Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Cancelleria federale CaF

Agosto 2019

Voto elettronico – Test pubblico d'intrusione 2019

Rapporto finale del Comitato direttivo

Sistema testato: sistema completamente verificabile della Posta svizzera (versione di febbraio 2019)

Indice

1 Scopo del documento

Il presente rapporto riassume la struttura organizzativa, lo svolgimento e le conclusioni tratte dal test pubblico d'intrusione 2019 (*public intrusion test*; PIT) al quale è stato sottoposto il sistema di voto elettronico della Posta svizzera.

2 Contesto

Sulla base dell'articolo 8*a* della legge federale sui diritti politici (LDP, RS 161.1), dal 2004 i Cantoni sperimentano il voto elettronico nel quadro del progetto *Vote électronique* (VE) della Confederazione e dei Cantoni. Il diritto federale disciplina i criteri per lo svolgimento delle prove di voto elettronico nell'ordinanza sui diritti politici (ODP, RS 161.11) e nell'ordinanza della CaF concernente il voto elettronico (OVE, RS 161.116).

In totale 15 Cantoni hanno più volte permesso a parte del proprio elettorato di votare via Internet in occasione di vari scrutini federali. Dal 2015 vengono impiegati sistemi dotati della cosiddetta verificabilità individuale. Tuttavia, per ampliare ulteriormente il voto elettronico, è necessario introdurre la cosiddetta verificabilità completa. Per autorizzare l'impiego di un simile sistema, l'OVE esige una certificazione preliminare e la pubblicazione del codice sorgente.

Nell'aprile del 2017 la Confederazione e i Cantoni hanno deciso di condurre anche un progetto pilota inteso a sottoporre i sistemi di voto elettronico completamente verificabili a un test pubblico d'intrusione (PIT). Questa procedura consente di testare la sicurezza di un sistema esponendolo a degli attacchi. L'OVE esige già nell'ambito del processo di certificazione lo svolgimento di un test d'intrusione da parte di un organismo accreditato. Con il test pubblico d'intrusione un sistema può essere testato da persone interessate provenienti da tutto il mondo.

Lo svolgimento di un PIT ha diversi obiettivi. Le segnalazioni dei partecipanti possono contribuire direttamente a migliorare la sicurezza. Inoltre, questo genere di test consente a esperti indipendenti di sviluppare competenze e conoscenze nell'ambito del voto elettronico. Questa procedura permette a lungo termine di prevenire la dipendenza da singole persone e organizzazioni e di contribuire al dibattito pubblico. Il test pubblico d'intrusione costituisce anche uno strumento di trasparenza volto a instaurare la fiducia nel sistema di voto. Per il buon esito di un PIT è necessaria la collaborazione attiva del maggior numero possibile di persone competenti. Il dibattito pubblico in atto nei media e a livello politico sul test pubblico d'intrusione è una dimostrazione della cultura dell'errore che regna nell'ambito del voto elettronico.

3 Sistema testato

In Svizzera negli ultimi anni sono stati utilizzati due diversi sistemi di voto elettronico con verificabilità individuale: il sistema della Posta svizzera (utilizzato ultimamente dai Cantoni di Friburgo, Neuchâtel, Turgovia e Basilea Città) e il sistema del Cantone di Ginevra (utilizzato ultimamente dai Cantoni di Berna, Lucerna, San Gallo[1], Argovia, Vaud e Ginevra).

Il 28 novembre 2018 le autorità ginevrine hanno reso noto che avrebbero cessato di esercitare il loro sistema al più tardi nel febbraio 2020. Hanno di conseguenza abbandonato l'ulteriore sviluppo del sistema ai fini della verificabilità completa, rendendo così inutile la realizzazione di un PIT.

L'unico sistema sottoposto al test pubblico d'intrusione è stato il sistema dotato di verificabilità completa della Posta svizzera (di seguito Posta). Non si trattava quindi del sistema impiegato attualmente, ma di quello che potrà essere utilizzato per scrutini a livello federale soltanto se adempirà tutti i requisiti del diritto federale e avrà ottenuto l'autorizzazione d'esercizio definitiva da parte delle autorità.

