Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundeskanzlei BK

Sektion Politische Rechte

Öffentlicher Intrusionstest

Faktenblatt des Leitungsausschusses von Bund und Kantonen

25. Februar 2019

Anforderungen von Bund und Kantonen

Bund und Kantone haben 2017 beschlossen, dass E-Voting-Systeme mit vollständiger Verifizierbarkeit einem öffentlichen Intrusionstest (*public intrusion test*; PIT) unterzogen werden müssen.

Damit stellen sie jenes Infrastrukturelement auf die Probe, das die Stimmen aufbewahrt und während vier Wochen vom Internet aus erreichbar ist.

Bund und Kantone haben für den PIT gemeinsame Anforderungen erlassen. Zu diesen gehören:

- Der Systemanbieter stellt sein System während vier Wochen für den Test zur Verfügung;
- Als Grundlage für die Teilnehmenden sind die Systemdokumentation sowie der Quellcode offenzulegen;
- Teilnehmende dürfen ihre Erkenntnisse aus dem Test publizieren, wobei der Systemanbieter eine Wartefrist festlegen darf;
- Durch seine Einwilligung schützt der Systemanbieter die PIT-Teilnehmenden vor Strafverfolgung;
- Diese Einwilligung umfasst Angriffe auf das E-Voting-System, mit dem Ziel, Stimmen zu manipulieren, abgegebene Stimmen zu lesen, das Stimmgeheimnis zu brechen oder Sicherheitsvorkehrungen ausser Kraft zu setzen oder zu umgehen, die die Stimmen und sicherheitsrelevante Daten schützen.

Ablauf

Ein Leitungsausschuss bestehend aus Fachleuten von Bund und Kantonen überwacht und begleitet die Durchführung des PIT.

Bund und Kantone haben für die Durchführung des PIT die Firma SCRT beauftragt. Sie ist für die Kommunikation mit den Teilnehmenden zuständig. SCRT registriert die Teilnehmenden, nimmt deren Rückmeldungen entgegen und wertet sie aus. Dazu betreibt SCRT eine Internet-Plattform (PIT-Plattform[1]).

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

Plausible Befunde leitet SCRT die Meldung an die Schweizerische Post weiter. Für Rückmeldungen, die eine Schwachstelle aufzeigen, stellt die Post den Teilnehmenden eine Entschädigung in Aussicht (CHF 100.- bis maximal 50'000.- pro Rückmeldung; maximal 150'000.- insgesamt). Die Kriterien für Entschädigungen und deren Höhe sind vordefiniert und für die Teilnehmenden auf der PIT-Plattform einsehbar.

Sobald alle Auswertungen abgeschlossen sind, verfasst der Leitungsausschuss einen Bericht zuhanden des Steuerungsausschusses Vote électronique, der die Erkenntnisse aus dem PIT zusammenfasst. Der Steuerungsausschuss veröffentlicht den Bericht im Sommer 2019.

Sicherheit und Transparenz

Die Sicherheit von E-Voting kann durch einen PIT nicht bewiesen werden. Vielmehr bietet er die Chance, nicht bekannte Schwachstellen zu entdecken und bei Bedarf zu beheben. Zudem ermöglicht er die Beteiligung von zusätzlichen Kreisen von Fachpersonen an der öffentlichen Debatte. Auch diese kann mittelbar zur Sicherheit beitragen.

Das Bundesrecht stellt hohe Anforderungen an die Sicherheit der Systeme und deren Betrieb. Die Anforderungen richten sich auf die gesamte Prozesskette bei der Durchführung von Urnengängen. Die Anforderungen von Bund und Kantonen machen beim PIT bewusst das E-Voting-System zum Gegenstand, und zwar mit Blick auf die Sicherheit der Stimmen. Angriffe auf Elemente der Prozesskette, wie sie im Folgenden aufgeführt sind, sind nicht Bestandteil des PIT.

