Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundeskanzlei BK

August 2019

Vote électronique - Öffentlicher Intrusionstest 2019

Schlussbericht des Steuerungsausschusses

System unter Test: Vollständig verifizierbares System der Schweizerischen Post (Version vom Februar 2019)

Inhaltsverzeichnis

1 Zweck des Dokuments

Der vorliegende Bericht fasst die Organisationsstruktur, den Ablauf sowie die Schlussfolgerungen aus dem öffentlichen Intrusionstest 2019 (*public intrusion test*; PIT) des Systems der Schweizerischen Post für die elektronische Stimmabgabe zusammen.

2 Hintergrund

Auf der Grundlage von Art. 8*a* des Bundesgesetzes über die politischen Rechte (BPR, SR 161.1) führen die Kantone seit dem Jahr 2004 Versuche mit der elektronischen Stimmabgabe durch. Dies erfolgt im Rahmen des Projekts Vote électronique (VE) von Bund und Kantonen. Die bundesrechtlichen Versuchsbedingungen sind in der Verordnung über die politischen Rechte (VPR, SR 161.11) sowie der Verordnung der Bundeskanzlei über die elektronische Stimmabgabe (VEleS, SR 161.116) geregelt.

Insgesamt haben 15 Kantone anlässlich eidgenössischer Urnengänge wiederholt einem Teil ihres Elektorats ermöglicht, die Stimme via Internet abzugeben. Seit 2015 kommen Systeme zum Einsatz, die die Systemeigenschaft der sogenannten individuellen Verifizierbarkeit aufweisen. Als eine Voraussetzung für eine weitere Ausdehnung der elektronischen Stimmabgabe gilt die Einführung der sogenannten vollständigen Verifizierbarkeit. Für den Ersteinsatz eines solchen Systems verlangt die VEleS die vorgängige Zertifizierung der Systeme sowie die Offenlegung des Quellcodes.

Zudem haben Bund und Kantone im April 2017 beschlossen, vollständig verifizierbare E-Voting-Systeme im Sinne eines Pilotversuchs einem öffentlichen Intrusionstest zu unterziehen. Bei einem Intrusionstest wird die Sicherheit eines Systems geprüft, indem es Angriffen ausgesetzt wird. Die VEleS verlangt bereits im Rahmen der Zertifizierung die Durchführung eines Intrusionstests durch eine akkreditierte Stelle. Mit einem öffentlichen Intrusionstest können zusätzlich interessierte Personen aus aller Welt ein System testen.

Die Durchführung eines öffentlichen Intrusionstests dient verschiedenen Zielsetzungen. So können die Rückmeldungen der Teilnehmenden unmittelbar dazu beitragen, dass die Sicherheit verbessert wird. Zudem trägt die Durchführung eines öffentlichen Intrusionstests dazu bei, dass unabhängige Fachpersonen Kompetenzen und Wissen im Bereich der elektronischen Stimmabgabe aufbauen. Dies könnte längerfristig der Abhängigkeit von einzelnen Personen und Organisationen entgegenwirken und der öffentlichen Debatte zuträglich sein. Der öffentliche Intrusionstest bildet zudem ein Instrument der Transparenz und soll zur Vertrauensbildung beitragen. Ein erfolgreicher öffentlicher Intrusionstest setzt die aktive Mitarbeit einer möglichst grossen Zahl kompetenter Personen voraus. Die öffentliche Debatte in Medien und Politik rund um einen öffentlichen Intrusionstest ist zudem ein Prüfstein für die Fehlerkultur im E-Voting-Umfeld.

3 Getestetes System

In der Schweiz gelangten in den letzten Jahren zwei unterschiedliche Systeme mit individueller Verifizierbarkeit für die elektronische Stimmabgabe zum Einsatz: Das System der Schweizerischen Post (zuletzt eingesetzt von den Kantonen Freiburg, Neuchâtel, Thurgau und Basel-Stadt) sowie das System des Kantons Genf (zuletzt eingesetzt von den Kantonen Bern, Luzern, St. Gallen[1], Aargau, Waadt und Genf).

