Final report
Public intrusion test (PIT)
Online voting system with universal verifiability

Drafted by Swiss Post for the
PIT Management Committee

25 June 2019
Berne, Switzerland

Table of Content

1. Management summary

Swiss Post conducted a public intrusion test (PIT) on its electronic voting (e-voting) system. The system with universal verifiability, which is not yet in use, was tested.

The aim of the PIT was to give independent IT specialists the opportunity to put Swiss Post's e-voting system to the test with deliberate attempts at manipulation and attack. Any vulnerabilities identified will be evaluated, classified according to severity and resolved depending on the risk involved. The results of the intrusion test will be used for the development of the e-voting system. Furthermore, a PIT is a requirement by the Swiss government and the cantons for systems with universal verifiability.

The public intrusion test was successfully conducted from 25 February to 24 March 2019, with 3,186 researchers and IT specialists from 137 countries taking part.

An appropriate Code of Conduct was drawn up, enabling Swiss Post to protect its other IT systems while offering participants legal security (impunity from prosecution).

A total of 173 findings were submitted. Most findings (145) were rejected by SCRT SA, the company mandated by the Confederation and the cantons, or proved to be duplicates (12). 16 of the findings (submitted by 12 researchers) were confirmed. According to the assessment of the Federal Chancellery and the cantons, all the accepted findings relating to possible vulnerabilities fall into the category of best practices (LOW severity and INFO). These researchers received remuneration. A total of CHF 2,000 out of CHF 150,000 was paid to the researchers for the 16 accepted findings.

In light of the number, quality and type of notifications, it can be said that qualified IT security experts subjected the system to a thorough test. At no point did any of the attacks compromise or infiltrate the system as a whole or individual parts of it. Nor were any votes manipulated (in the certified ballot box).

The entire PIT was observed and governed by representatives of the Swiss Federal Chancellery and of the cantons. Furthermore, an external notary's office certified the encryption, decryption and counting of the ballot boxes as well as the associated verification process.

There is a separate source code disclosure programme. In the public discussion, the intrusion test and the source code disclosure were often confused.

2. Introduction

Swiss cantons have offered online voting to members of their electorate since 2004. During this time, more than 300 trials have taken place during Federal votes and elections in 15 cantons. In order to expand online voting to a broader public, Federal regulations oblige the cantons to meet an additional set of requirements.[1] These include full verifiability of the system, performing numerous audits and publishing the software components' source code. Additionally, the Swiss Confederation and the cantons have decided that the systems need to be publicly tested within the setting of a public intrusion test (PIT).

Swiss Post complied with this obligation and organized a PIT from 25 February to 24 March 2019. This period of four weeks corresponded to the duration of a Swiss federal vote.

The aim of this final report is to summarize the PIT and give insights to the PIT Management Committee, which consists of representatives from the Swiss Federal Chancellery and canton representatives. The PIT Management Committee has observed the whole PIT and is the overarching governance in this instance.

Additionally, this report will be made public for interested experts and the broader public in order to be as transparent as possible.

3. Delimitation of the scope of this report

There is a separate source code disclosure programme. The source code programme is not the subject of this report.

Swiss Post published the source code and a technical manual of its next generation e-voting system on 7 February 2019.

The difference between the public intrusions test and the source code disclosure programme essentially consists of the following aspects:

- **Public intrusion test (PIT):**

  The researchers actively try to penetrate the running Swiss Post e-voting system from outside to manipulate votes. This test is a black box or grey box test. In such a test, the researchers have only limited information about the structure of the system, the source code of the software, interaction of the software and protection mechanisms.

- **Source code disclosure programme:**

  The source code and some specifications were made available to interested researchers worldwide for analysis and research purposes. The analysis of the source code is referred to as a white box or glass box test. There are no attacks on a running system from outside. Instead, the code is examined to learn about source code vulnerabilities. The source code disclosure programme has an unlimited duration, whereas the PIT had a specified time frame with a start and an end.

  Access to the source code required the acceptance of terms of use in order to ensure responsible disclosure and protect the copyright holders independent of participation in the PIT.
  Even after completion of the PIT, the source code remains disclosed.

  In the course of the public intrusion test, three major vulnerabilities in the source code were discovered and reported. The media and other stakeholders did not always distinguish between the source code disclosure program and the public intrusion test.

[1] https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting.html

4. Setup

4.1 Code of Conduct

A major effort was made to develop an appropriate Code of Conduct that would allow Swiss Post to protect its systems and provide a legal safe harbour for the participants (impunity from prosecution). The nature of Swiss criminal law and the lack of experience with bug bounty programs in Switzerland made this a complex endeavour. The expert feedback on the Code of Conduct for the public intrusion test was mostly positive.

Swiss Post has elaborated its Code of Conduct with representatives from the Swiss Federal Chancellery, canton representatives and with the support of experts in the field.

The key points of the Code of Conduct were:

- Swiss Post has committed to pay compensations for accepted findings (max. CHF 150,000)
- Participants retain the right to publish their findings, regardless of whether they were confirmed or rejected.
- The primary scope of the PIT included all attacks on the system aimed at reading votes or manipulating the election
- Swiss Post provided the participants with a legal safe harbour.

The full Code of Conduct can be found here: https://www.onlinevote-pit.ch/conduct/

4.2 Organization

The aim of the PIT was to give independent IT specialists the opportunity to put Swiss Post's e-voting system to the test with deliberate attempts at manipulation and attack. Any vulnerabilities identified will be evaluated, classified according to severity and resolved depending on the risk involved. The results of the intrusion test will be used for the development of the e-voting system. Furthermore, the PIT is a requirement by the Swiss government and the cantons and is therefore co-organized and supervised by the Swiss government and a specific group of Swiss cantons.

SCRT SA acted as contractor on behalf of the Swiss Confederation and the cantons. SCRT ran the online portal where the researchers registered and submitted their findings. SCRT was responsible for registration, issue management, pre-processing findings, first-level support and any queries the researchers had regarding the PIT.

A dedicated organization was built up for the duration of the PIT at Swiss Post. Due to the high number of participants and international interest in the PIT, the operational and support processes were adjusted to accommodate several thousand researchers.

The so-called PIT SWAT team, an interdisciplinary group of IT specialists within Swiss Post, met twice a day in order to process the findings pre-processed by SCRT on an ongoing basis and in the fastest and most effective way possible. In addition, our technology partner Scytl was closely involved in this process to provide an in-depth analysis and answer very specific questions put forward by the SWAT team.

SCRT SA operated as single point of contact for the researchers and was able to evaluate the majority of the findings during the pre-screening process so that Swiss Post was able to focus its efforts on the critical issues.

The Swiss Post PIT Management gathered twice a week in order to discuss the PIT SWAT team's results before they were presented to the PIT Management Committee. The final decision on whether a finding was accepted and published was made by the PIT Management Committee, which consisted of representatives from the Swiss Federal Chancellery and representatives from the cantons.

The interplay between all involved parties was very effective and successful. We would like to thank everyone involved for their efforts and valuable contributions that made this pioneering project a success. It was one of the first public tests of an online voting system anywhere in the world [2].

4.3 System and infrastructure

The scope of the PIT was strictly limited to the dedicated e-voting test system that is modelled 1:1 on productive systems. Any other Swiss Post services and infrastructures and any services and infrastructures for its customers, suppliers and any other public or private entities were off-limits.