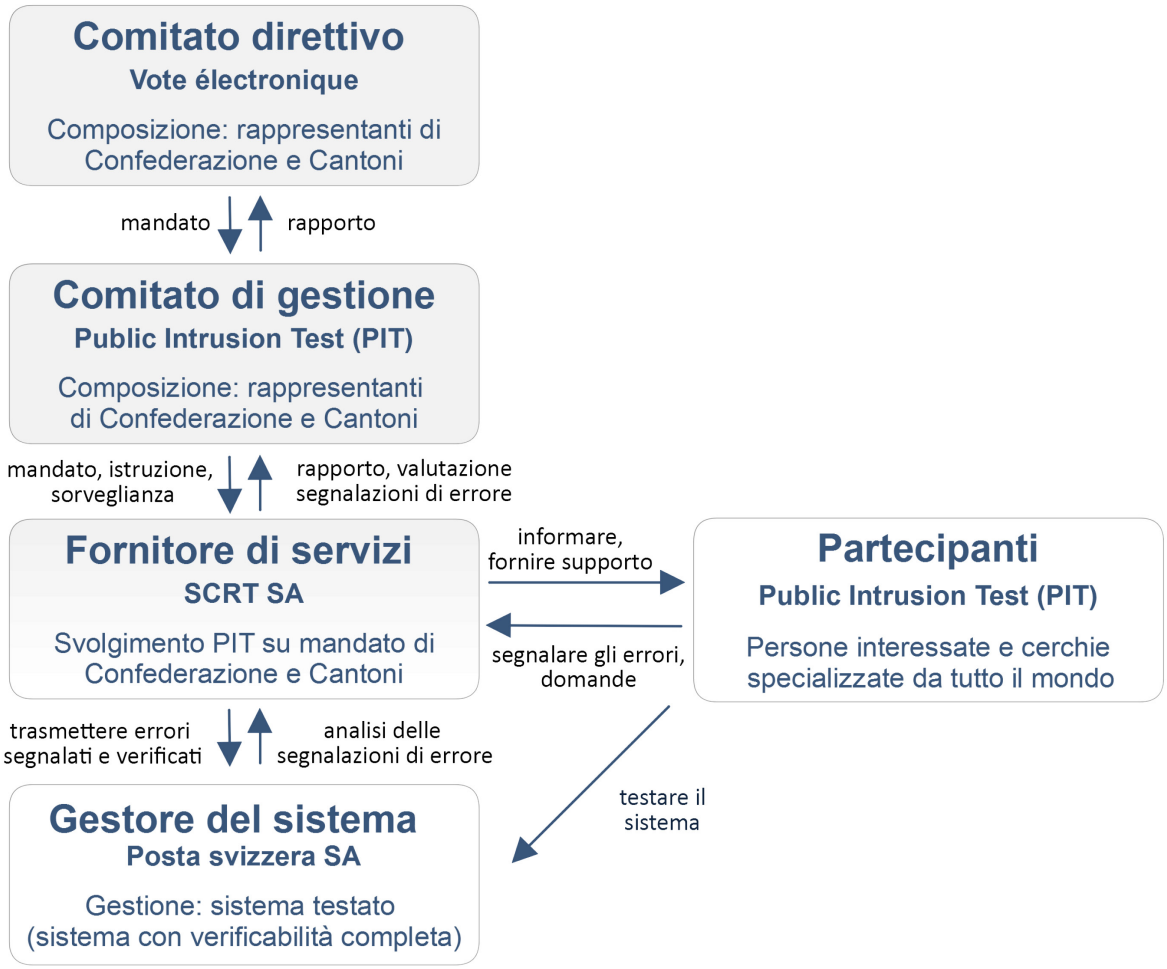
La struttura del sistema utilizzato per il PIT era la copia esatta di quella del futuro sistema produttivo. Per non limitare inutilmente l'accesso dei partecipanti è stata disattivata soltanto una configurazione tecnica di sicurezza che consente di bloccare gli indirizzi IP sospetti mediante l'applicazione Fail2Ban.

4 Disposizione sperimentale e organizzazione

La Confederazione e i Cantoni hanno concordato di effettuare un test pubblico d'intrusione congiunto e hanno stabilito requisiti comuni all'indirizzo del gestore del sistema[2]. Inoltre hanno partecipato al finanziamento del test nel quadro delle Linee guida della Strategia di e-Government Svizzera della Confederazione, dei Cantoni e dei Comuni con un importo di 250 000 franchi. Di questi, 150 000 franchi sono stati versati alla Posta e 100 000 franchi alla società SCRT quale fornitore di servizi della Confederazione e dei Cantoni.

[1] Il Cantone di San Gallo prevede di utilizzare in futuro il sistema della Posta svizzera.
[2] https://www.bk.admin.ch/dam/bk/it/dokumente/pore/Requisiti%20da%20Confederazione%20e%20Cantoni_test%20di%20intrusione%20pubblici.pdf.download.pdf/Requisiti%20da%20Confederazione%20e%20Cantoni_test%20di%20intrusione%20pubblici.pdf

Struttura organizzativa del PIT



La Posta ha messo a disposizione il sistema per il test pubblico d'intrusione dal 25 febbraio al 24 marzo 2019 e ne ha gestito il funzionamento. Ha previsto di ricompensare i partecipanti che le avrebbero sottoposto segnalazioni utili con importi dai 100 ai 50 000 franchi al massimo per segnalazione, per un totale di 150 000 franchi. I partecipanti potevano consultare i criteri di rimunerazione sulla piattaforma Internet messa a disposizione per il test pubblico d'intrusione (piattaforma PIT[3]).

