK geregelt werden, wird eine grössere Flexibilität bei allfälligem Anpassungsbedarf erreicht.	30	Tief	Wird akzeptiert

Umgang	Restrisiko und Begründung	Score	Wahrsch.	Entscheid
BK-VE-R10 Zulassung eines mangelhaften Systems				
Minimieren	Mit der Durchführung von unabhängigen und öffentlichen Überprüfungen der Systeme und ihrer Betriebsmodalitäten können Schwachstellen zwar nicht vollständig ausgeschlossen werden. Jedoch handelt es sich dabei um wirksame Instrumente, um Schwachstellen möglichst zu verhindern. Da die Versuche mit der elektronischen Stimmabgabe nur in einem begrenzten Umfang durchgeführt werden, können die Auswirkungen von nicht vollständig erfüllten Anforderungen minimiert werden. Ausserdem werden kontinuierliche Verbesserungen der Prozesse und Instrumente ermöglicht. Darüber hinaus sollen die Massnahmen, die im Zusammenhang mit dem Monitoring und dem Management von Vorfällen getroffen werden, eine wirksame Untersuchung von allfälligen Vorfällen ermöglichen.	27	Tief	Wird akzeptiert
BK-VE-R11 Einsatz eines nicht zugelassenen Systems				
Minimieren	Mit den Anforderungen an eine zuverlässige und nachvollziehbare Kompilierung und an ein zuverlässiges und nachvollziehbares Deployment wird sichergestellt, dass das effektiv eingesetzte System dem geprüften System entspricht. Damit kann jedoch ein böswilliger Eingriff nach der Installation nicht ausgeschlossen werden. Da die Zugriffe kontrolliert und die entsprechenden Daten gesammelt werden, sollte ein solcher Eingriff jedoch entdeckt werden können.	44	Tief	Wird beobachtet
BK-VE-R12 Gefährdung Weiterentwicklung Sicherheitsanforderungen				
Minimieren	Durch die Förderung und Finanzierung der Forschung wird das Interesse an E-Voting aufrechterhalten. Dies gilt auch für den Einbezug und die Zusammenarbeit mit der Wissenschaft. Ausserdem ermöglicht das Beobachten der Entwicklungen in verschiedenen Bereichen, von Fortschritten zu profitieren, die ausserhalb des Wirkungsfelds der BK gemacht werden.	18	Tief	Wird akzeptiert
BK-VE-R13 Mangel an unabhängigen Expertinnen und Experten				
Minimieren	Die Teilnahme an Veranstaltungen zum Thema E-Voting bietet der BK die Möglichkeit, sich einen Überblick über die Expertinnen und Experten auf diesem Gebiet und über ihre Kompetenzen zu verschaffen. Damit kann jedoch nicht garantiert werden, dass sich diese Expertinnen und Experten bereit erklären, bei der Durchführung von unabhängigen Überprüfungen von E-Voting-Systemen mitzuwirken.	32	Tief	Wird beobachtet
BK-VE-R14 Neue Technologien führen zu Verletzung Stimmgeheimnis				
Beobachten	Die Zukunft lässt sich nicht vorhersagen. Dieses Risiko kann nicht weiter minimiert werden, als dass die technologischen Entwicklungen beobachtet und Massnahmen ergriffen werden, sobald diese verfügbar und notwendig sind.	35	Tief	Wird beobachtet
BK-VE-R15 Systemausfall während Urnengang				
Minimieren	Die Krisenvereinbarung sieht einen solchen Fall vor und bietet Lösungsansätze für diese Problematik. Damit kann dieses Risiko jedoch nicht vollständig ausgeschlossen werden. Die Tatsache, dass momentan die Post – und damit ein Unternehmen in öffentlicher Hand	30	Tief	Wird akzeptiert