4.4 Structure of the ballot

When preparing for real votes and elections, Swiss Post creates the necessary number of ballot boxes in accordance with the instructions received from the cantons. The canton generates the voting cards.

For the PIT, the number of ballot boxes and voting cards was nevertheless adjusted to optimize the testing conditions for the researchers. It was Swiss Post and not the cantons which created the voting cards.

For the purposes of the test, Swiss Post created 100, 000 voting cards. Of those, 99,000 were reserved for the researchers. These were divided up and assigned to ten different ballot boxes. Swiss Post kept 1,000 voting cards for itself. These were divided up and assigned to a further 39 ballot boxes.

The aim of this was to provide each researcher with a large number of voting cards to enable them to test the system comprehensively. Swiss Post retained some of the voting cards in case they were needed for forensic analyses or to reproduce the findings.

[2] In 2010, the Washington D.C. Board of Elections and Ethics (BOEE) asked specialists to conduct a public test of an online voting system. This involved an open source platform via which PDF files could be uploaded and downloaded (see Wolchok, Scott; Wustrow, Eric; Isabel, Dawn; Halderman, J.Alex. Attacking the Washington, D.C. Internet Voting System. In: Keromytis A.D. (eds) Financial Cryptography and Data Security. FC 2012. Lecture Notes in Computer Science, vol 7397. Springer, Berlin Heidelberg.

5. Participants

In total, **3,186 people** from the following countries registered for the PIT:

Country:	Percentage:
Switzerland	26.49%
France	13.15%
United States of America	6.84%
Germany	4.49
India	4.36%
Poland	2.89%
United Kingdom	2.86%
Canada	2.82%
Italy	2.54%
Spain	2.13%
Romania	1.44%
Turkey	1.41%
Ukraine	1.32%
Bulgaria	1.26%
Belgium	1.16%
Netherlands	1.16%
Hungary	1.00%
Others	22.68%

Illustration 1: Participant's countries of origin based on information provided by participants

Interesting to know:

- Exactly 4,500 different IP addresses accessed the pit.evoting-test.ch server via HTTP/HTTPS during the PIT. The origin of the IP addresses corresponds largely to the country table above.
- There were 651 IP addresses that sent more than 50 requests spread over more than 10 minutes (with 50 requests and 10 minutes being an arbitrary indicator of active engagement with the system).
- There were attempts to vote from 793 different IP addresses (Request to the Swiss Post authentication URI) via pit.evoting-test.ch.
- There were 954 IP addresses in total for these two groups, which corresponds to the number of active PIT participants. This corresponds with 30% of registered participants and was in line with Swiss Post's expectations

6. Findings

6.1 Overview

A total number of 173 findings were received on the PIT platform. 90 different people reported them. After careful inspection:

- 145 were rejected.
- 12 were duplicates.
- 16 were accepted and received a compensation.

All of the 16 findings that were accepted belong in the "best-practice" category. There were no accepted findings falling into a higher category. This means that it was not possible to compromise or infiltrate the system or parts of it at any point. Nor were any votes manipulated.

A total of CHF 2,000 out of CHF 150,000 was paid to the researchers for the 16 accepted findings. This corresponds to 1.33% of the total amount made available from Swiss Post to pay out as compensation for the PIT.

This report covers only those findings that have been exploited in the scope of the PIT and those that constitute a misconfiguration according to industry best practice. Findings which could not be exploited remotely or which are only visible in the source code were rejected for the PIT, but redirected to the source code programme where they were evaluated again. When evaluating whether or not findings should be accepted and compensated, the responsible bodies decided strongly in favour of the participants, even if the effective technical risk of the findings was minimal or sometimes non-existent.

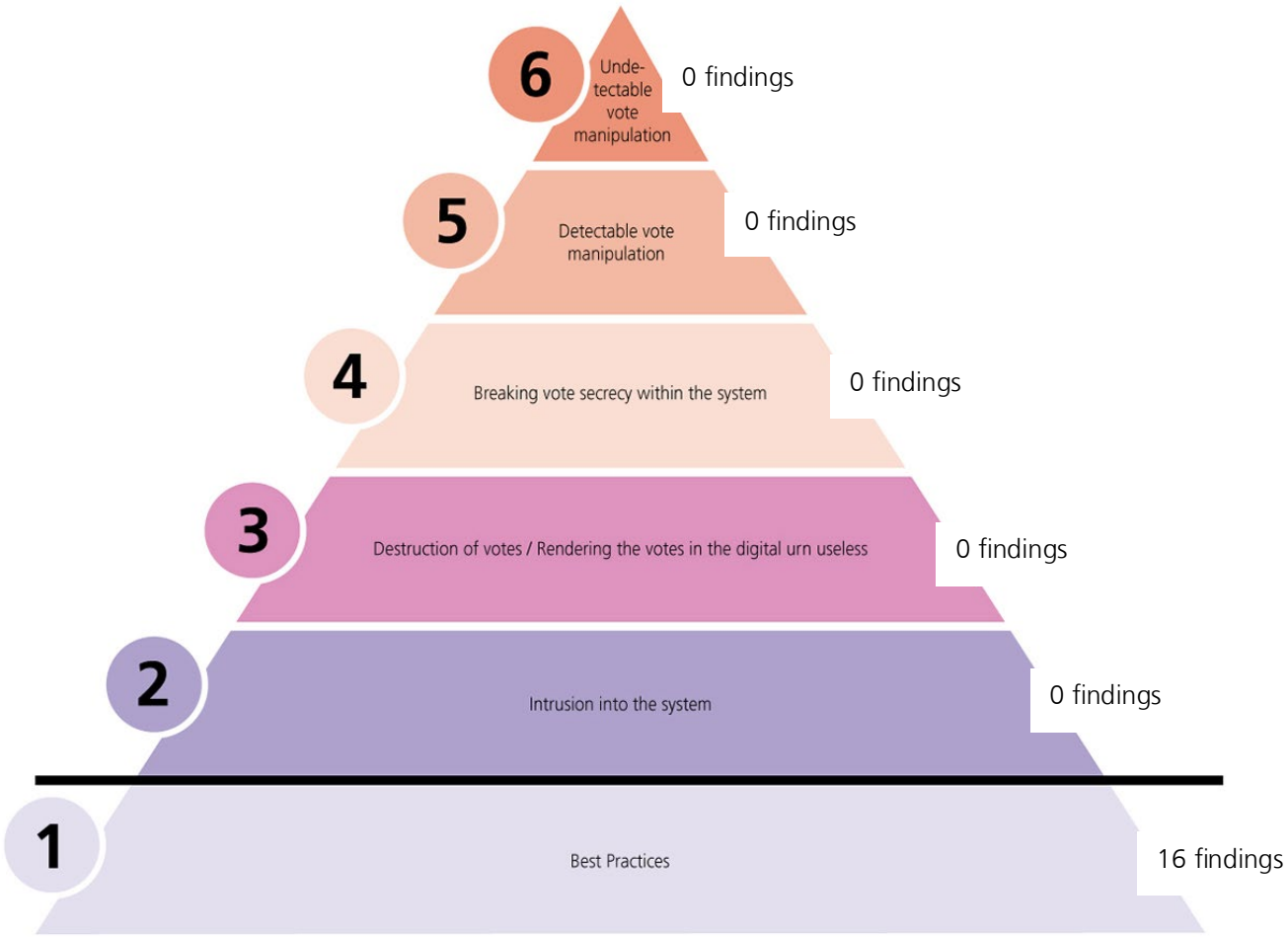

Illustration 2: In the PIT, 16 best practice findings were accepted. There were no findings in any other category

6.2 Severity HIGH (categories 5 and 6)

⇨ No findings of the severity HIGH were accepted during the PIT.