Die Genfer Behörden haben am 28. November 2018 bekanntgegeben, dass sie ihr System längstens bis Februar 2020 betreiben werden. Die Weiterentwicklung des Systems zur vollständigen Verifizierbarkeit wurde in der Folge abgebrochen. Damit wurde auch ein öffentlicher Intrusionstest hinfällig.

Dem PIT wurde allein das um die vollständige Verifizierbarkeit erweiterte System der Schweizerischen Post (nachfolgend Post) unterzogen. Es handelte sich dabei um das zukünftige System und nicht um dasjenige, das bereits im Einsatz stand. Das System kann erst nach Erfüllung aller bundesrechtlichen Anforderungen und der abschliessenden Erteilung der Betriebsbewilligung durch die Behörden für eidgenössische Urnengänge eingesetzt werden.

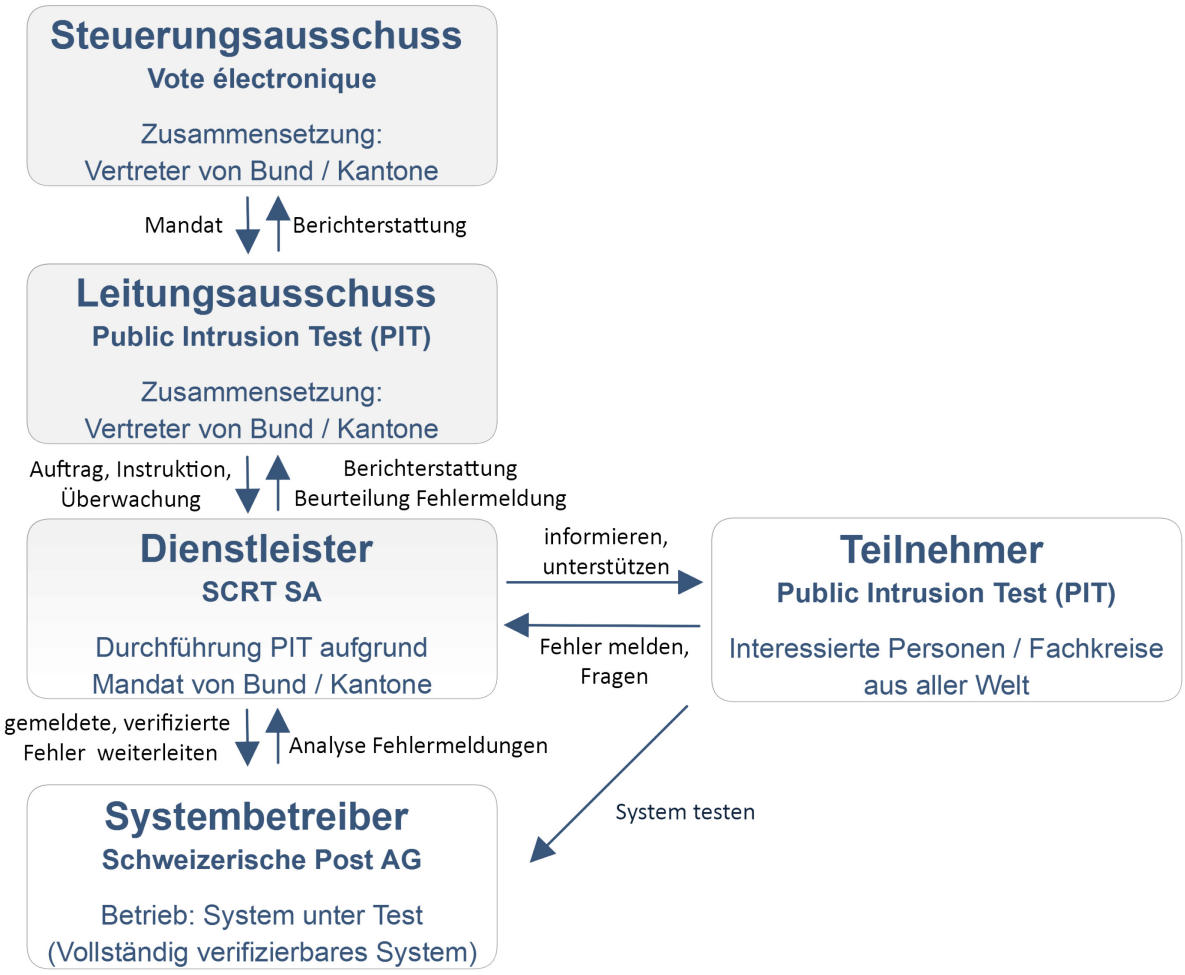
Der Systemaufbau des PIT Test-Systems entsprach 1:1 dem vorgesehenen produktiven Systemaufbau. Es wurde einzig eine sicherheitstechnische Konfiguration (das Ausschliessen von auffälligen IP-Adressen mittels Fail2Ban) deaktiviert, um die teilnehmenden Personen nicht unnötig einzuschränken.