Umgang	Restrisiko und Begründung	Score	Wahrsch.	Entscheid
	– Systemanbieterin ist, bietet jedoch eine starke Sicherheit in diesem Bereich.			
BK-VE-R16 Wegfall Stimmkanal wegen unzureichender Zusammenarbeit				
Minimieren	Da der Bund bei den Verträgen zwischen den Kantonen und ihren Dienstleistern nicht Vertragspartei ist, kann er auf dieser Ebene nicht tätig werden. Im Rahmen von Projektgremien, in denen die verschiedenen Akteure vertreten sind, können mögliche Schwierigkeiten antizipiert und diskutiert werden. Schliesslich können auch mit der finanziellen Beteiligung des Bundes an den Umsetzungskosten der Kantone einige dieser Herausforderungen gemildert werden.	23	Tief	Wird akzeptiert
BK-VE-R17 Wegfall Stimmkanal wegen fehlender Ressourcen				
Minimieren	E-Voting ist Teil des Umsetzungsplans der DVS. In diesem Rahmen werden die Kantone bei der Einführung von E-Voting unterstützt. Mit einer langfristigen Überprüfung der Rollen und Aufgaben könnten die Kantone potentiell entlastet werden.	28	Tief	Wird akzeptiert
BK-VE-R18 Überschreitung der Limiten im Bundesrecht				
Minimieren	Die Kantone sind für die Durchführung von eidgenössischen Urnengängen und damit für alle Stimmkanäle zuständig. Sie treffen die notwendigen Massnahmen, um den Zugang zum elektronischen Stimmkanal zu kontrollieren (z.B. vorgängiges Anmeldeverfahren, Einschränkung auf Stimmberechtigte bestimmter Gemeinden). Die Zulassungs- und Bewilligungsverfahren ermöglichen die Einhaltung der Limite auf nationaler Ebene.	27	Tief	Wird akzeptiert

Tabelle 6: Restrisiken und endgültige Entscheidung.

Wahrscheinlichkeit	Auswirkungen (Risiko-Score) 32 – 49 (Hoch)	22 – 31 (Mittel)	17 – 21 (Tief)
Hoch			**R8** Systemausfall infolge Angriff durch einen politisch motivierten Akteur mit hohen Ressourcen
Mittel			**R4** Negativkampagne gegen E-Voting in (sozialen) Medien **R5** Stimmenkauf über anonyme Plattform **R7** Verletzung Stimmgeheimnis durch einen politisch motivierten Akteur mit hohen Ressourcen
Tief	**R2** Mangelnde Erkennung systematischer Fehler **R11** Einsatz eines nicht zugelassenen Systems **R13** Mangel an unabhängigen Expertinnen und Experten **R14** Neue Technologien führen zu Verletzung Stimmgeheimnis	**R3** Mangelnde Akzeptanz von E-Voting **R6** Manipulation der Stimmen durch einen politisch motivierten Akteur mit hohen Ressourcen **R9** Unzulängliche Anforderungen **R10** Zulassung eines mangelhaften Systems **R15** Systemausfall während Urnengang **R16** Wegfall Stimmkanal wegen unzureichender Zusammenarbeit **R17** Wegfall Stimmkanal wegen fehlender Ressourcen **R18** Überschreitung der Limiten im Bundesrecht	**R1** Erheblicher Sicherheitsmangel im System **R12** Gefährdung Weiterentwicklung Sicherheitsanforderungen

Tabelle 7: Übersicht der Restrisiken, die nach der Umsetzung von Minimierungsmassnahmen verbleiben.

Durch die Bundeskanzlei genehmigt:

Walter Thurnherr, Bundeskanzler

Unterschrift: .....

Barbara Perriard, Leiterin Sektion Politische Rechte

Unterschrift: .....

Aurore Borer, Teilprojektleiterin Vote électronique

Unterschrift: i.V. .....

Anhang I Detaillierte Analyse der Risiken

BK-VE-R1 Erheblicher Sicherheitsmangel im System

Bedrohung	Ein erheblicher Sicherheitsmangel, der das System betrifft, wird während eines Urnengangs entdeckt.
Sicherheitsziele *(Art. 4 Abs. 3 VEleS)*	a. Korrektheit des Ergebnisses b. Wahrung des Stimmgeheimnisses und Ausschluss von vorzeitigen Teilergebnissen
Auswirkungen	Der elektronische Stimmkanal muss ausgesetzt und eine Untersuchung durchgeführt werden, um festzustellen, welche Auswirkungen der Sicherheitsmangel hat und ob er ausgenutzt wurde. Wenn der Sicherheitsmangel ausgenutzt wurde und nicht nachgewiesen werden kann, welche Stimmen manipuliert wurden und welche nicht, dürfen keine der elektronisch abgegebenen Stimmen berücksichtigt werden. Wenn das Ergebnis des Urnengangs aufgrund dieser Stimmen hätte anders ausfallen können, könnte eine Beschwerde zur Aufhebung des Urnengangs führen. Die Reputation der Behörden wäre stark beeinträchtigt. Die Versuche mit der elektronischen Stimmabgabe könnten eingestellt werden.