6.3 Severity MEDIUM (categories 2 to 4)

⇨ No findings of the severity MEDIUM were accepted during the PIT.

6.4 Severity LOW (best practice findings, category 1)

⇨ Three findings of the severity LOW were accepted during the PIT.

- **Crafted X-Forwarded-For HTTP header injection**
  By inserting a crafted X-Forwarded-For HTTP header in the requests performed for some of the web services, an attacker was able to insert a chosen IP address into the application logs of the back-end system. No impact on the voting process was demonstrated. It is advisable to implement a security best practice to prevent this issue. This will be fixed after the PIT.

- **Use of 'unsafe-eval' and 'unsafe-inline' in Content Security Policy**
  The e-voting system declares a Content-Security-Policy HTTP header containing the 'unsafe-eval' and 'unsafe-inline' terms. By doing so, it lowers the protection (at browser level) against the exploitation of hypothetical cross-site scripting (XSS) vulnerabilities.
  This is a known issue for which Swiss Post expected a report. Swiss Post is tracking it actively.

- **Use of cipher suites without forward secrecy support**
  The e-voting system accepts connections from clients (browsers) using TLS 1, TLS 1.1 & TLS 1.2. Two cipher suites, which are part of TLS 1.2 and accepted by the voting system, do not provide forward secrecy:

  TLS_RSA_WITH_AES_256_GCM_SHA384
  TLS_RSA_WITH_AES_128_GCM_SHA256

  These cipher suites are neither weak nor broken. However, the lack of forward secrecy implies that decryption of the messages between clients and the e-voting server would be possible in the future, if at some point an attacker succeeded in accessing the TLS encryption keys used by the e-voting server. It is important to note that the votes themselves are encrypted separately, before being transmitted over TLS. This finding therefore does not apply to the encryption of the votes, which would remain secure.

  Note that the server and the clients will generally only use these cipher suites if a stronger and better cipher suite supported by both of them is not available.

  Swiss Post plans a thorough review of the cipher suites permitted for use in the voting system after the PIT.

6.5 Severity INFO (best practice findings, category 1)

⇨ 13 findings of the severity INFO were accepted during the PIT.

Security findings of the severity INFO do not constitute a security finding in themselves. However, sometimes these small inconsistencies facilitate a bigger finding. Swiss Post has therefore accepted these issues and plans to solve them.

- **Missing HTTP to HTTPS redirection on 'pit-admin.evoting-test.ch'**
  Both HTTP (TCP/80) and HTTPS (TCP/443) ports are available on the address 'pit-admin.evoting-test.ch'. Security best practices state that, upon connecting to the cleartext HTTP port, clients should be automatically redirected to the encrypted (HTTPS) service instead. By blocking the client immediately instead of redirecting it, this system does not act in accordance with security best practices.

- **Outdated version of Bootstrap web framework**
  The landing page of the e-voting system uses a well-known front-end web framework called Bootstrap. The version of this framework that is used - 4.2.1 - is affected by a known vulnerability potentially leading to cross-site scripting (XSS) occurrences in some specific scenarios that do not apply here. However, it is a security best practice to use the latest version of a framework. The patch for this vulnerability (CVE-2019-8331) was released on 15 February 2019.

- **Vulnerable TLS cipher-suites (LUCKY13)**
  The front-end systems accessible at https://pit.evoting-test.ch and https://pit-admin.evoting-test.ch support and accept HTTPS connections using a variety of ciphers including cipher suites provided by outdated and vulnerable versions of TLS (TLS 1.0).

  While this may appear at first glance as not conforming to security best practices, it is actually done on purpose and in a way that does not make the e-voting system vulnerable to flaws derived from these weak cryptographic protocols. Indeed, connections using weak cipher suites are only accepted by the front-end (and not by the e-voting system itself) and are only used to display a message to the voters, instructing them to use a recent and up-to-date web browser. The e-voting system itself, on the other hand, only accepts connections using TLS 1.2 cipher suites.

  However, some specific cipher suites that are part of TLS 1.2 (and accepted by the voting system), specifically those using block ciphers with CBC mode of operation, may be vulnerable to a padding oracle attack known as “Lucky13”.

  While this vulnerability is known to be mostly theoretical and almost impossible to actually exploit outside of lab environments, it would be advisable to implement a security best practice and disable the use of these cipher suites altogether.

- **Missing 'Expect-CT' HTTP header**
  The 'Expect-CT' header - which is currently an Internet draft - has been proposed to allow sites to opt into reporting and enforcing certificate transparency requirements. The goal of this mechanism is to prevent the use of “rogue” certificates for a given domain from going unnoticed.

  The e-voting system does not implement this header and therefore does not benefit from this mechanism.

  Note that this header has not yet been formally adopted as a standard and may not be supported by all browsers yet.

- **Missing 'base-uri' in Content Security Policy**
  The Content Security Policy HTTP header declared by the e-voting system does not declare the 'base-uri' directive. By doing so, it lowers the protection (at browser level) against the exploitation of hypothetical cross-site scripting (XSS) vulnerabilities.

- **Incorrect 'HTTP-Strict-Transport-Security' header on 'pit-admin.evoting-test.ch'**
  When connecting to 'pit-admin.evoting-test.ch' on port 443, the server sends an HTTP-Strict-Transport-Security header even for plaintext HTTP connections, which is a violation of RFC 6797. The additional header also does not contain the 'includeSubdomains' directive, which would constitute a security best practice.

- **Multiple occurrences of 'X-XSS-Protection' HTTP header**
  Some error messages sent as responses by the web server (specifically, the '403 Forbidden' status code) include two identical occurrences of the 'X-XSS-Protection' security header. This behaviour is non-standard, and could lead to undefined behaviour in some browsers.

- **Use of outdated version of AngularJS**
  Both voter and admin portals use a well-known JavaScript web framework called AngularJS.
  The version of this framework used by the e-voting system is 1.6.9. While no vulnerability is currently known to affect this version, it is however not supported anymore and should therefore be upgraded to a currently supported version.

- **Strict Transport Security misconfiguration**
  Upon the reception of requests where content has been tampered with, the server usually responds with an error message. In some specific cases (e.g. status code 422) this response may include two occurrences of the 'Strict Transport Security' HTTP header with inconsistent contents (the declarations on both headers are not identical).

  This behaviour is non-standard, and could lead to an undefined interpretation of the 'Strict Transport Security' directives in some browsers. As HSTS preloading is used, this should however not cause insecure situations.

- **Missing charset declaration in some response's Content-Type header**
  Some HTTP responses sent by the e-voting system are missing the charset parameter in the Content-Type header.

  While this does not currently have any known impact, it is however a breach of secure development best practices.

- **Missing CSP header in redirect responses**
  Some responses from the e-voting server - specifically "302 Redirect" re-directions - are missing Content Security Policy HTTP headers. They are thus inconsistent with the rest of the application and in breach of security best practices.

