International Post Corporation

Swiss Post temporarily suspends its e-voting system

29-03-2019

The public intrusion test ordered by the Confederation and the cantons on Swiss Post's new e-voting system is complete. Although the electronic ballot box could not be hacked, feedback on the published source code reveals critical errors. Since the integrity of votes and elections is a top priority, Swiss Post is taking action. It will correct the source code and have it reviewed again by independent experts. It will therefore not provide its e-voting system to the cantons for the votes of 19 May.

Swiss Post conducted a public intrusion test (hacker test) on its new, universally verifiable e-voting system between 25 February and 24 March 2019. In addition to the intrusion test, it published the source code for its e-voting system on 7 February. Although the notarized ballot box could not be hacked, feedback on the published source code reveals critical errors (see press release and blog post). An error also affects the individually verifiable system used by the cantons of Thurgau, Neuchâtel, Friborg and Basel-Stadt since 2016. It can be ruled out that previous votes or elections have been manipulated. The error would cause invalid votes to be cast. This would systematically be detected on decrypting the ballot box.

Integrity is a top priority

The integrity of votes and elections is a top priority for Swiss Post. It is aware of the high level of responsibility it carries as the system provider of an e-voting system in Switzerland. It will therefore correct the source code and have it reviewed again by independent experts. Consequently, it will temporarily suspend operation of its system and will not provide it to the cantons for the votes of 19 May.

No manipulated votes

During the four-week endurance test, around 3,200 international IT experts inflicted targeted attacks on the new e-voting system. After the completion of the intrusion test, there were no manipulated votes in the electronic ballot box. The hackers did not manage to infiltrate the e-voting system. Attempts at overloading the system through DDoS attacks were unsuccessful. The hackers submitted a total of 173 findings. The Federal Chancellery, Cantons and Swiss Post confirmed 16 of them. They fall under the lowest classification level, "Best Practice", and are thus considered non-critical. The entire assessment process for the findings was overseen by representatives of the Confederation and the cantons. Swiss Post will take account of the findings in the further development of the new e-voting system. That was the very point of the public intrusion test and source code disclosure. The source code will remain open to the public to allow researchers to continue the verification process and report their observations to Swiss Post.

Source: Swiss Post