Evaluation

	Ersteinschätzung		**Nach der Minimierung**	
Wahrscheinlichkeit	Mittel		Tief	
Kriterien	**Wert**	**Score**	**Wert**	**Score**
Reputation und Vertrauen	Hoch (3)	15	Tief (1)	5
Rechtliches	Hoch (3)	15	Tief (1)	5
Kontinuität	Mittel (2)	6	Tief (1)	3
Finanzen	Tief (1)	3	Tief (1)	3
Produktivität	Tief (1)	1	Tief (1)	1
Risiko-Score		**40**		**17**

BK-VE-R2 Mangelnde Erkennung systematischer Fehler

Bedrohung	In mehreren Kantonen werden falsch angezeigte Prüfcodes gemeldet, aber aufgrund einer fehlenden Koordination zwischen den Kantonen und der BK erfolgt auf nationaler Ebene keine Alarmierung.
Sicherheitsziele *(Art. 4 Abs. 3 VEleS)*	a. Korrektheit des Ergebnisses
Auswirkungen	Da das Problem nicht erkannt werden konnte, konnten die notwendigen Untersuchungen nicht rechtzeitig eingeleitet und die Stimmberechtigten nicht zusätzlich über die besondere Wichtigkeit der Überprüfung der Prüfcodes sensibilisiert werden. Stimmende Personen, die ihre Prüfcodes nicht überprüft hatten, konnten eine Stimme definitiv abgeben, die nicht ihrer Absicht entsprach. Die nicht manipulierten können nicht von den manipulierten Stimmen unterschieden werden, weshalb keine der elektronisch abgegebenen Stimmen berücksichtigt werden dürfen. Wenn das Ergebnis des Urnengangs aufgrund dieser Stimmen hätte anders ausfallen können, könnte eine Beschwerde zur Aufhebung des Urnengangs führen. Die Reputation der Behörden wäre stark beeinträchtigt. Die Versuche mit der elektronischen Stimmabgabe könnten eingestellt werden.

Evaluation

	Ersteinschätzung		**Nach der Minimierung**	
Wahrscheinlichkeit	Mittel		Tief	
Kriterien	**Wert**	**Score**	**Wert**	**Score**
Reputation und Vertrauen	Hoch (3)	15	Mittel (2)	10
Rechtliches	Hoch (3)	15	Mittel (2)	10
Kontinuität	Mittel (2)	6	Mittel (2)	6
Finanzen	Mittel (2)	6	Mittel (2)	6
Produktivität	Mittel (2)	2	Mittel (2)	2
Risiko-Score		**44**		**34**

BK-VE-R3 Mangelnde Akzeptanz von E-Voting

Bedrohung	Der elektronische Stimmkanal wird nicht ausreichend akzeptiert.
Sicherheitsziele *(Art. 4 Abs. 3 VEleS)*	a. Korrektheit des Ergebnisses
Auswirkungen	Entweder wird der elektronische Stimmkanal einfach nicht genutzt oder er wird genutzt, aber ein grosser Teil der Bevölkerung akzeptiert die Ergebnisse des Stimmkanals nicht.

Evaluation

	Ersteinschätzung		**Nach der Minimierung**	
Wahrscheinlichkeit	Mittel		Tief	
Kriterien	**Wert**	**Score**	**Wert**	**Score**
Reputation und Vertrauen	Hoch (3)	15	Mittel (2)	10
Rechtliches	Tief (1)	5	Tief (1)	5
Kontinuität	Hoch (3)	9	Hoch (3)	9
Finanzen	Tief (1)	3	Tief (1)	3
Produktivität	Tief (1)	1	Tief (1)	1
Risiko-Score		**33**		**28**

BK-VE-R4 Negativkampagne gegen E-Voting in (sozialen) Medien

Bedrohung	In den Medien oder in sozialen Netzwerken wird eine Kampagne gegen den elektronischen Stimmkanal geführt. Diese kann auf Ereignissen rund um die elektronische Stimmabgabe im Ausland, auf angeblich fehlenden öffentlichen Kontrollmöglichkeiten, auf falschen Behauptungen über die Verifizierbarkeit oder auf einer mangelhaften Kommunikation der Behörden beruhen.
Sicherheitsziele *(Art. 4 Abs. 3 VEleS)*	a. Korrektheit des Ergebnisses
Auswirkungen	Während eines laufenden Urnengangs könnte das Vertrauen der Stimmberechtigten stark sinken und sie von der Nutzung des elektronischen Stimmkanals abhalten. Ausserdem könnte eine schlechte Kommunikation die Glaubwürdigkeit der Behörden beeinträchtigen. Schliesslich besteht die Möglichkeit von Beschwerden.