- **Cross-origin request possible on specific endpoint**
  One specific endpoint of the e-voting system - /extended_authenticate - accepts 'text/plain' content-type instead of the 'application/json' observed for other endpoints.

  Because of this and due to the fact that for 'text/plain' content-type, the browser does not perform a "pre-flight" CORS check, it is possible to perform requests to this endpoint from any arbitrary origin domain.

  While the usefulness of this attack appears to be very limited, this configuration is not consistent with security best practices.

- **Missing CSP header on http://pit-admin.evoting-test.ch/**
  Upon connection attempts to http://pit-admin.evoting-test.ch/ (using plain HTTP), the server responds with a '403 Forbidden' response and effectively rejects the connection attempt. This response does not however define a Content Security Policy (CSP) header, which is inconsistent with security best practices.

6.6 Rejected findings

Of the findings which did not receive any compensation, the majority were rejected during the pre-screening process by SCRT. These are not covered in this report.

Swiss Post adopted a forthcoming policy with the acceptance of the PIT findings. Swiss Post accepted most findings that passed the SCRT pre-screening process.

However, there were seven exceptions to this general approach. Swiss Post rejected the following findings, even though they did pass the pre-screening stage by SCRT:

- **No "partial-abstention" verification codes**
  The conceptual attack reported is not possible by design. The system does not provide the option of not participating for individual ballots. This is a deliberate design choice and not a functional bug.

- **No brute force protection**
  No security impact could be demonstrated based on the lack of brute force protection, as enumerating initialization codes is unrealistic given the size of the namespace.

- **Ability to create a 408 request timeout on the API**
  The researcher sent a bad request and misinterpreted the correct behaviour of the server as a sign of a successful attack.

- **Vote manipulation - session manipulation**
  The finding does not constitute a manipulation of a vote. It was an unsuccessful man-in-the-middle attack. The system behaved as expected.

- **HTTP body sanitization bypass request**
  The finding is relevant for the source code access programme and has been forwarded for further evaluation. However, the malicious payload proposed was detected on the Swiss Post front-end servers and the attack failed on the life system. The finding is therefore not relevant in the scope of the PIT.

- **Outdated version of Node.js dependencies**
  The reported Node.js is only used during unit testing, but not in the productive e-voting systems.

- **Trusted Types not used in Content Security Policy**
  Trusted Types is an experimental proposal that has not been adopted as a best-practice standard by the security industry.

  Note that this rejection contrasts with the finding pertaining to the Expect-CT header, which Swiss Post has accepted (see above). In Swiss Post's opinion, Expect-CT is more advanced in its development than Trusted Types and can therefore be considered close to an industry best practice, while Trusted Types cannot.

7. IT operations

7.1 IP addresses participating in the PIT

Two IP addresses were prepared for the PIT. One IP address corresponded to the e-voting server itself (pit.evoting-test.ch), while the other corresponded to the admin portal (pit-admin.evoting-test.ch).

7.1.1 pit.evoting-test.ch

- Exactly 4,500 IP addresses accessed the server pit.evoting-test.ch via HTTP/HTTPS during the PIT.
- There were 651 IP addresses that sent more than 50 requests spread over more than 10 minutes.
- 793 IP addresses attempted to vote via pit.evoting-test.ch.
- The total of these two groups consists of 954 IP addresses. These IP addresses are considered to be active PIT participants.
- 477 IP addresses successfully cast at least one vote.

7.1.2 pit-admin.evoting-test.ch

- A total number of 2,281 IP addresses accessed the server pit-admin.evoting-test.ch via HTTP/HTTPS during the PIT.
- Three IP addresses were able to pass the multiple authentication and authorization steps to connect to the administration portal. All three IP addresses were known Swiss Post IP addresses used by Swiss Post administrators and constituted planned and permitted access. No researchers were able to pass the multiple authentication and authorization steps to connect to the administration portal.
- As no researchers were able to access the Admin portal successfully, the remainder of this report concentrates on the voter portal.

7.2 IPs per country

The geo-location of the actively participating IP addresses closely mirrors the self-declared country of origin of the registered participants on the OnlinePit-Vote platform. In fact, the first five countries are identical except for the order of Germany and India, whose positions need to be inverted for the active PIT.

Country	IP Count	Percent
CH	267	27.93%
FR	93	9.73%
US	75	7.86%
IN	68	7.12%
DE	41	4.30%
PL	35	3.67%
GB	30	3.15%
NL	23	2.42%
ES	22	2.31%
IT	21	2.21%
BE	16	1.68%
UA	11	1.16%
TR	11	1.16%
SE	11	1.16%
EG	11	1.16%
RO	10	1.06%
HU	10	1.06%
Various	199	20.86%
Total	954	100.00%

7.3 Duration of test per IP

- Several IPs were active for almost the full duration of the PIT. However, the median duration during which the IPs were actively performing HTTP requests was 49 minutes.

7.4 Number of requests

- The 954 IP addresses actively participating in the PIT performed a total number of 953,061 requests against the voter portal.
- This means that on average, there were 999 requests with a median of 128 requests per IP and a standard deviation of 7,744 requests.

7.5 Status codes

The 953,061 requests resulted in the following HTTP status codes statistics:

Entry	Count	Percent
200	358255	37.59%
206	74	0.01%
301	24419	2.56%
302	6993	0.73%
304	316	0.03%
400	29846	3.13%
401	3151	0.33%
403	275868	28.95%
404	217149	22.78%
406	57	0.01%
408	34660	3.64%
412	1	0.00%
413	22	0.00%
414	1	0.00%
415	20	0.00%
416	4	0.00%
417	21	0.00%
422	703	0.07%
500	1492	0.16%
503	9	0.00%
Total	953061	100.00%

The absence of status codes 502 point to a good availability of the back-end system.

The 1,492 requests that led to the status code 500 need to be analysed more closely. With regard to these requests, no findings were reported. One or two situations in which the voting server returned the status code 500 were already known. No finding was reported concerning these requests. Even before the PIT, there were one or two situations where the voting server responded with a status code 500.

Further analysis made it possible to establish an additional third case, where the voting server responded with a status 500. This constitutes an error and has been reported to Scytl.

Protection measures on the reverse proxy make it very difficult for an attacker to exploit this kind of backend failure further.

7.6 Voting process

The researchers probed the voting process extensively. In a normal vote, the requests to the voting servers closely mirror the steps in the voting process. However, the voting protocol makes it possible to repeat the same requests multiple times, and the voting server will act accordingly without this being transparent to the client (possibly an attacker).

The requests from the researchers can therefore be summarized as follows:

Request	Number	
Login attempts	231,556	(from 662 different IPs)
Login successes	3,969	(from 647 different IPs)
Login fails	227,587	(from 488 different IPs)
Auth token successes	2,588	(from 607 different IPs)
Auth token fails	4,822	(from 56 different IPs)
Vote submission successes	1,757	(from 510 different IPs)
Vote submission fails	11,234	(from 80 different IPs)
Vote confirmation successes	4,251	(from 477 different IPs)
Vote confirmation fails	2,972	(from 54 different IPs)

Illustration 3: Voting process requests

In a normal Swiss vote, the login fails are below 10% of the successful logins and there are very few additional fails.

7.7 OWASP ModSecurity Core Rule Set

The voter access to the e-voting system is protected by the OWASP ModSecurity Core Rule Set (CRS). CRS is configured at paranoia level 4, the highest paranoia level available in the rule set. Swiss Post has fine-tuned the CRS installation over the course of several years. This means that very few false positives remain and the positives triggered by the rule set can generally be seen as indicators of an attack.