4 Versuchsanordnung / Organisation

Bund und Kantone haben beschlossen, im Bereich der öffentlichen Intrusionstests gemeinsam zu handeln. Sie haben zuhanden der Systembetreiber gemeinsame Anforderungen erlassen[2]. Zudem haben sie den öffentlichen Intrusionstest via den von Bund, Kantonen und Gemeinden getragenen Schwerpunktplan von E-Government Schweiz mit CHF 250'000 unterstützt. Davon wurden CHF 150'000 der Post und CHF 100'000 der Firma SCRT als Dienstleister von Bund und Kantonen entrichtet.

[1] Der Kanton St. Gallen plant künftig das System der Schweizerischen Post einzusetzen.
[2] https://www.bk.admin.ch/dam/bk/de/dokumente/pore/Anforderungen%20von%20Bund%20und%20Kantonen_%C3%96ffentliche%20Intrusionstests.pdf.download.pdf/Anforderungen%20von%20Bund%20und%20Kantonen_%C3%96ffentliche%20Intrusionstests.pdf

Übersicht: Organisation PIT



Die Post stellte das System für den öffentlichen Intrusionstest vom 25. Februar bis zum 24. März 2019 zur Verfügung und war für den Betrieb besorgt. Für wertvolle Rückmeldungen stellte sie den Teilnehmenden eine Entschädigung in Aussicht (CHF 100 bis maximal 50'000 pro Rückmeldung; maximal CHF 150'000 insgesamt). Die Kriterien für eine Entschädigung waren vordefiniert und für die Teilnehmenden auf einer eigens für den öffentlichen Intrusionstest bereitgestellten Internetplattform (PIT-Plattform[3]) einsehbar.

Der Leitungsausschuss (LA) von Bund und Kantonen hat den öffentlichen Intrusionstest im Auftrag des Steuerungsausschusses Vote électronique (SA) begleitet und überwacht. Er diente Bund und Kantonen als Anlaufstelle für Fragen betreffend den öffentlichen Intrusionstest. Während des Tests hatte der LA die Aufgabe, zeitgerecht Auskunft über den aktuellen Stand der Erkenntnisse zu geben. Er koordinierte die Kommunikation unter den beteiligten Akteuren und erarbeitete die Elemente für die behördliche Kommunikation an die Adresse der Öffentlichkeit.

[3] https://www.onlinevote-pit.ch/

Bund und Kantone haben für die Durchführung des öffentlichen Intrusionstests die darauf spezialisierte Firma SCRT mandatiert; sie handelte auf Anweisung des LA. SCRT war für die Kommunikation mit den Teilnehmenden zuständig, akquirierte, registrierte und unterstützte die Teilnehmenden, nahm deren Rückmeldungen entgegen und wertete diese aus. Dazu betrieb SCRT die PIT-Plattform.

Personen aus aller Welt waren eingeladen, am PIT teilzunehmen. Bei der Registrierung über die PIT-Plattform nahmen sie von den Verhaltensregeln der Post Kenntnis und mussten sich mit ihnen einverstanden erklären (Vereinbarung mit der Post). Die Verhaltensregeln betrafen den Testumfang sowie das Vorgehen bei entdeckten Mängeln und gewährten bei Einhaltung der Verhaltensregeln Straffreiheit.

Die Versuchsanordnung hat in der Öffentlichkeit Kritik hervorgerufen.

