Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Chancellery FCh

Political Rights Section

Sektion Politische Rechte

Public Intrusion Test

Fact sheet produced by the Management Committee of the Confederation and the Cantons

25 February 2019

Federal and cantonal requirements

In 2017, the Confederation and the cantons decided that completely verifiable e-voting systems would have to undergo a public intrusion test (PIT).

For a four-week period, they are therefore opening up the infrastructure which stores votes and which is accessible via the internet.

The Confederation and the cantons have drawn up a set of common requirements for the PIT. These include:

- The system provider will open up the system for a four-week testing period;
- Test participants will have access to system documentation and the source code;
- Participants are allowed to publish their findings from the test. The system provider may however impose a delay period;
- By providing its consent the system provider protects PIT participants from criminal prosecution;
- This consent covers attacks on the e-voting system aimed at manipulating votes, reading votes cast, breaching voter secrecy, or disabling or circumventing security measures intended to protect the ballots and security-relevant data.

Procedure

A management committee comprised of experts from the Confederation and cantons monitor and supervise the running of the PIT.

The Confederation and the cantons have commissioned SCRT to run the PIT. It is responsible for communicating with test participants. SCRT registers participants, gathers their feedback and evaluates it. To this end, SCRT operates an internet platform (PIT platform[1]).

SCRT reports plausible findings to Swiss Post. Participants who submit a report pointing to a qualifying vulnerability are potentially eligible for a compensatory payment from Swiss Post (CHF 100 up to a maximum of CHF 50,000 per report; max. CHF 150,000 in total). The criteria

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

for compensatory payments and the amount are predetermined and can be found on the PIT platform.

As soon as all evaluations have been completed, the management committee will prepare a report for the Steering Committee Vote électronique summarising the findings from the PIT. The Steering Committee will publish the report in the summer (2019).

Security and transparency

A PIT cannot prove the security of e-voting. Instead, it offers the opportunity to detect unknown vulnerabilities, and to remedy them if necessary. It also allows a wider field of experts to take part in the public debate. This too can contribute indirectly to improving security.

Federal legislation places high demands on the security of systems and their operation. The requirements cover the entire process chain when conducting ballots. The requirements set out by the Confederation and the cantons deliberately make the e-voting system the object of the PIT, with a view to vote security. Attacks on elements of the process chain, as listed below, are not part of the PIT.

Reasons for excluding DDoS attacks

DDoS (Distributed Denial of Service) is an attack on computer systems with the aim of disrupting their availability. DDoS attacks are not part of the PIT. Reasons: Firstly, these are known attacks against Internet-based systems and are not specific to e-voting. In the event of a sustained attack, voters are still able to submit a postal vote or vote in person at the ballot box. The Federal Council's instruction that e-voting cease as early as noon on Saturday also counteracts the effects of DDoS attacks. Secondly, DDoS are not being included within the scope of the PIT because they would render the system being tested inaccessible and thus disrupt the PIT. The effectiveness of the existing defence mechanisms against DDoS attacks can be tested more effectively by simulating DDoS attacks outside a PIT.

Reasons for excluding attacks on voter user platforms

Attacks on third-party infrastructure (in particular user platforms of private individuals) are not legally permissible and are therefore excluded from the scope of the PIT. Voter verification mechanisms – in particular individual verifiability – are intended to protect these user platforms, as well as safeguard the instructions given to voters by the cantons. The test includes the elimination of the individual verifiability, i.e. the verification mechanisms of the voters.

Of course, a participant could agree to another participant attacking his user platform. However, in the event of a successful attack, the organisers of the PIT could not distinguish between a real and a simulated attack. The PIT is therefore not a suitable means of testing user platform security. However, simulated demonstrations of attacks are not prohibited. They could be useful in terms of discussions on the security of e-voting.

Reasons for excluding social engineering attacks

Social engineering is a collective term for attacks aimed at influencing actors via fake messages. For example, one strategy could be to encourage voters to deviate from the instructions given by the authorities for e-voting (e.g. to not check the verification codes). Or attempts could be made to influence employees of the system provider or the canton concerned. However, as the stakeholders are aware that the PIT is taking place, it can be assumed that they would be prepared for social engineering attacks. The test conditions would therefore not reflect reality. A PIT is therefore not a suitable means of testing robustness against social engineering attacks.

PIT on cantonal infrastructure

The preparation of data for the ballot, the printing of voting material, as well as the decryption and counting of votes is carried out by the cantonal authorities. These steps are performed on physically monitored infrastructure, which is also physically separated from any networks. This is in contrast to the e-voting system, which can be accessed via the internet for four weeks. It is more efficient to check the protective measures within the infrastructure. Testing as part of a PIT (remotely) is unlikely to produce meaningful results.

Members of the management committee of the Confederation and the cantons

Oliver Spycher, Dep. Head, Vote électronique, Federal Chancellery

Philipp Egger, Head, IT and Infrastructure, St. Gallen Cantonal Chancellery

Nicolas Fellay, Head of Political Rights, Fribourg Cantonal Chancellery

Bruno Ledergerber, Dep. Head, Elections and Votes, Canton of Zurich Statistical Office