A total of 53,537 requests were blocked due to alerts triggered by the CRS. Note that some of the alerts were below a certain anomaly threshold and were therefore ignored, unless they came with additional violations in the same request.

7.8 ModSecurity whitelisting

- Voter access to the e-voting system is protected by a custom whitelist that covers API endpoints (URIs), parameters and certain other characteristics of the requests.
- It is technically possible that a request triggers one or several CRS rules and whitelisting rules before eventually being blocked or redirected to the encrypted port of the service. The numbers presented in the previous sections are therefore not identical to the numbers presented here.
- A total number of 314, 939 whitelist violations were observed within the set of requests performed by the participating IP addresses.
- A total of 221,302 requests were blocked due to whitelist violations.

7.9 ModSecurity JavaScript HashCheck

- The JavaScript files returned to the voting clients are tested for consistency on the way to the client. (This security check aims to protect the security of the vote from internal attackers.)
- These tests were passed by 71,885 requests. On 759 occasions, this test failed due to a weak cipher used by the client (a known issue with the rule set). However, 42 failures are not readily explainable.
- On the productive system, this check only fails in rare edge cases. The 42 failures will have to be investigated further.
- Note that no finding has been reported with regards to this possible misbehaviour.

7.10 Additional security measures

The e-voting system in use has additional security measures that further minimize the chances of an external attacker reaching the e-voting servers. However, these measures were switched off in accordance with the PIT Management Committee for the public intrusion test.

7.11 Mod_qos

Mod_qos has been used to defend against DoS attacks and to slow down aggressive scanners, which could pose a threat to the availability of the e-voting system. There is zero tolerance for scanning in the productive e-voting setup, and any detected scanners would be stopped right away. That is why the back-end systems are not built to cope with aggressive scanning / probing / fuzzying of requests. For the purposes of the PIT, additional protection for the back-end systems had to be implemented in order to guarantee the availability of the system.

After DoS threats were received and DoS probes were observed in the days leading to the start of the PIT, relatively hard qos limits were enforced that led to the temporary blocking of IP. Observations during the first days of the PIT showed that qos unnecessarily hindered a number of researchers in their analysis. The limits were therefore relaxed on 27 February (see below).

The following number of IP addresses were blocked on the individual date:

2019-02-25: **93**
2019-02-26: **43**
2019-02-27: **29**
2019-02-28: **26**
2019-03-01: **22**
2019-03-02: **21**
2019-03-03: **12**
2019-03-04: **8**
2019-03-05: **14**
2019-03-06: **11**
2019-03-07: **20**
2019-03-08: **7**
2019-03-09: **7**
2019-03-10: **10**
2019-03-11: **12**
2019-03-12: **8**
2019-03-13: **8**
2019-03-14: **6**
2019-03-15: **11**
2019-03-16: **7**
2019-03-17: **6**
2019-03-18: **9**
2019-03-19: **5**
2019-03-20: **5**
2019-03-21: **5**
2019-03-22: **11**
2019-03-23: **3**
2019-03-24: **3**

A total of 335 individual IP addresses were temporarily blocked by mod_qos.

7.12 Maintenance changes

The OpenSSL project announced an OpenSSL release for 26 February 2019. The release notes indicated a possible security flaw in the SSL/TLS ciphers used by the voting portal. Swiss Post asked the PIT Management Committee to agree on the update of the software of the reverse proxies to the new version. The PIT Management Committee agreed to this proposal.

This change was carried out on 27 February 2019, without any downtime for the researchers.

The relaxation of the strict qos settings was scheduled and implemented during the same change, and the execution went equally smoothly.

7.13 Reverse proxy

The reverse proxy performed as expected and caught most of the attacks. The majority of the findings were discovered on the reverse proxy. The analysis of these findings reveals that the maturity level of the reverse proxy is very high, because only three findings with low severity and several findings with severity info remain to be fixed.

8. IT security

8.1 Overview

The PIT has not caused any significant operational challenges for Swiss Post. Our current cyber defence assessment shows that most of the participants have followed the Code of Conduct.

The following graphic shows the geographic distribution of the client IP addresses that were involved in the security events registered on our Internet perimeter:

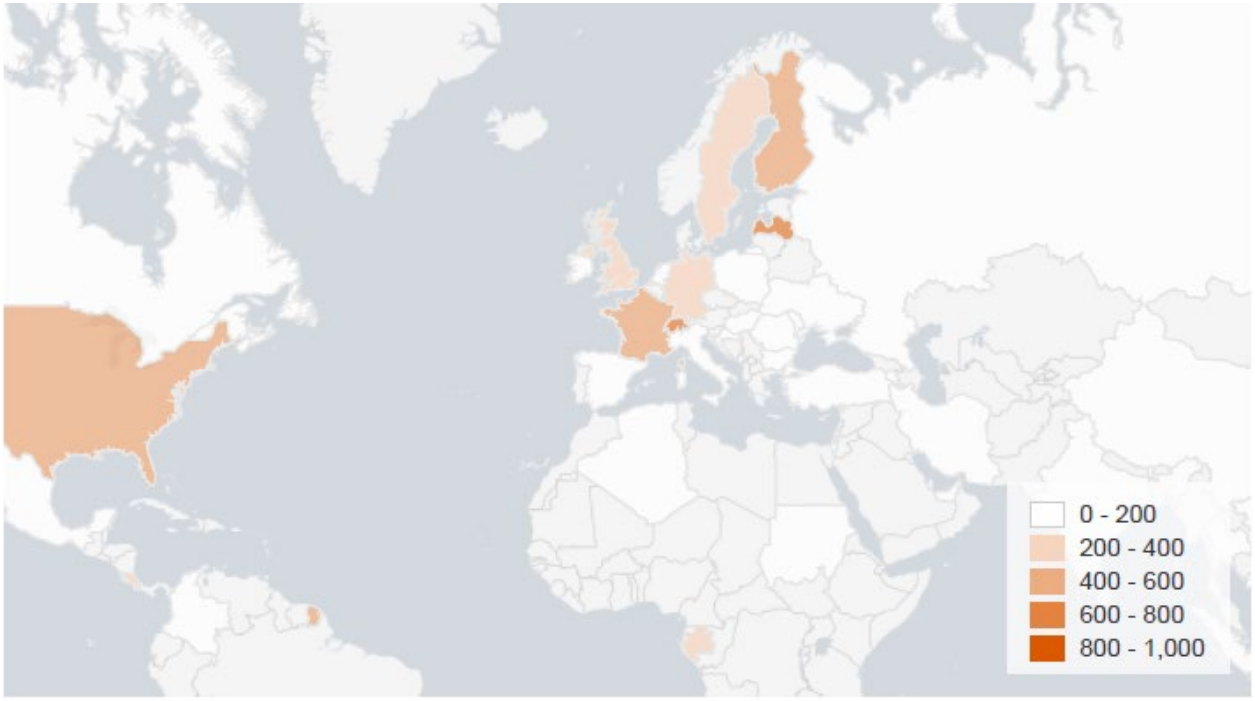

Illustration 4: Geographic distribution of registered security events during the PIT

If the configuration had been used for real votes, 74% of the network traffic generated during the PIT to the e-voting server would have been blocked due to traffic shaping, rate limiters, etc. But in order to lower the entry barrier for the researchers, our scrubbing system was put in simulation mode / deactivated.