- Im Einklang mit den Anforderungen von Bund und Kantonen hat die Post den Test auf Angriffe auf die E-Voting-Infrastruktur der Post beschränkt und die Verhaltensregeln dementsprechend festgelegt. Infrastrukturen der Kantone, der Druckereien sowie weitere Dienstleistungen der Post durften damit nicht angegriffen werden. Zudem waren Angriffe mit dem Ziel, dass das System für die Stimmenden unerreichbar wird, ausgeschlossen (Denial-of-service-Angriffe). Ebenfalls vom Test ausgeschlossen waren Angriffe auf die Benutzerplattformen der Stimmberechtigten. Dasselbe galt für jegliche Angriffe, die darauf abzielen, via gefälschte Nachrichten die Akteure dazu zu bringen, von den vorgesehenen Prozessen abzuweichen (Social-Engineering). Bund und Kantone haben auf die Kritik reagiert (vgl. Ziffer 5).

- Die Anforderungen von Bund und Kantonen an den PIT verpflichteten die Post, den Quellcode des Systems gemäss den Bestimmungen in Art. 7*a* f. VEleS vor dem Test offenzulegen. Dies sollte den Teilnehmenden Gelegenheit geben, sich auf den Test vorzubereiten. Für den Zugang zum Quellcode hat die Post den Teilnehmenden gesonderte Nutzungsbedingungen unterbreitet. Die Kritik betraf einerseits diese Nutzungsbedingungen und anderseits die Aufbereitung des Quellcodes. So machten Kritiker in den Nutzungsbedingungen unzulässige Einschränkungen am Recht geltend, den Quellcode zu untersuchen, zu verändern, zu kompilieren und auszuführen sowie dazu Studien zu verfassen und diese zu publizieren. Dieses Recht wird in Art. 7b Abs. 4 VEleS eingeräumt. Unter Verweis auf die schwierige Lesbarkeit und eine ungenügende Dokumentation des Quellcodes wurden auch Verstösse gegen Art. 7b Abs. 1 VEleS vorgeworfen. Die Bundeskanzlei hat die Post aufgefordert, die Rahmenbedingungen zur Veröffentlichung des Quellcodes zu überprüfen und anzupassen.[4]

5 Ablauf

Am 7. Februar 2019 haben die Bundeskanzlei sowie die Kantone Freiburg, Graubünden, Neuenburg, St. Gallen und Thurgau den öffentlichen Intrusionstest per Medienmitteilung angekündigt[5]. Ab diesem Tag konnten sich Interessierte auf der PIT-Plattform anonym zur Teilnahme registrieren. SCRT hat den Test über Twitter und weitere Kanäle gegenüber Fachkreisen angekündigt. Am selben Tag hat die Post den Quellcode zugänglich gemacht.

[4] https://www.bk.admin.ch/bk/de/home/dokumentation/medienmitteilungen.msg-id-74307.html
[5] https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-73898.html

Anlässlich des Beginns der Testarbeiten und infolge des grossen Medieninteresses hat die Bundeskanzlei am 25. Februar 2019 die Medienschaffenden zu einem Hintergrundgespräch eingeladen. Vertreter von Bund und Kantonen sowie der Post haben Faktenblätter abgegeben und standen für Fragen zur Verfügung[6]. Die Faktenblätter erläuterten die Zielsetzung des PIT und erklärten dessen Geltungsbereich. Damit antworteten Bund und Kantone auf die vielfach geäusserte Kritik an den Testmodalitäten. Entsprechende Erläuterungen waren über die Webseite der Bundeskanzlei unter Fragen und Antworten (Q&A) zugänglich.[7]

Während des Tests konnten die Teilnehmenden über die PIT-Plattform Stimmrechtsausweise beziehen, Fragen stellen und Rückmeldungen einreichen. SCRT hat die Rückmeldungen triagiert und die Teilnehmenden über die Beurteilung informiert. Handelte es sich bei einer Rückmeldung um eine potentielle Verwundbarkeit (vulnerability), hat SCRT neben dem LA die Post informiert. In regelmässigen Abständen haben SCRT sowie die Post dem LA ihre Beurteilung der Rückmeldungen unterbreitet. Es kam weder zwischen SCRT und der Post noch mit dem LA zu Differenzen in der Beurteilung von Rückmeldungen.