Evaluation

	Ersteinschätzung		**Nach der Minimierung**	
Wahrscheinlichkeit	Hoch		Mittel	
Kriterien	**Wert**	**Score**	**Wert**	**Score**
Reputation und Vertrauen	Mittel (2)	10	Tief (1)	5
Rechtliches	Tief (1)	5	Tief (1)	5
Kontinuität	Mittel (2)	6	Tief (1)	3
Finanzen	Mittel (2)	6	Tief (1)	3
Produktivität	Mittel (2)	2	Tief (1)	1
Risiko-Score		**29**		**17**

BK-VE-R5 Stimmenkauf über anonyme Plattform

Bedrohung	Eine Gruppe, die über eine anonyme Kaufplattform verfügt, lanciert eine grossangelegte Kampagne zum Stimmenkauf.
Sicherheitsziele *(Art. 4 Abs. 3 VEleS)*	a. Korrektheit des Ergebnisses b. Wahrung des Stimmgeheimnisses und Ausschluss von vorzeitigen Teilergebnissen f. keine missbräuchliche Verwendung von Beweisen zum Stimmverhalten
Auswirkungen	Die Plattform ermöglicht einen anonymen Verkauf, so dass es schwierig ist, die Personen zu identifizieren, die ihre Stimme verkauft haben. Ausserdem ist es nicht möglich, die betroffenen Stimmen in der Urne zu identifizieren, weshalb keine der elektronisch abgegebenen Stimmen berücksichtigt werden dürfen. Wenn das Ergebnis des Urnengangs aufgrund dieser Stimmen hätte anders ausfallen können, könnte eine Beschwerde zur Aufhebung des Urnengangs führen. Die Reputation der Behörden wäre stark beeinträchtigt. Die Versuche mit der elektronischen Stimmabgabe würden höchstwahrscheinlich eingestellt werden.

Evaluation

	Ersteinschätzung		**Nach der Minimierung**	
Wahrscheinlichkeit	Mittel		Mittel	
Kriterien	**Wert**	**Score**	**Wert**	**Score**
Reputation und Vertrauen	Hoch (3)	15	Tief (1)	5
Rechtliches	Hoch (3)	15	Tief (1)	5
Kontinuität	Hoch (3)	9	Tief (1)	3
Finanzen	Tief (1)	3	Tief (1)	3
Produktivität	Tief (1)	1	Tief (1)	1
Risiko-Score		**43**		**17**

BK-VE-R6 Manipulation der Stimmen durch einen politisch motivierten Akteur mit hohen Ressourcen

Bedrohung	Einen politisch motivierten Akteur mit hohen Ressourcenmobilisiert seine Ressourcen und es gelingt ihm, Stimmen im System zu manipulieren.
Sicherheitsziele *(Art. 4 Abs. 3 VEleS)*	a. Korrektheit des Ergebnisses
Auswirkungen	Der elektronische Stimmkanal müsste eingestellt und eine Untersuchung durchgeführt werden, um festzustellen, welche Stimmen manipuliert wurden und welche nicht. Ist dies nicht möglich, dürfen keine der elektronisch abgegebenen Stimmen berücksichtigt werden. Wenn das Ergebnis des Urnengangs aufgrund dieser Stimmen hätte anders ausfallen können, könnte eine Beschwerde zur Aufhebung des Urnengangs führen. Die Reputation der Behörden wäre stark beeinträchtigt. Die Versuche mit der elektronischen Stimmabgabe würden höchstwahrscheinlich eingestellt werden. Wenn die Manipulation nicht entdeckt wird, könnte eine Entscheidung getroffen worden sein, die nicht dem Willen der Bevölkerung entspricht.

Evaluation

	Ersteinschätzung		**Nach der Minimierung**	
Wahrscheinlichkeit	Mittel		Tief	
Kriterien	**Wert**	**Score**	**Wert**	**Score**
Reputation und Vertrauen	Hoch (3)	15	Mittel (2)	10
Rechtliches	Hoch (3)	15	Mittel (2)	10
Kontinuität	Hoch (3)	9	Mittel (2)	6
Finanzen	Tief (1)	3	Tief (1)	3
Produktivität	Tief (1)	1	Tief (1)	1
Risiko-Score		**43**		**30**

BK-VE-R7 Verletzung Stimmgeheimnis durch einen politisch motivierten Akteur mit hohen Ressourcen

