Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundeskanzlei BK

Sektion Politische Rechte

Dialog mit der Wissenschaft 2020

Management Summary zur Zusammenfassung

1. Hintergrund und Vorgehen

Im Rahmen des Auftrags des Bundesrats vom 26. Juni 2019 hat die Bundeskanzlei (BK) unter Mitwirkung verschiedener Kantone einen Dialog mit der Wissenschaft geführt. Der Dialog hatte zum Ziel, der Unterarbeitsgruppe von Bund und Kantonen als Grundlage für die Erarbeitung von Empfehlungen zu dienen. Die BK hat mit 23 Expertinnen und Experten aus Forschung und Industrie Fragen rund um die elektronische Stimmabgabe erörtert.[1] Der Dialog hatte einen technischen Fokus. Die meisten Expertinnen und Experten verfügten über einen Hintergrund in einem Bereich der exakten Wissenschaften, drei Experten hatten einen gesellschaftswissenschaftlichen Hintergrund.

Zunächst hat die BK den Expertinnen und Experten am 14. Februar 2020 einen Fragebogen mit rund 60 Fragen unterbreitet.[2] Ausgehend von den Antworten hat sie vom 5. Mai bis zum 17. Juli 2020 einen moderierten schriftlichen Online-Dialog durchgeführt. Zu jedem Diskussionsblock hat der Moderator den an der Diskussion beteiligten Expertinnen und Experten eine Zusammenfassung unterbreitet. Die Zusammenfassung zu den Diskussionsblöcken sowie die Zusammenfassung der Antworten auf den Fragebogen sind im Hauptdokument «Summary of the Expert Dialog» enthalten.

2. Allgemeine Einschätzung

Die Expertinnen und Experten sehen Handlungsbedarf bei der Sicherheit, der Transparenz sowie der unabhängigen Prüfung. Gleichzeitig vertreten die Expertinnen und Experten die Ansicht, dass während der letzten 15 Jahre wertvolle Ergebnisse erzielt wurden. Sie empfehlen, Fragen der Sicherheit auch bei den übrigen Stimmkanälen zu analysieren. Fragen der Vertrauensbildung sind weiter zu vertiefen.

Die Expertinnen und Experten unterstreichen die Wichtigkeit, Fachpersonen – namentlich aus der Wissenschaft – bei der Konzeption, der Entwicklung und der Prüfung von E-Voting Systemen laufend einzubeziehen. Die Beauftragung eines wissenschaftlichen Komitees wurde verschiedentlich angeregt.

3. Bereitstellung eines sicheren Systems

3.1 Behörden sollen weiterhin die Sicherheit vorgeben

Es soll nach Ansicht der Expertinnen und Experten die Aufgabe der Behörden bleiben, Risiken zu beurteilen und bei Bedarf Massnahmen vorzusehen. Ein wissenschaftliches Komitee könnte dabei eine Funktion übernehmen.

3.2 Standardisierung der kryptografischen Bausteine

Die bereits heute geforderten Sicherheitsbeweise im Bereich der Kryptografie sind wichtig, sie sollen laufend dem aktuellen Stand der Wissenschaft angepasst werden. Zudem raten die Expertinnen und Experten den Behörden auf eine Standardisierung der kryptografischen Bausteine hinzuwirken.

[1] Vgl. dazu die Liste der mandatierten Expertinnen und Experten unter www.bk.admin.ch > Politische Rechte > E-Voting.
[2] Vgl. dazu den Fragebogen unter www.bk.admin.ch > Politische Rechte > E-Voting.

3.3 Qualität und Überprüfbarkeit des Quellcodes gewährleisten

Es muss darauf geachtet werden, dass die Systemdokumentation und der Quellcode in einer Form vorliegen, die eine effiziente Überprüfung der Konformität mit den rechtlichen Anforderungen zulässt. Die Expertinnen und Experten haben als mögliche Grundlage für die Entwicklungsprozesse verschiedene Standards genannt. Simplizität soll bei der Systemkonzeption als Grundprinzip gelten.

3.4 Mehr Diversität als Grundvoraussetzung für Vertrauenswürdigkeit

Diversität unter den Komponenten, die für die Verifizierbarkeit wichtig sind (sog. Kontrollkomponenten und Verifier), bildet für die Expertinnen und Experten eine Grundvoraussetzung für die Vertrauenswürdigkeit eines Systems: Fehler in einzelnen Komponenten sollen dank anderen, korrekt funktionierenden Komponenten keine negative Auswirkung auf die Verifizierbarkeit haben (exponentieller Sicherheitsgewinn). Zu den Elementen für eine Diversifizierung gehört die Software. Verbesserungspotenzial sehen die Expertinnen und Experten auch bei der Generierung der Systemparameter (beispielsweise der Prüfcodes für die individuelle Verifizierbarkeit), die verifizierbar und verteilt durchgeführt werden sollte. Für den Druck der Stimmrechtsausweise haben sie Lösungen für einen verteilten Druckprozess skizziert. Die Expertinnen und Experten anerkennen die Kosten und Erhöhung der Komplexität beim Betrieb, die durch die Einführung von mehr Diversität entsteht, unterstreichen jedoch den Mehrwert.

3.5 Public Bulletin Board für noch mehr Verifizierbarkeit

Als komplementärer Ansatz, um die Verifizierbarkeit auszubauen und unabhängiger zu gestalten, wurde der Einsatz eines sogenannten öffentlichen Anschlagbretts (public bulletin board) diskutiert, das aus der wissenschaftlichen Literatur zu E-Voting bekannt ist. Die Expertinnen und Experten betrachten ein solches öffentliches Anschlagbrett als geeignetes Instrument für die Vertrauensbildung, sehen das Vertrauen aber auch gefährdet, wenn bei der Konzeption oder der Umsetzung Fehler gemacht werden. Die Bedürfnisse der Stimmenden, namentlich bei der Kommunikation, der visuellen Darstellung oder der Benutzerfreundlichkeit müssen frühzeitig untersucht und berücksichtigt werden.

