Public hacker test on Swiss Post's e-voting system

Swiss Post will be carrying out resilience testing, also known as a public intrusion test (PIT), on its e-voting system between 25 February and 24 March 2019. During the test, hackers and other independent IT specialists can challenge the Swiss Post e-voting system with deliberate attacks. How does the intrusion test work and what happens if anything is found? The answers to the key questions are given below.

How does the intrusion test work?

The test simulates a federal vote. As with normal voting procedures, the casting of votes is opened and then the intrusion test takes place four weeks prior to voting Sunday. 24 March 2019 is taken as voting Sunday. The intrusion test thus lasts from 25 February until 24 March.

Those interested in participating need to register on the www.onlinevote-pit.ch platform. The Confederation and cantons have commissioned the independent company SCRT SA to perform the intrusion test and operate the platform.

Participants can download their voting cards for the test on the platform. As with normal votes, the card contains the codes necessary to participate in the simulated vote and thus the intrusion test. Unlike normal contests, participants can obtain several voting cards, which are not sent by post but are instead available electronically.

Participants can submit their findings on the www.onlinevote-pit.ch platform. The company SCRT will look into the findings and if plausible, will forward them to Swiss Post.

Swiss Post will then analyse the findings and where necessary, reproduce them. If it is able to confirm a finding, it will release it for publication and the person who submitted the finding will be entitled to financial compensation if they were the first to report it.

On Sunday 24 March, the electronic ballot box will be decrypted and opened by the fictional electoral commission. Findings can be submitted until 25 March at midnight.

Why is Swiss Post performing an intrusion test on its e-voting system?

Swiss Post believes that only a transparent e-voting solution can be successful in the long term. By opening it up to an intrusion test, it is exposing its system to the intelligence and skill of sophisticated hackers to identify whether, when and how its e-voting system can be compromised.

It will incorporate the results of the intrusion test into the development of its e-voting system. Swiss Post will identify and rectify any vulnerabilities that may be found.

Last but not least, the intrusion test should also establish hard facts and thereby contribute to a fact-based discussion of e-voting.

Intrusion tests are an established procedure within the IT field and are a standard part of developing many IT systems.

What exactly can participants check for?

They can check the Swiss Post e-voting system for individual and universal verifiability.

The types of attack must be directly related to Swiss Post's e-voting

system. Other attacks are not permitted to be used and no compensation will be granted if used. These include:

- Attacks on other Swiss Post systems or applications
- Attacks on the voter's end device
- Attacks based on the assumption that voters do not keep to instructions, e.g. a voter does not check the ballot casting key

Detail can be found in the [Code of Conduct](#).

What will Swiss Post do in the event of discovering a vulnerability?

Anyone conducting a public intrusion test deliberately exposes themselves to the sophistication of independent hackers and must expect findings.

Swiss Post will professionally analyse findings and rectify any relevant errors or vulnerabilities as quickly as possible.

Are there any differences between the intrusion test and a genuine electoral contest?

Yes, there are some differences. The following in particular:

- Swiss Post will deactivate certain security measures within the system to enable participants to concentrate fully on attacking the core system. During normal operations, Swiss Post has gathered experience in recent years on how to quickly identify potential hackers. These warning signals will be ignored for the intrusion test.
- For practical reasons, the voting cards are sent electronically for the intrusion test instead of by post. The cards are also generated by Swiss Post and not the cantonal authorities.
- The testers are able to order several voting cards, not just one.

Who can participate?

Everyone is entitled to register. There are no restrictions. However, certain individuals are not entitled to compensation, e.g. Swiss Post employees.

Where can participants register?

On the www.onlinevote-pit.ch platform.

Why do participants need to register?

Registration is necessary for three reasons:

- It ensures that participants are legally entitled to attack the system
- It ensures that compensation can be paid in the event of a confirmed finding
- It clarifies the rules of conduct for participants

Why is an external company performing the intrusion test? What function is performed by this company during the intrusion test?

The Confederation and cantons have commissioned the Swiss company SCRT SA to implement the intrusion test on an operational level. This ensures independent performance and initial analysis of the results. SCRT SA specializes in performing intrusion tests. Its most important tasks are:

- Operating the platform www.onlinevote-pit.ch for registration and submission of findings
- Initial review of submitted findings
- Communication with participants and coordination between participants and Swiss Post

Where can participants submit their findings? When is the deadline for submitting findings?

Participants needs to submit their findings by Monday 25 March 2019 at midnight at www.onlinevote-pit.ch.

How does the evaluation process work for findings?

The independent company commissioned by the Confederation and cantons, SCRT SA, performs an initial review of the findings. If a finding is plausible, SCRT SA forwards it to a group of specialists within Swiss Post. They analyse and evaluate the finding and also try to reproduce it.

After this analysis, the person who submitted the finding will be notified as to whether their finding can be confirmed.

The rules of publication described in the Code of Conduct apply to confirmed findings.

What are the rules for compensation?

A participant will receive compensation if he or she is the first to submit the finding and provided that it is confirmed by the Confederation, the cantons and Swiss Post. The extent of compensation granted depends on the severity of the finding. The following categories have been defined.

Category	Minimum compensation in CHF
Best Practice (uncritical optimisation possibilities)	100
Intrusion into the e-voting system	1,000
Corrupting votes or rendering them unusable	5,000
Successful attack on voting secrecy on the	

servers	10,000
Manipulation of votes detected by the system	20,000
Undetected manipulation of votes	30,000 - 50,000

Details on the compensation to be granted can be found in the conditions of participation.

What rules do participants need to follow?

The rules of conduct and conditions of participation have been published here. These define exactly what participants are permitted to test, as well as compensation and the rules for publishing findings.

Whom should participants contact if they have questions about the intrusion test?

Questions can be submitted via a contact form on the www.onlinevote-pit.ch platform.

Where is the source code published?

Swiss Post published the source code here on 7 February 2019. Registration is required to view this. The source code is published permanently to ensure Swiss Post meets the legal requirements. More information on the source code can be found in the blog post.

More information on the intrusion test can also be found in the press release of the Federal Chancellery.