Bedrohung	Einen politisch motivierten Akteur mit hohen Ressourcen mobilisiert seine Ressourcen und es gelingt ihm, das Stimmgeheimnis zu brechen.
Sicherheitsziele *(Art. 4 Abs. 3 VEleS)*	b. Wahrung des Stimmgeheimnisses und Ausschluss von vorzeitigen Teilergebnissen f. keine missbräuchliche Verwendung von Beweisen zum Stimmverhalten
Auswirkungen	Der betreffende Akteur kann diese Informationen kurz- oder langfristig gegen die stimmenden Personen verwenden. Er kann die Informationen auch an Staaten oder an kriminelle Gruppierungen verkaufen, die sie dann zum Nachteil der stimmenden Personen verwenden können. Die Angelegenheit wird öffentlich bekannt und das Vertrauen in den elektronischen Stimmkanal und in die Behörden wird schwer beeinträchtigt. Die Versuche mit der elektronischen Stimmabgabe müssten eingestellt werden.

Evaluation

	Ersteinschätzung		**Nach der Minimierung**	
Wahrscheinlichkeit	Mittel		Mittel	
Kriterien	**Wert**	**Score**	**Wert**	**Score**
Reputation und Vertrauen	Hoch (3)	15	Tief (1)	5
Rechtliches	Mittel (2)	10	Tief (1)	5
Kontinuität	Hoch (3)	9	Mittel (2)	6
Finanzen	Tief (1)	3	Tief (1)	3
Produktivität	Tief (1)	1	Tief (1)	1
Risiko-Score		**38**		**20**

BK-VE-R8 Systemausfall infolge Angriff durch einen politisch motivierten Akteur mit hohen Ressourcen

Bedrohung	Einen politisch motivierten Akteur mit hohen Ressourcenmobilisiert seine Ressourcen und es gelingt ihm, das Ergebnis des Urnengangs zu beeinflussen, indem Stimmberechtigte von der Stimmabgabe abgehalten werden.
Sicherheitsziele *(Art. 4 Abs. 3 VEleS)*	a. Korrektheit des Ergebnisses c. Erreichbarkeit und Funktionsfähigkeit des Stimmkanals
Auswirkungen	Angriffe können dazu führen, dass das System für alle oder für einen Teil der Stimmberechtigten nicht verfügbar ist, und sie dadurch von der Stimmabgabe ausgeschlossen werden. Die Auslandschweizer Stimmberechtigten können ihre Stimme nicht mehr rechtzeitig abgeben. Dies kann dazu führen, dass die Ergebnisse des Urnengangs angefochten werden. E-Voting wird wahrscheinlich in Frage gestellt, da eine der Zielgruppen von dem Angriff besonders betroffen war.

Evaluation

	Ersteinschätzung		**Nach der Minimierung**	
Wahrscheinlichkeit	Hoch		Hoch	
Kriterien	**Wert**	**Score**	**Wert**	**Score**
Reputation und Vertrauen	Mittel (2)	10	Tief (1)	5
Rechtliches	Mittel (2)	10	Tief (1)	5
Kontinuität	Mittel (2)	6	Tief (1)	3
Finanzen	Tief (1)	3	Tief (1)	3
Produktivität	Mittel (2)	2	Tief (1)	1
Risiko-Score		**31**		**17**

BK-VE-R9 Unzulängliche Anforderungen

Bedrohung	Die bundesrechtlichen Anforderungen sind unzulänglich und das gewünschte Sicherheitsniveau kann damit nicht aufrechterhalten werden.
Sicherheitsziele *(Art. 4 Abs. 3 VEleS)*	a. Korrektheit des Ergebnisses b. Wahrung des Stimmgeheimnisses und Ausschluss von vorzeitigen Teilergebnissen c. Erreichbarkeit und Funktionsfähigkeit des Stimmkanals d. Schutz der persönlichen Informationen über die stimmberechtigten Personen e. Schutz der für die stimmberechtigten Personen bestimmten Informationen vor Manipulationen f. keine missbräuchliche Verwendung von Beweisen zum Stimmverhalten
Auswirkungen	Das System und dessen Betrieb könnten leichter beeinträchtigt werden und die Kritik würde in der Öffentlichkeit und in den Medien sicherlich zunehmen. Die Reputation der Behörden würde stark beeinträchtigt und die Fortsetzung der Versuche in Frage gestellt werden.