Gründe für den Ausschluss von DDOS-Attacken

Unter DDoS (Distributed Denial of Service) versteht man einen Angriff auf Computer-Systeme mit dem Ziel, deren Verfügbarkeit zu stören. DDoS-Attacken sind nicht Gegenstand des PIT. Gründe: Erstens handelt es sich dabei um bekannte Attacken gegen internetbasierte Systeme, ohne E-Voting spezifischen Charakter. Für den Fall einer anhaltenden Attacke bleibt den Stimmberechtigten die briefliche oder persönliche Stimmabgabe an der Urne offen. Auch die bundesrätliche Anordnung, dass die elektronische Urne bereits am Samstag, 12 Uhr zu schliessen ist, wirkt den Auswirkungen von DDOS-Attacken entgegen. Zweitens werden DDoS nicht im Rahmen des PIT getestet, da diese das zu testende System unerreichbar machen und damit den PIT stören würden. Die Wirksamkeit der vorhandenen Abwehrmechanismen gegen DDoS-Attacken kann effektiver getestet werden, indem DDOS-Attacken ausserhalb eines PIT simuliert werden.

Gründe für den Ausschluss von Attacken auf die Benutzerplattformen der Stimmberechtigten

Attacken auf fremde Infrastrukturen (insbesondere auch Benutzerplattformen von Privatpersonen) sind rechtlich nicht zulässig und daher vom Umfang des PIT ausgenommen. Zum Schutz dieser Benutzerplattformen dienen die Prüfmechanismen der Stimmberechtigten – insbesondere die individuelle Verifizierbarkeit – sowie die Instruktionen der Kantone zuhanden der Stimmberechtigten. Das Aushebeln der individuellen Verifizierbarkeit, d.h. der Prüfmechanismen der Stimmberechtigten ist Bestandteil des Tests.

Selbstverständlich könnte sich ein Teilnehmer damit einverstanden erklären, dass ein anderer Teilnehmer seine Benutzerplattform angreift. Im Fall eines erfolgreichen Angriffs könnten die Organisatoren des PIT jedoch nicht unterscheiden, ob es sich um einen echten oder einen simulierten Angriff handelt. Der PIT ist damit keine geeignete Massnahme für die Sicherheit der Benutzerplattformen. Simulierte Demonstrationen von Angriffen sind jedoch nicht

verboten. Sie könnten mit Blick auf Diskussionen rund um die Sicherheit bei E-Voting durchaus nützlich sein.

Gründe für den Ausschluss von Social-Engineering Attacken

Social-Engineering ist ein Sammelbegriff für Angriffe, die darauf abzielen, via gefälschte Nachrichten die Akteure zu beeinflussen. Beispielsweise könnte eine Strategie darin bestehen, die Stimmberechtigten dazu zu bringen, von den behördlichen Instruktionen für die elektronische Stimmabgabe abzuweichen (z.B. Verzicht auf Kontrolle der Prüfcodes). Oder es könnte versucht werden, die Mitarbeitenden des Systemanbieters oder des zuständigen Kantons zu beeinflussen. Da die Akteure jedoch wissen, dass der PIT stattfindet, ist davon auszugehen, dass sie sich speziell auf Social-Engineering-Angriffe einstellen würden. Dadurch entfernt sich die Testanordnung von der Praxis. Damit ist ein PIT keine geeignete Massnahme, um die Robustheit gegen Social-Engineering-Angriffe zu testen.

PIT für die Infrastruktur bei den Kantonen

Die Aufbereitung der Daten für die Durchführung des Urnengangs, der Druck des Stimmmaterials sowie die Entschlüsselung und die Auszählung der Stimmen finden bei den Kantonen statt. Beide Schritte werden auf physisch überwachten Infrastrukturen durchgeführt, die von jeglichen Netzwerken physisch getrennt sind. Dies steht im Gegensatz zum E-Voting-System, das während vier Wochen vom Internet aus erreichbar ist. Es ist effizienter, die Schutzmassnahmen innerhalb der Infrastruktur zu prüfen. Ein Test im Rahmen eines PIT (aus der Distanz) wird kaum aussagekräftige Ergebnisse hervorbringen.

Mitglieder des Leitungsausschusses von Bund und Kantonen

Oliver Spycher, Stv. Projektleiter Vote électronique, Bundeskanzlei

Philipp Egger, Leiter Informatik und Infrastruktur, Staatskanzlei St. Gallen

Nicolas Fellay, Verantwortlicher politische Rechte, Staatskanzlei Freiburg

Bruno Ledergerber, Stv. Leiter Wahlen & Abstimmungen, Statistisches Amt Kanton Zürich