SWISS POST Menu

How findings are categorized in the public intrusion test

06.03.2019

Security Cantons

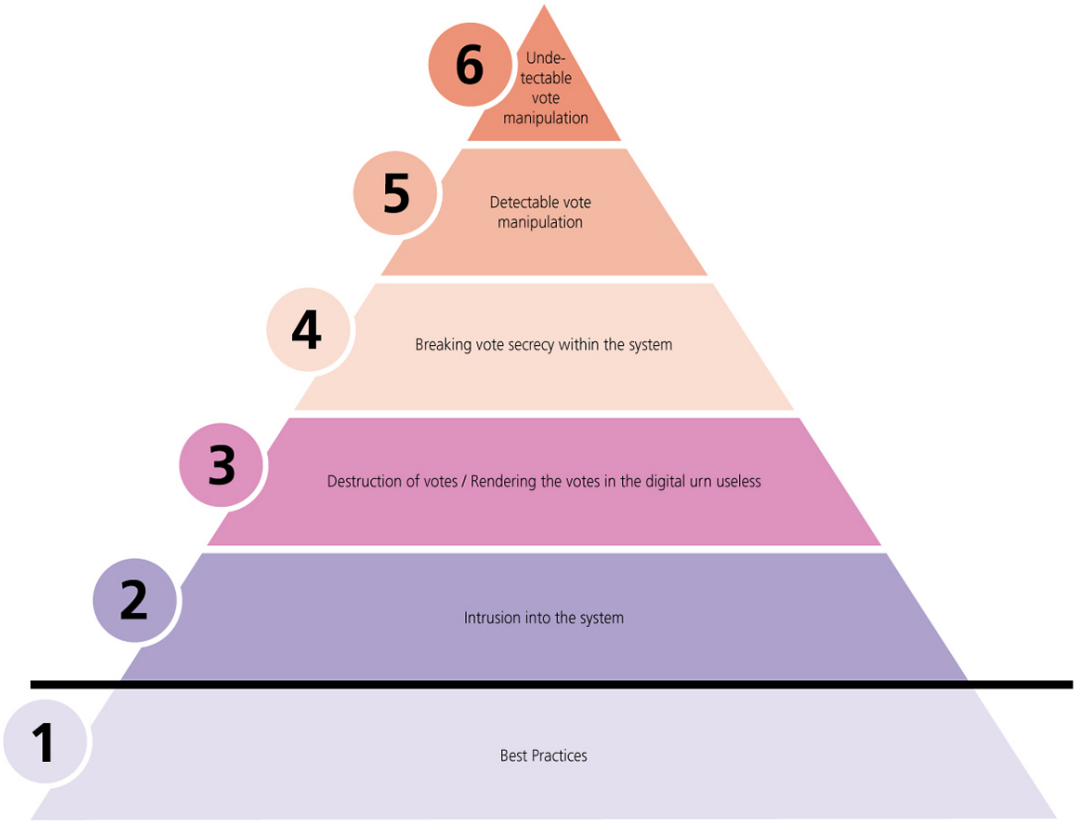
Swiss Post is conducting a public intrusion test on its e-voting system on behalf of the Confederation and the cantons from 25 February to 24 March 2019. Some 3,000 individuals from the IT security community around the world are challenging the e-voting system and will report any findings. How will these findings be handled and categorized? What compensation will Swiss Post pay if weak points are confirmed? This blog post provides the answers.

If, during the public intrusion test, a participant believes that he or she is able to manipulate the system or has found a weak point, he or she will report this on the platform at www.onlinevote-pit.ch. The independent company commissioned by the Confederation and cantons, SCRT SA, will perform an initial review of the findings. If a finding is plausible, SCRT SA will forward it to Swiss Post's e-voting experts to check. After the analysis, the participant will be informed by SCRT SA whether he or she has actually discovered a vulnerability. If a finding is confirmed, it will be published on the platform at www.onlinevote-pit.ch and the participant will receive compensation. In addition, researchers are free to publish their findings after they have been confirmed. Many other intrusion tests do not allow this.

The entire process is overseen by representatives of the Confederation and the cantons.

What happens if a finding is indeed confirmed?

Confirmed findings will be categorized as follows:



Category 1 Best Practices includes findings that show uncritical optimization opportunities. It is common for several findings of this category to come to light in intrusion tests, and some such findings are also expected in this intrusion test.

For a finding to be included in category **2 Penetration into the system**, a hacker must succeed in penetrating the servers of the e-voting system (i.e. gaining shell access). In itself, shell access is not sufficient for manipulating the electronic casting of ballots in a way that goes undetected. However, it would make it theoretically possible to carry out activities on the server which have effects on the system. Findings in this second category are compensated with at least CHF 1,000.

Category **3 Destruction of votes or rendering votes void on the server** is where we include successful attempts at tampering with the e-voting system in such a way that the counting of votes is no longer possible. These findings from category 3 will be compensated with at least CHF 5,000.

In category **4 Breach of voting secrecy within the system**, we include attacks on the system which allow attackers to find out who has voted, or how someone has voted, by means of snooping on the e-voting system. Should such an attempt be successful, the effort will be compensated with at least CHF 10,000.

For a finding to be included in **category 5**, hackers will succeed in **Manipulating votes in the ballot box**; i.e. turning "yes" into "no" votes, for example. Participants who manage this will be compensated with at least CHF 20,000 for his or her efforts.

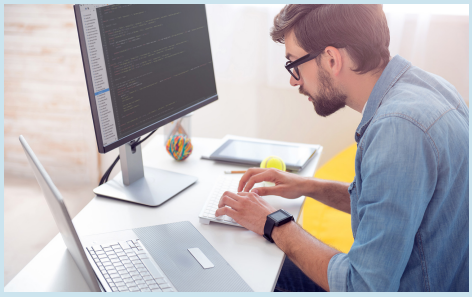
Manipulations of categories 1 to 5 will be detected and reported by the e-voting system and corresponding control mechanisms.

Should it be possible to **manipulate votes in the ballot box in such a way that the manipulation is not noticed during a normal ballot**, the finding would fall into **Category 6**. For successful penetrations of the system in category 6, compensation payments of between CHF 30,000 and CHF 50,000 are provided for.

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

The findings from the public intrusion test are incorporated into the further development of the latest generation e-voting system.

Share



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

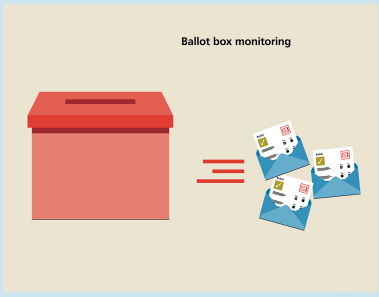
07.02.2019 | Swiss Post will be carrying out resilience testing, also known as a public intrusion test (PIT), on its e-voting system between 25 February and 24 March 2019. How does the intrusion test work and what happens if anything is found? The answers to the key questions.

More

Swiss Post publishes the source code for its e-voting system

07.02.2019 | Swiss Post is publishing the source code for its e-voting system in accordance with the requirements of the Confederation and cantons. The information published particularly relates to the core elements of the encryption components.

More



Are e-voting results verifiable?

11.06.18 | E-voting enables the elec to cast their votes and vote in elect electronically wherever they are an supplements the two existing optio Thanks to universal verifiability, vot electoral authorities have full contr times over the votes cast and can re detect any manipulation.

More