Evaluation

	Ersteinschätzung		**Nach der Minimierung**	
Wahrscheinlichkeit	Tief		Tief	
Kriterien	**Wert**	**Score**	**Wert**	**Score**
Reputation und Vertrauen	Hoch (3)	15	Mittel (2)	10
Rechtliches	Hoch (3)	15	Mittel (2)	10
Kontinuität	Mittel (2)	6	Mittel (2)	6
Finanzen	Tief (1)	3	Tief (1)	3
Produktivität	Tief (1)	1	Tief (1)	1
Risiko-Score		**40**		**30**

BK-VE-R10 Zulassung eines mangelhaften Systems

Bedrohung	Der Bund hat ein System zugelassen, das die bundesrechtlichen Sicherheitsanforderungen nicht erfüllt.
Sicherheitsziele *(Art. 4 Abs. 3 VEleS)*	a. Korrektheit des Ergebnisses b. Wahrung des Stimmgeheimnisses und Ausschluss von vorzeitigen Teilergebnissen c. Erreichbarkeit und Funktionsfähigkeit des Stimmkanals d. Schutz der persönlichen Informationen über die stimmberechtigten Personen e. Schutz der für die stimmberechtigten Personen bestimmten Informationen vor Manipulationen f. keine missbräuchliche Verwendung von Beweisen zum Stimmverhalten
Auswirkungen	Wenn eine missbräuchliche Verwendung des Systems nicht ausgeschlossen werden kann und das Ergebnis des Urnengangs aufgrund der elektronisch abgegebenen Stimmen hätte anders ausfallen können, muss der Urnengang höchstwahrscheinlich aufgehoben werden. Die Reputation der Behörden wäre stark beeinträchtigt. Die Versuche mit der elektronischen Stimmabgabe müssten eingestellt werden.

Evaluation

	Ersteinschätzung		**Nach der Minimierung**	
Wahrscheinlichkeit	Mittel		Tief	
Kriterien	**Wert**	**Score**	**Wert**	**Score**
Reputation und Vertrauen	Hoch (3)	15	Mittel (2)	10
Rechtliches	Hoch (3)	15	Mittel (2)	10
Kontinuität	Hoch (3)	9	Tief (1)	3
Finanzen	Mittel (2)	6	Tief (1)	3
Produktivität	Mittel (2)	2	Tief (1)	1
Risiko-Score		**47**		**27**

BK-VE-R11 Einsatz eines nicht zugelassenen Systems

Bedrohung	Es wird ein System eingesetzt, das nicht dem zugelassenen System entspricht.
Sicherheitsziele *(Art. 4 Abs. 3 VEleS)*	a. Korrektheit des Ergebnisses b. Wahrung des Stimmgeheimnisses und Ausschluss von vorzeitigen Teilergebnissen c. Erreichbarkeit und Funktionsfähigkeit des Stimmkanals d. Schutz der persönlichen Informationen über die stimmberechtigten Personen e. Schutz der für die stimmberechtigten Personen bestimmten Informationen vor Manipulationen f. keine missbräuchliche Verwendung von Beweisen zum Stimmverhalten
Auswirkungen	Das System wäre nicht von einer unabhängigen Stelle oder von der Öffentlichkeit überprüft worden. Somit kann nicht gewährleistet werden, dass es keine Sicherheitsmängel gibt. Wenn das Ergebnis des Urnengangs aufgrund der elektronisch abgegebenen Stimmen hätte anders ausfallen können, könnte eine Beschwerde zur Aufhebung des Urnengangs führen. Die Reputation der Behörden wäre stark beeinträchtigt.

Evaluation

	Ersteinschätzung		**Nach der Minimierung**	
Wahrscheinlichkeit	Mittel		Tief	
Kriterien	**Wert**	**Score**	**Wert**	**Score**
Reputation und Vertrauen	Hoch (3)	15	Hoch (3)	15
Rechtliches	Hoch (3)	15	Hoch (3)	15
Kontinuität	Mittel (2)	6	Mittel (2)	6
Finanzen	Mittel (2)	6	Mittel (2)	6
Produktivität	Mittel (2)	2	Mittel (2)	2
Risiko-Score		**44**		**44**

BK-VE-R12 Gefährdung Weiterentwicklung Sicherheitsanforderungen

Bedrohung	Ein fehlendes Interesse von Expertinnen und Experten im Bereich von Vote électronique führt dazu, dass die Sicherheitsanforderungen nicht weiterentwickelt werden und sie nicht mehr den aktuellen Kenntnisstand abbilden.
Sicherheitsziele *(Art. 4 Abs. 3 VEleS)*	a. Korrektheit des Ergebnisses b. Wahrung des Stimmgeheimnisses und Ausschluss von vorzeitigen Teilergebnissen c. Erreichbarkeit und Funktionsfähigkeit des Stimmkanals d. Schutz der persönlichen Informationen über die stimmberechtigten Personen e. Schutz der für die stimmberechtigten Personen bestimmten Informationen vor Manipulationen f. keine missbräuchliche Verwendung von Beweisen zum Stimmverhalten
Auswirkungen	Die Expertinnen und Experten würden keine weitere Forschung zum Thema E-Voting betreiben und möchten nicht mehr in die Arbeiten einbezogen werden. Die Versuche mit der elektronischen Stimmabgabe könnten nicht unter guten Bedingungen weitergeführt und müssten höchstwahrscheinlich eingestellt werden.