8.2 DDoS attack

On 27 February 2019, there was a short peak in the network traffic because of a DDoS attack (UDP floods) without any effects on the availability due to an automatic mitigation on the Internet backbone.

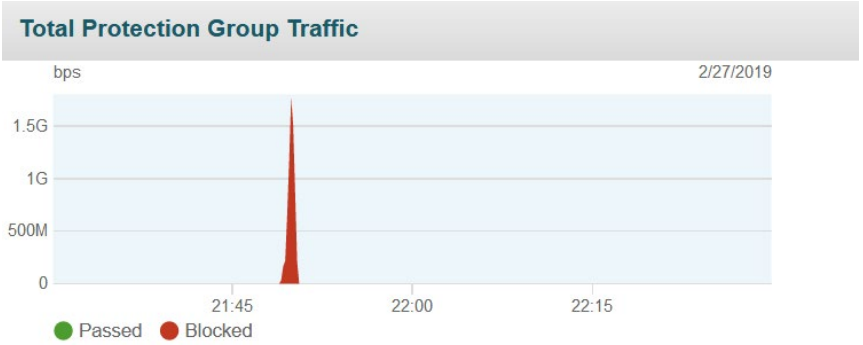

Illustration 5: Peak in the network traffic due to a DDoS attack

8.3 Attack trends

As expected, on both the intrusion prevention systems and the web application firewalls, a large number of security events were registered during the PIT for the servers, many of them due to well-known security scanners. No suspicious events were recorded on endpoint instruments.

No unauthorized access was recorded on the Swiss Post systems at any time.

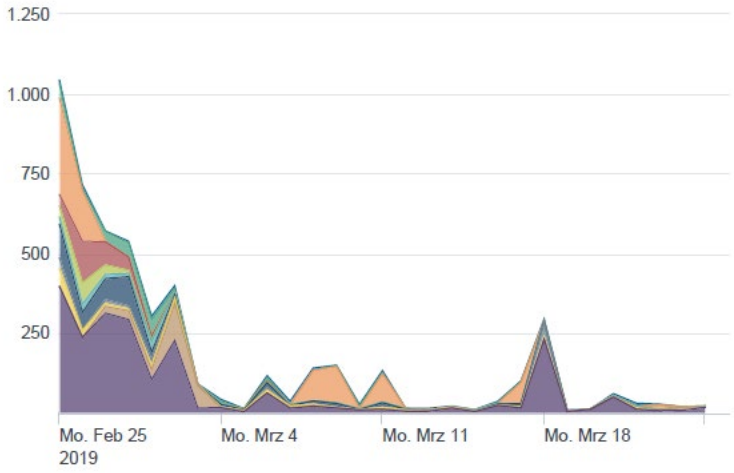

Illustration 6: Attack trend IPS

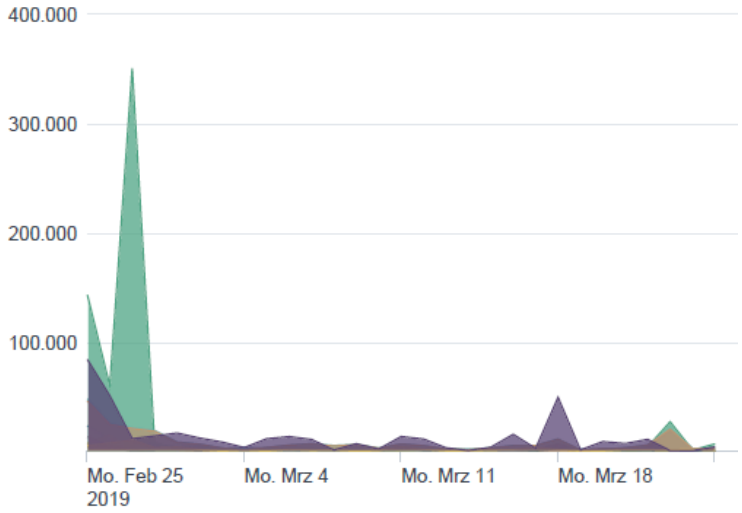

Illustration 7: Attack trend reverse proxy

The following cumulative graph shows the time course and categorization of client IP addresses that took place during the PIT:

- Green: Source IP addresses that successfully started a vote without any suspicious behaviour (84)
- Yellow: Source IP addresses that successfully started a vote and showed suspicious behaviour on other non-PIT Systems (436)
- Red: Source IP addresses that didn't start a vote but showed suspicious behaviour on both PIT and non-PIT systems (3587)

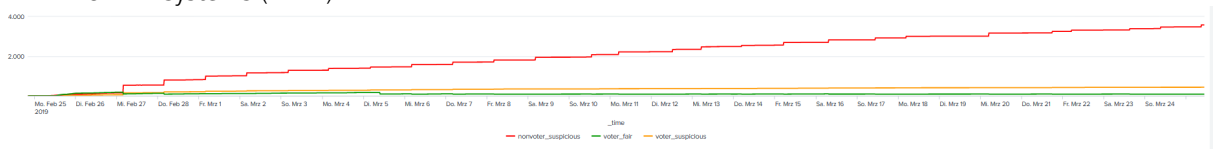

Illustration 8: Source IP address classifier

9. Application monitoring

The PIT infrastructure was stable during the entire PIT. At no time was there a threat to its availability. There is evidence from a large number of independent sources that the system was not compromised or infiltrated.

9.1 Workload during PIT

The following chapter contains various graphs which show the condition of the PIT infrastructure during the PIT. None of the defined thresholds for acceptable workload were reached, neither for individual components nor for the infrastructure as a whole. The PIT infrastructure would have been able withstand a workload ten times greater.

9.1.1 Control components

The graph below shows the average values of the received loads of all Linux control components. Since the control components are physically redundant twice, the load could be processed at any time without problems.

For the control components there were 74 CPU cores available, of which no more than 1.6 CPU cores were used (2%).

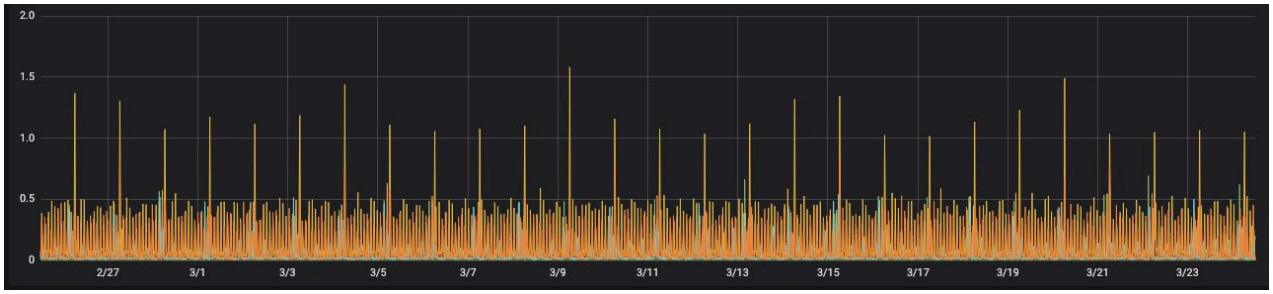

Illustration 9: Overview CPU usage control components

9.1.2 CPUs

The following graph shows the CPU utilization of all active PIT e-voting server systems during execution. The load was never higher than 23% on single online voting systems. Given that the threshold for manageable CPU utilisation is 80%, it is evident that the systems easily withstood the PIT.