6 Resultat

Bis zum Abschluss des Tests am 24. März 2019 haben sich 3'186 Teilnehmende aus 137 Ländern[8] registriert. Tatsächlich auf der PIT-Plattform eingeloggt haben sich 1'090 Personen oder Teams. 822 Personen haben Stimmrechtsausweise für den Test bezogen. Letztlich haben 80 Personen insgesamt 173 Rückmeldungen über die PIT-Plattform eingereicht. Bei 16 Rückmeldungen konnte SCRT einen Verstoss gegen beste Praktiken der Sicherheitstechnik durch die Post feststellen[9]. Die Post hat die entsprechenden Teilnehmenden mit Beträgen von insgesamt CHF 2'000 entschädigt. Ein Eindringen in die Infrastruktur, eine Manipulation von Stimmen oder ein Brechen des Stimmgeheimnisses konnte im Rahmen des PIT nicht festgestellt werden.

Allerdings konnten Forschende ausserhalb des PIT anhand der im Rahmen der Offenlegung des Quellcodes veröffentlichten Systemunterlagen insgesamt drei erhebliche Mängel am System identifizieren[10]. Einer der Mängel betraf auch das produktiv im Einsatz stehende, individuell verifizierbare System. Er führte zum Entscheid der Post, das System anlässlich des Urnengangs vom 19. Mai 2019 nicht zum Einsatz zu bringen. Zudem hat die Bundeskanzlei eine Standortbestimmung angekündigt, mit dem Ziel, dass solchen Fehlern künftig rechtzeitig zuvorgekommen wird. Es wurde kein Angriff auf das System gemeldet, der sich einen dieser Mängel zunutze gemacht hätte. Da die Mängel nicht mit einem Angriff auf das unter Test stehende System aufgezeigt wurden, fielen die Rückmeldungen nicht in den Geltungsbereich des PIT.

7 Schlussfolgerungen

Es ist als Erfolg zu werten, dass eine Vielzahl kompetenter Personen aus der ganzen Welt aktiv am Test mitgewirkt hat. Ihre Arbeit hat es erlaubt, Mängel der Kategorie «Best-Practices» zu beheben und damit die Sicherheit des Gesamtsystems weiter zu erhöhen. Ihre Erfahrung

[6] https://www.bk.admin.ch/bk/de/home/politische-rechte/e-voting/oeffentlicher_intrusionstest.html
[7] https://www.bk.admin.ch/bk/de/home/politische-rechte/e-voting/oeffentlicher_intrusionstest.html
[8] Gemäss Deklaration der Teilnehmenden
[9] Ziffer 4.3 Anhang sowie https://www.onlinevote-pit.ch/stats/
[10] https://www.bk.admin.ch/bk/de/home/dokumentation/medienmitteilungen.msg-id-74508.html

mit der elektronischen Stimmabgabe in der Schweiz werden sie möglicherweise auch in Zukunft einbringen können, so zum Beispiel, indem sie sich bei anderer Gelegenheit mit sicherheitstechnischen Fragestellungen befassen oder indem sie sich an der öffentlichen Debatte beteiligen.

Es ist davon auszugehen, dass die Teilnehmenden sich nicht nur aus Expertinnen und Experten zusammensetzten, sondern ebenfalls aus interessierten Bürgerinnen und Bürgern. Der PIT hat ihnen die Gelegenheit gegeben, sich mit einem E-Voting-System vertraut zu machen, das in Zukunft möglicherweise in ihrem Kanton eingesetzt wird.

Die Post hat die Anforderungen von Bund und Kantonen in den meisten Punkten erfüllt. Sie hat unter hohem Ressourceneinsatz und mit qualifiziertem Personal einen erkenntnisreichen PIT ermöglicht. Der Handlungsbedarf liegt im Bereich der Aufbereitung und der Offenlegung des Quellcodes. Dieser ist anzugehen.

Die vielfach geäusserte Kritik am Geltungsbereich des PIT gilt es für die Zukunft zu verwerten. Gerade mit Blick auf Sicherheitsthemen, die nicht im Rahmen eines öffentlichen Intrusionstests behandelt werden können, sind bei der bevorstehenden Standortbestimmung der Bundeskanzlei Massnahmen zu prüfen, die einen konstruktiven Dialog mit unabhängigen Fachpersonen fördern und strukturieren. Auch mit Blick auf die Systementwicklung sowie Prüfarbeiten zur Qualitätssicherung sollen unabhängige Fachpersonen verstärkt einbezogen werden.