4. Mandatierte und Öffentliche Prüfung

4.1 Mandatierte Überprüfung

Der Zertifizierung der Systeme wird keine entscheidende Bedeutung beigemessen. Dennoch könnte im Rahmen der Prüfung des Betriebs eine Zertifizierung sinnvoll sein (Zertifizierung nach ISO27001). Statt auf Zertifizierungen, sollen die Behörden auf unabhängige Prüfungen durch Personen mit den nötigen Kompetenzen setzen. Kryptografinnen und Kryptografen sollen auch bei der Prüfung des Quellcodes und des Betriebs beigezogen werden. Die Überprüfung muss einem ganzheitlichen Konzept folgen, um Lücken zu verhindern. Die Überprüfung soll durch den Bund oder ein unabhängiges Komitee in Auftrag gegeben werden.

4.2 Öffentliche Überprüfung

Die Expertinnen und Experten messen der öffentlichen Überprüfung eine grosse Wichtigkeit zu. Sie würden es begrüssen, wenn der 2019 durchgeführte PIT durch ein ständig laufendes Bug-Bounty Programm (BBP) mit finanzieller Entschädigung ersetzt würde. Das BBP soll sich nicht auf erfolgreiche Angriffe auf die Infrastruktur des Anbieters beschränken, sondern auch Fehler in der Dokumentation des Systems sowie im Quellcode zum Gegenstand haben. Die Festlegung der Zielsetzung und der Modalitäten sowie die Oberaufsicht über das BBP werden beim Bund oder einem unabhängigen Komitee gesehen.

Zusätzlich zum BBP könnten auch weitere Massnahmen für die Beteiligung der Öffentlichkeit geprüft werden, wie beispielsweise Hackathons. Auch der Einbezug von Personen ohne einen technischen

Hintergrund könnte sich als sinnvoll erweisen, beispielsweise im Rahmen eines Citizen-Science Projekts, das sich der Benutzerfreundlichkeit oder der Kommunikation widmet.

4.3 Transparenz und Offenlegung des Quellcodes

Transparenz bildet die Voraussetzung für eine wirksame öffentliche Überprüfung. Bei der Offenlegung des Quellcodes sollte nach Ansicht der Expertinnen und Experten auf eine Geheimhaltungserklärung unbedingt verzichtet werden.

Nebst dem Quellcode sollen alle Unterlagen offengelegt werden, die nötig sind, um zu verstehen wie das System funktioniert und betrieben wird. Zudem soll es möglich sein, das System auf eigenen Rechnern zu testen. Mit Blick auf den Fall, dass Anpassungen am Quellcode nicht unmittelbar offengelegt werden, raten Experten, eine erste Iteration an Prüfungen vorzunehmen, um unnötige Fehler und den damit verbundenen Vertrauensverlust zu vermeiden.

Mängel sollen offengelegt und Hinweise aus der Öffentlichkeit beantwortet werden. Die detaillierten Bestimmungen dazu soll der Bund festlegen. Die Mehrheit der Expertinnen und Experten rät zudem, Prüfberichte zu publizieren. Manche geben aber zu bedenken, dass Prüfberichte, die qualitativ mangelhaft sind, zu einem Vertrauensverlust führen können.

Die Expertinnen und Experten halten es für möglich, dass eine Offenlegung auch ohne Open Source Lizenz[3] eine zielführende öffentliche Prüfung ermöglicht. Allerdings erachten sie eine Offenlegung unter einer Open Source Lizenz als erfolgsversprechender.

4.4 Umgang mit Nichtkonformitäten

Idealerweise findet die Überprüfung so weit im Vorfeld statt, dass Nichtkonformitäten so früh entdeckt werden, dass sie für den Einsatz behoben werden können. Für den Umgang mit Nichtkonformitäten, die spät entdeckt werden, sollen Entscheidungsprozesse festgelegt werden.

Nicht bei jeder Nichtkonformität muss der Einsatz von E-Voting gestoppt werden. Die Expertinnen und Experten halten es für nachvollziehbar, dass geringe Risiken akzeptiert werden. Die Schwierigkeit besteht darin, das Risiko richtig einzuschätzen. Vergleiche mit bereits akzeptierten Risiken können helfen. Ebenso zu berücksichtigen gilt es den faktischen Verlust des Stimmrechts von Teilen des Auslandschweizer Elektorats sowie die Tatsache, dass der Verzicht auf E-Voting eine verstärkte Nutzung der ebenfalls risikobehafteten brieflichen Stimmabgabe zur Folge hat. Je stärker eine Nichtkonformität das System betrifft und je weniger sie sich auf die umgebenden Prozesse beschränkt, desto eher muss sie behoben werden. Fehler im kryptografischen Protokoll oder dessen Umsetzung im Quellcode sollen grundsätzlich nicht akzeptiert werden.

5. Einschätzung der Expertinnen und Experten zum Dialog

Der Dialog mit der Wissenschaft bildet für die Expertinnen und Experten einen Meilenstein. Nach ihrer Einschätzung hat er zu wertvollen Ergebnissen geführt. Sie regen an, ihn als Ausgangspunkt für einen ständigen Austausch zu verstehen.

[3] Open Source Lizenzen erlauben die Verwendung der Software für beliebige Zwecke.