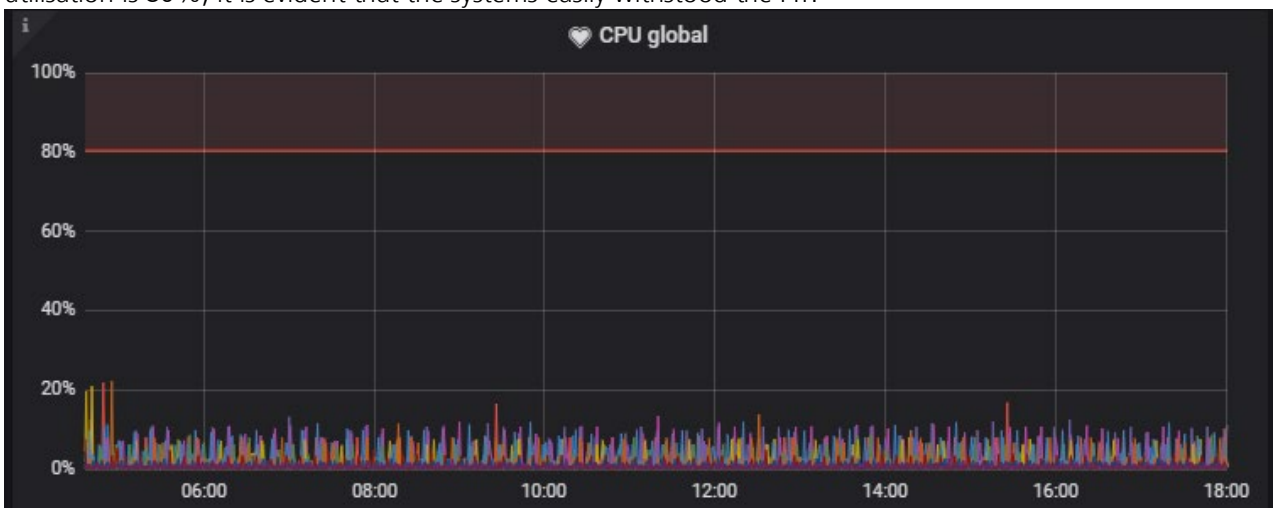

Illustration 10: PIT CPU global usage

9.1.3 Network

Below you can see the internal network traffic (network traffic within the PIT infrastructure) during the PIT. The load over the entire period was minimal and was never hazardous to the systems. This is due to the diligent architecture of the system and the various layers of security measures implemented. Only small temporary peaks are visible. These are due to attempted brute-force attacks. It is also easy to see that the load and activity at the beginning of the public intrusion test was considerably higher than towards the end.

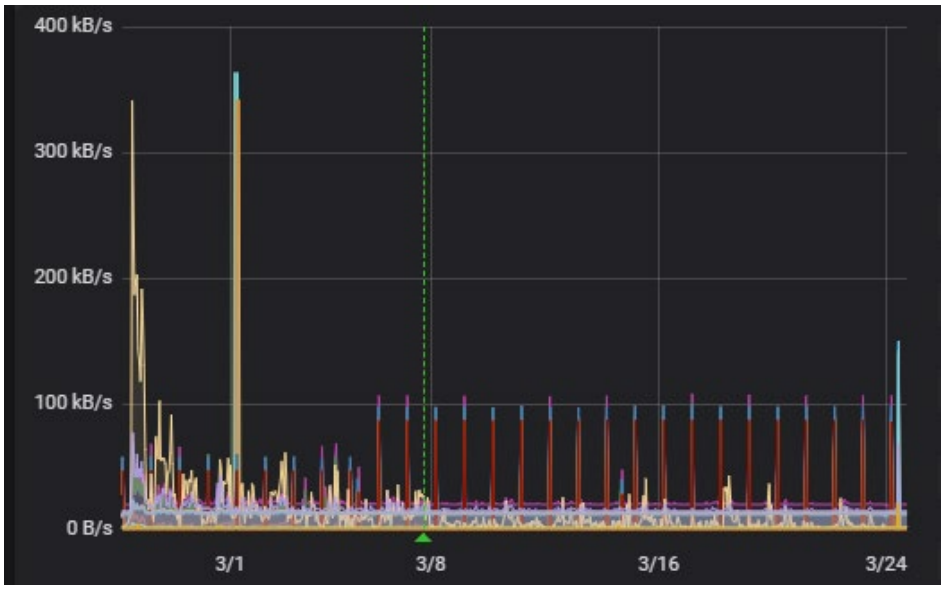

Illustration 11: PIT network utilization

9.1.4 Message queues

Below is an overview of all message queues in the PIT environment. It shows the number of messages in the individual queues over the entire execution period. The queues were not used to full capacity at any time. Peaks were noticed at the beginning of the PIT. Our experience with votes with a comparable number of participants (about 3,000) is that the number of the messages per queue can be many times higher and can be processed by the broker system without any problems.

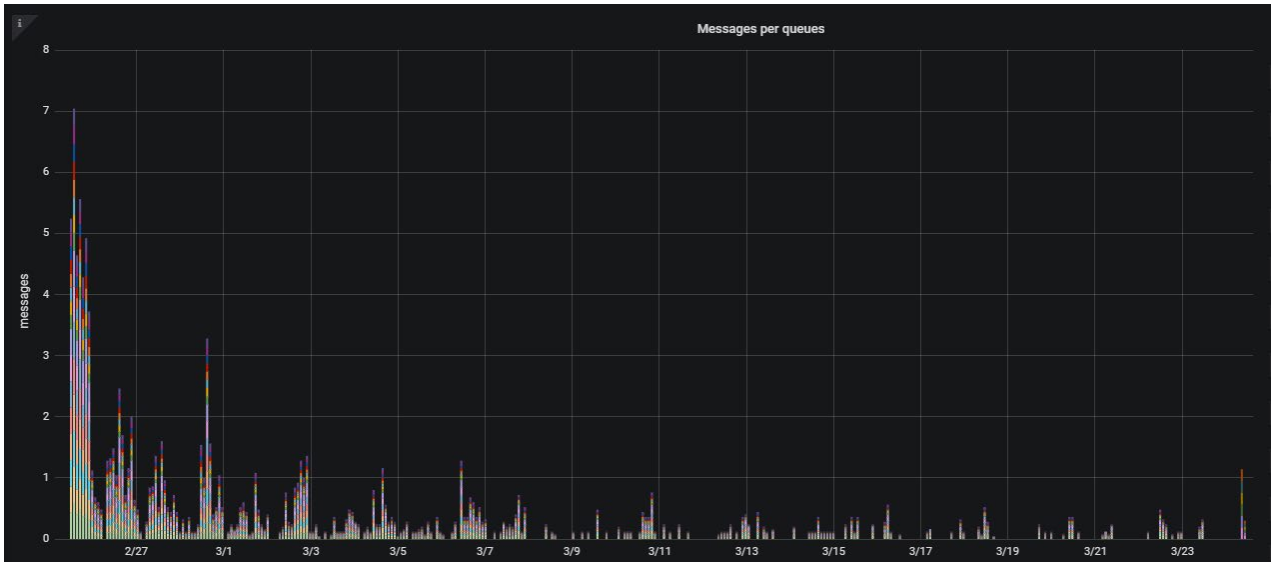

Illustration 12: PIT message queues

9.2 Monitoring and alarming

The standard Swiss Post security regulations for server systems were developed and implemented for the public intrusion test with extended security standards. These include dedicated autonomous and decoupled server systems as well as dedicated network zones. Internal communication is restricted and secured by internal firewalls.