Evaluation

	Ersteinschätzung		**Nach der Minimierung**	
Wahrscheinlichkeit	Mittel		Tief	
Kriterien	**Wert**	**Score**	**Wert**	**Score**
Reputation und Vertrauen	Mittel (2)	10	Tief (1)	5
Rechtliches	Mittel (2)	10	Tief (1)	5
Kontinuität	Hoch (3)	9	Tief (1)	3
Finanzen	Hoch (3)	9	Tief (1)	3
Produktivität	Mittel (2)	2	Mittel (2)	2
Risiko-Score		**40**		**18**

BK-VE-R13 Mangel an unabhängigen Expertinnen und Experten

Bedrohung	Für die Durchführung von Überprüfungen mangelt es an qualifizierten unabhängigen Expertinnen und Experten.
Sicherheitsziele *(Art. 4 Abs. 3 VEleS)*	a. Korrektheit des Ergebnisses b. Wahrung des Stimmgeheimnisses und Ausschluss von vorzeitigen Teilergebnissen c. Erreichbarkeit und Funktionsfähigkeit des Stimmkanals d. Schutz der persönlichen Informationen über die stimmberechtigten Personen e. Schutz der für die stimmberechtigten Personen bestimmten Informationen vor Manipulationen f. keine missbräuchliche Verwendung von Beweisen zum Stimmverhalten
Auswirkungen	Die Überprüfung der Systeme müsste aufgeschoben werden und ein möglicher Einsatz würde verzögert. Langfristig könnte dies die Kantone und Systemanbieter von ihren Vorhaben abbringen und die Versuche mit der elektronischen Stimmabgabe damit zum Stillstand bringen.

Evaluation

	Ersteinschätzung		**Nach der Minimierung**	
Wahrscheinlichkeit	Mittel		Tief	
Kriterien	**Wert**	**Score**	**Wert**	**Score**
Reputation und Vertrauen	Mittel (2)	10	Mittel (2)	10
Rechtliches	Tief (1)	5	Tief (1)	5
Kontinuität	Mittel (2)	6	Mittel (2)	6
Finanzen	Hoch (3)	9	Hoch (3)	9
Produktivität	Mittel (2)	2	Mittel (2)	2
Risiko-Score		**32**		**32**

BK-VE-R14 Neue Technologien führen zu Verletzung Stimmgeheimnis

Bedrohung	Eine neue Technologie verbreitet sich und führt dazu, dass die Sicherheitsanforderungen für die Wahrung des Stimmgeheimnisses nicht mehr ausreichen (z.B. Quantencomputer).
Sicherheitsziele *(Art. 4 Abs. 3 VEleS)*	b. Wahrung des Stimmgeheimnisses und Ausschluss von vorzeitigen Teilergebnissen
Auswirkungen	Das System und sein Betrieb könnten leichter beeinträchtigt werden und die Kritik würde in der Öffentlichkeit und in den Medien sicherlich zunehmen. Die Reputation der Behörden würde stark beeinträchtigt und die Fortsetzung der Versuche in Frage gestellt werden.

Evaluation

	Ersteinschätzung		**Nach der Minimierung**
Wahrscheinlichkeit	Tief		Keine Veränderung, da das Risiko überwacht wird, ohne dass weitere Massnahmen ergriffen werden.
Kriterien	**Wert**	**Score**	
Reputation und Vertrauen	Mittel (2)	10	
Rechtliches	Hoch (3)	15	
Kontinuität	Mittel (2)	6	
Finanzen	Tief (1)	3	
Produktivität	Tief (1)	1	
Risiko-Score		**35**	

BK-VE-R15 Systemausfall während Urnengang

Bedrohung	Der Systemanbieter ist während eines Urnengangs nicht mehr in der Lage, sein System zur Verfügung zu stellen, obwohl bereits Stimmen abgegeben wurden.
Sicherheitsziele *(Art. 4 Abs. 3 VEleS)*	a. Korrektheit des Ergebnisses c. Erreichbarkeit und Funktionsfähigkeit des Stimmkanals
Auswirkungen	Die elektronisch abgegebenen Stimmen sind endgültig verloren. Wenn das Ergebnis des Urnengangs aufgrund dieser Stimmen hätte anders ausfallen können, könnte eine Beschwerde zur Aufhebung des Urnengangs führen. Die Reputation der Behörden wäre stark beeinträchtigt. Die Versuche mit der elektronischen Stimmabgabe könnten eingestellt werden.