Die wertvollsten Meldungen betrafen die erheblichen Mängel, die im Quellcode festgestellt wurden. Es sind keine Meldungen über erfolgreiche Versuche, ins System einzudringen, eingegangen. Für die Zukunft sind Anreize für die Bekanntgabe wertvoller Beobachtungen im Quellcode und der Dokumentation zu prüfen. Die gemachten Erfahrungen sind ferner wegweisend für die Etablierung einer Qualitäts- und Fehlerkultur im Umfeld der elektronischen Stimmabgabe.

Es darf vermutet werden, dass die Mediatisierung des PIT auch zur verstärkten Beteiligung an der Analyse des Quellcodes beigetragen hat.

Beim diesjährigen Test handelt es sich um die erstmalige Durchführung eines PIT mit der elektronischen Stimmabgabe. Die Erfahrungen werden in allfällige weitere Durchführungen einfliessen.

8 Weiterführende Dokumente / Berichte / Verweise

Informationen des Bundes, der Kantone und des für die Durchführung beauftragten Dienstleisters (SCRT) im Zusammenhang mit dem öffentlichen Intrusionstest:

Dokument / Bericht / Link	Link
Webseite des Bundes mit Informationen zum öffentlichen Intrusionstest 2019	https://www.bk.admin.ch/bk/de/home/politische-rechte/e-voting/oeffentlicher_intrusionstest.html

Anforderungen von Bund und Kantonen zu öffentlichen Intrusionstests	https://www.bk.admin.ch/dam/bk/de/dokumente/pore/Anforderungen%20von%20Bund%20und%20Kantonen_%C3%96ffentliche%20Intrusionstests.pdf.download.pdf/Anforderungen%20von%20Bund%20und%20Kantonen_%C3%96ffentliche%20Intrusionstests.pdf
Faktenblatt der Bundeskanzlei zum PIT	https://www.bk.admin.ch/dam/bk/de/dokumente/pore/PIT_Factsheet%20BK_DE.pdf.download.pdf/PIT_Factsheet%20BK_DE.pdf
Faktenblatt des Leitungsausschusses zum PIT	https://www.bk.admin.ch/dam/bk/de/dokumente/pore/PIT_Factsheet%20Leitungsausschuss_DE.pdf.download.pdf/PIT_Factsheet%20Leitungsausschuss_DE.pdf
Registrierungsplattform PIT für Interessierte und Teilnehmende	https://www.onlinevote-pit.ch/
Fragen und Antworten zum PIT (FAQ) für Interessierte und Teilnehmende	https://www.onlinevote-pit.ch/faq/
Akzeptierte und publizierte PIT Findings	https://www.onlinevote-pit.ch/stats/

Informationen des Systembetreibers, der Schweizerischen Post, im Zusammenhang mit dem öffentlichen Intrusionstest:

Dokument / Bericht / Link	**Link**
Detaillierter technischer Schlussbericht des Systembetreibers (Post CH AG)	https://www.post.ch/-/media/post/evoting/dokumente/abschlussbericht-oeffentlicher-intrusionstest-post.pdf?la=de&vs=1
Terms, Conditions and Code of Conduct Public Intrusion Test (PIT)	https://www.onlinevote-pit.ch/conduct/
Webseite der Post mit Informationen zum öffentlichen Intrusionstest 2019	https://www.post.ch/de/geschaeftsloesungen/e-voting/publikationen-und-quellcode#oeffentlicher-intrusionstest-2019
Blogartikel der Post zum öffentlichen Intrusionstest	https://www.evoting-blog.ch/de/pages/2019/oeffentlicher-hackertest-am-e-voting-system-der-post

Blogartikel der Post zur Quellcode-Offenlegung	https://www.evoting-blog.ch/de/pages/2019/die-post-veroeffentlicht-den-quellcode-ihres-e-voting-systems
Link auf Informationsportal für Wähler inkl. Demosystem der Post	www.evoting.ch
Zugang zum Quellcode via Internetseite der Post	https://www.post.ch/de/geschaeftsloesungen/e-voting/publikationen-und-quellcode#offenlegung-quellcode

9 Anhang

Public Intrusion Test, Final Report, SCRT SA, 2019