At each security layer level, standard monitoring points were set up with extended monitoring points. These monitoring points were implemented with three different monitoring tools running in parallel. SPLUNK for Log, HP OVO and Grafana for resources, application, endpoints and process monitoring were used. Defined thresholds were used, which also allowed a proactive view of the overall system.

9.2.1 Noticeable actions on an application system

The only noticeable action of a researcher during the entire PIT run was a permanent brute-force attack with invalid initialization codes. The following graphic shows a part of the consistent log in attempts. These attacks were noticed by our monitoring system and we could check and estimate whether these attempts had an influence on the overall system. Since the system was never endangered, no mitigating steps were taken against these attacks.

Id	mytime	AnzahlFehlversuche
66d22222222222222222222222222222	2019.03.03 10	16
82222222222222222222222222222222	2019.03.03 10	16
82d22222222222222222222222222222	2019.03.03 10	16
892222222222222222222222222222222	2019.03.03 10	16
8992222222222222222222222222222222	2019.03.03 10	16
8a22222222222222222222222222222222	2019.03.03 10	16
8a8f22222222222222222222222222222222	2019.03.03 10	16
a022222222222222222222222222222222	2019.03.03 10	16
a08f22222222222222222222222222222222	2019.03.03 10	16
a0922222222222222222222222222222222	2019.03.03 10	16
a0d22222222222222222222222222222222	2019.03.03 10	16

10. Vote and ballot box verification

10.1 Introduction

As an additional verification measure, an external notary submitted 10 control votes in a dedicated ballot box at the beginning of the PIT. The external notary also verified the encryption process at the beginning of the PIT as well as the decryption process after the PIT through an electoral board.

The results at the end of the PIT were consistent with the values of the control votes recorded. This is additional evidence that the votes were not manipulated.

The PIT Management Committee, which consists of representatives of the Swiss Federal Chancellery and representatives of the state chancelleries of the cantons, also observed these procedures.

10.2 Votes cast

ID	Ballot box	Confirmed votes
1	Participants (public intrusion test)	773
2	Verification ballot box	10
3	Smoke tests	5
4	Test ballot box D2	3
5	Test ballot box D3	1
Total		792

10.3 Cryptographic verification

Following the decryption, the verification of the ballot was carried out with the Swiss Post-Scytl verification software. This software enables independent bodies to verify the ballot within the framework of universal verifiability.

A total of 54 verification points were checked in four different verification blocks: pre-election verification, ballot box verification, mixing-decryption verification and result verification.

It was already known to Swiss Post that three of these 54 verification points could not be passed successfully for the results of the PIT. An explanation of the functioning of this verification process is provided below to show why this failure to pass certain verification points is not due to security problems.

The verification process is based on cryptographic evidence through correct mixing and decryption of the votes and on secure audit logs (SecureLogs) which log the operations performed by the control components. The SecureLogs of the control components are compiled (copied) and consolidated using the Splunk monitoring and reporting software.

The following tests failed during the PIT closing ceremony:

- **Check Secure Log Integrity and Check Secure Log Signature:**

  The aim of these tests was to determine the integrity and authenticity of the SecureLogs. This prevents an attacker from modifying individual log entries or outputting a fake SecureLog file as a real one. This is achieved by concatenating each log entry with the preceding log entry (HMAC chain). The integrity of this HMAC chain is verified by the "secure log integrity test". At the same time, individual log entries are locked with a private key from the control component. By using the public key of the control component, the verifier can determine the authenticity of the SecureLogs beyond any doubt ("secure log signature" test).

Due to the magnitude of the PIT event, with over 8 GB log files and 4 million log entries, it went unnoticed when Splunk swapped the order of the log entries when consolidating the log files in very rare cases (if log entries are stored in the same millisecond). This broke the integrity of the HMAC chain in the data exported by Splunk. It is important to note that the original log files had not been altered and therefore the integrity of the HMAC chain in the original files was always intact.

Subsequently, a change was made to the Verifier to allow the Verifier to process the original SecureLogs of the CCs instead of the Splunk export. Thanks to this modification, it was determined that SecureLogs of the control components were integral and authentic in the public intrusion test. After the adjustments were made, both tests were successful.

- **Check vote ballot box:**

  This test compares the votes processed by the control components with the votes in the ballot box on the voting server. The goal of the test is to prevent an attacker from deleting votes in or adding votes to the ballot box.

  However, during the public intrusion test, there were eight voting attempts which did not correspond to a valid vote. For example, an attempt was made to vote YES and NO for the same question. After the vote was processed by the control components, the invalid vote was recognized by the system because a corresponding verification code could not be generated. The system displayed an error message to the voter, the voting card was blocked and the invalid vote was not placed in the electronic ballot box. This corresponds to the expected system behaviour (the voter can still vote by letter or at the ballot box). The verification software detected this behaviour because the eight votes were processed and locked by the control components, but were not stored in the ballot box.

11. Conclusion

Swiss Post feels that it should be considered a success that no successful attack was made on the system:

- At no point did any of the attacks compromise or infiltrate the system as a whole or individual parts of it. Nor were any votes manipulated (certified ballot box).
- At the end of the PIT, all votes could be decrypted and the system behaved flawlessly.

The participants' work nevertheless identified failings in the "best practices" category, thereby enabling Swiss Post to further increase the security of the system as a whole.

3,186 researchers and IT specialists from 137 countries registered for the PIT.

A total of 173 findings were submitted. Most findings (145) were rejected by SCRT SA, the company mandated by the Confederation and the cantons, or proved to be duplicates (12). 16 of the findings (submitted by 12 researchers) were confirmed. According to the assessment of the Federal Chancellery and the cantons, all the accepted findings relating to possible weaknesses fall into the category of best practices (LOW severity and INFO). These researchers received remuneration. A total of CHF 2,000 out of CHF 150,000 was paid to the researchers for these 16 confirmed findings.

In light of the number, quality and type of notifications, it can be said that qualified IT security experts subjected the system to a thorough test.

The attacks on the application had already largely failed at the first line of defence (reverse proxy / ModSecurity) and the second line of defence (sanitization of the requests by the API Gateway).

Most of the participants complied with the Code of Conduct. Occasional violations of the Code of Conduct were expected by Swiss Post and handled without any problems. These included scanning outside the e-voting systems and a minor DDoS attack on 27 February 2019.

Due to the high number of participants and international interest in the PIT, the operational and support processes were adjusted to accommodate several thousand researchers. The PIT infrastructure was also mapped out for a heavy stress test. An interdisciplinary team of IT specialists from various units concerned was available throughout the duration of the test. As the test appealed to an international audience, it had to be available at all times during the day and night, and at weekends.

In the public discussion, the intrusion test and the separate source code disclosure were often confused.

The PIT has shown that the e-voting system is currently so strong, that it is extremely difficult to infiltrate it from the outside. There are only a few accessible endpoints, which are very well protected.