Evaluation

	Ersteinschätzung		**Nach der Minimierung**	
Wahrscheinlichkeit	Tief		Tief	
Kriterien	**Wert**	**Score**	**Wert**	**Score**
Reputation und Vertrauen	Hoch (3)	15	Mittel (2)	10
Rechtliches	Hoch (3)	15	Mittel (2)	10
Kontinuität	Mittel (2)	6	Mittel (2)	6
Finanzen	Tief (1)	3	Tief (1)	3
Produktivität	Tief (1)	1	Tief (1)	1
Risiko-Score		**40**		**30**

BK-VE-R16 Wegfall Stimmkanal wegen unzureichender Zusammenarbeit

Bedrohung	Streitigkeiten zwischen den Behörden und der Post stören die Zusammenarbeit derart stark, dass der elektronische Stimmkanal nicht mehr weiterentwickelt werden kann oder unterbrochen werden muss.
Sicherheitsziele *(Art. 4 Abs. 3 VEleS)*	c. Erreichbarkeit und Funktionsfähigkeit des Stimmkanals
Auswirkungen	Die Versuche mit der elektronischen Stimmabgabe wären nicht mehr möglich.

Evaluation

	Ersteinschätzung		**Nach der Minimierung**	
Wahrscheinlichkeit	Mittel		Tief	
Kriterien	**Wert**	**Score**	**Wert**	**Score**
Reputation und Vertrauen	Tief (1)	5	Tief (1)	5
Rechtliches	Tief (1)	5	Tief (1)	5
Kontinuität	Hoch (3)	9	Hoch (3)	9
Finanzen	Tief (1)	3	Tief (1)	3
Produktivität	Tief (1)	1	Tief (1)	1
Risiko-Score		**23**		**23**

BK-VE-R17 Wegfall Stimmkanal wegen fehlender Ressourcen

Bedrohung	Den Kantonen fehlen die Ressourcen für die Umsetzung des elektronischen Stimmkanals.
Sicherheitsziele *(Art. 4 Abs. 3 VEleS)*	c. Erreichbarkeit und Funktionsfähigkeit des Stimmkanals
Auswirkungen	Die Kantone würden ihre Vorhaben zum Einsatz der elektronischen Stimmabgabe aufgeben und die Versuche würden dadurch eingestellt.

Evaluation

	Ersteinschätzung		**Nach der Minimierung**	
Wahrscheinlichkeit	Mittel		Tief	
Kriterien	**Wert**	**Score**	**Wert**	**Score**
Reputation und Vertrauen	Mittel (2)	10	Mittel (2)	10
Rechtliches	Tief (1)	5	Tief (1)	5
Kontinuität	Hoch (3)	9	Hoch (3)	9
Finanzen	Tief (1)	3	Tief (1)	3
Produktivität	Tief (1)	1	Tief (1)	1
Risiko-Score		**28**		**28**

BK-VE-R18 Überschreitung der Limiten im Bundesrecht

Bedrohung	Die tatsächliche Nutzung des elektronischen Stimmkanals übersteigt die Limitierung des zugelassenen Elektorats (30 % kantonal und 10 % national).
Sicherheitsziele *(Art. 4 Abs. 3 VEleS)*	a. Korrektheit des Ergebnisses
Auswirkungen	Wenn das Ergebnis des Urnengangs aufgrund dieser Stimmen hätte anders ausfallen können, könnte eine Beschwerde zur Aufhebung des Urnengangs führen. Die Reputation der Behörden wäre mittelschwer beeinträchtigt. Die Versuche mit der elektronischen Stimmabgabe könnten eingestellt werden.

Evaluation

	Ersteinschätzung		**Nach der Minimierung**	
Wahrscheinlichkeit	Tief		Tief	
Kriterien	**Wert**	**Score**	**Wert**	**Score**
Reputation und Vertrauen	Mittel (2)	10	Mittel (2)	10
Rechtliches	Hoch (3)	15	Mittel (2)	10
Kontinuität	Mittel (2)	6	Tief (1)	3
Finanzen	Mittel (2)	6	Tief (1)	3
Produktivität	Mittel (2)	2	Tief (1)	1
Risiko-Score		**39**		**27**