Il comitato di gestione composto da rappresentanti della Confederazione e dei Cantoni ha seguito e sorvegliato il test pubblico d'intrusione su mandato del comitato direttivo Vote électronique. Durante il test il comitato di gestione aveva il compito di fornire tempestivamente alla Confederazione e ai Cantoni informazioni in merito al PIT. Doveva inoltre coordinare la comunicazione tra gli attori coinvolti ed elaborare i contenuti della comunicazione ufficiale destinata al pubblico.

Il PIT è stato svolto su mandato della Confederazione e dei Cantoni dalla società specializzata SCRT, la quale operava su istruzioni del comitato di gestione. La società SCRT era responsabile della comunicazione con i partecipanti, del loro reclutamento, della loro registrazione e del

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

supporto; aveva inoltre il compito di raccogliere le loro segnalazioni e di valutarle, il tutto attraverso la piattaforma PIT.

Al PIT hanno potuto partecipare persone provenienti da tutto il mondo. Al momento dell'iscrizione tramite la piattaforma PIT, le persone hanno preso atto del codice di condotta definito dalla Posta e hanno dovuto accettarlo (convenzione con la Posta). Questo codice definiva la portata del test e la procedura da seguire in caso di scoperta di lacune, inoltre garantiva l'impunità a condizione di rispettare il codice di condotta.

La disposizione sperimentale ha sollevato critiche nell'opinione pubblica.

- Conformemente ai requisiti posti dalla Confederazione e dai Cantoni la Posta ha limitato il test agli attacchi all'infrastruttura di voto elettronico della Posta stabilendo il codice di condotta in questo senso e vietando di fatto ogni attacco alle infrastrutture dei Cantoni, alle tipografie e ad altri servizi della Posta. Erano inoltre esclusi gli attacchi perpetrati allo scopo di rendere il sistema inaccessibile agli elettori (attacchi *denial of service*), come pure gli attacchi contro le piattaforme utente degli elettori. Lo stesso dicasi per gli attacchi volti a spingere gli attori mediante messaggi falsi a non seguire le procedure previste (*social engineering*). La Confederazione e i Cantoni hanno reagito alle critiche (cfr. n. 5).

- I requisiti posti da Confederazione e Cantoni per il PIT obbligavano la Posta a pubblicare prima del test il codice sorgente del sistema, conformemente all'articolo 7*a* seg. OVE, in modo da permettere ai partecipanti di prepararsi. La Posta ha imposto ai partecipanti condizioni d'utilizzazione particolari per accedere al codice sorgente. Le critiche hanno riguardato, da un lato, queste condizioni d'utilizzazione e, dall'altro, la preparazione del codice sorgente. Infatti, i critici sostenevano che tali condizioni prevedevano restrizioni inammissibili al diritto, garantito dall'articolo 7*b* capoverso 4 OVE, di esaminare, modificare, compilare ed eseguire il codice sorgente e di redigere studi in proposito e pubblicarli. È stata addotta anche una violazione dell'articolo 7*b* capoverso 1 OVE, in quanto la Posta avrebbe pubblicato un codice sorgente difficile da leggere e una documentazione insufficiente. La Cancelleria federale ha esortato la Posta a verificare e adeguare le condizioni quadro per la pubblicazione del codice sorgente[4].

5 Svolgimento

Il 7 febbraio 2019 la Cancelleria federale e i Cantoni di Friburgo, dei Grigioni, di Neuchâtel, di San Gallo e di Turgovia hanno pubblicato un comunicato stampa per annunciare lo svolgimento del test pubblico d'intrusione[5]. A partire da quel giorno gli interessati hanno potuto registrarsi in modo anonimo sulla piattaforma PIT. La società SCRT ha annunciato il test alle cerchie specializzate su Twitter e mediante altri canali. Il giorno stesso la Posta ha pubblicato il codice sorgente.

Visto il grande interesse dei media, la Cancelleria federale li ha invitati a una seduta informativa il 25 febbraio 2019 in occasione del lancio del test. Rappresentanti della Confederazione, dei

[4] https://www.bk.admin.ch/bk/it/home/documentazione/comunicati-stampa.msg-id-74307.html
[5] https://www.admin.ch/gov/it/pagina-iniziale/documentazione/comunicati-stampa.msg-id-73898.html

Cantoni e della Posta hanno distribuito schede informative e risposto alle domande[6]. Con queste schede, sulle quali erano illustrati gli obiettivi del PIT e il suo campo d'applicazione, la Confederazione e i Cantoni intendevano rispondere alle molteplici critiche espresse sulle modalità del test. Spiegazioni in merito sono state pubblicate anche sul sito Internet della Cancelliera federale nella rubrica Domande e risposte (Q&A)[7].

Durante il test, accedendo alla piattaforma PIT i partecipanti potevano procurarsi carte di legittimazione di voto, formulare domande e sottoporre le loro segnalazioni. La società SCRT vagliava le segnalazioni e rispondeva alle domande dei partecipanti relative alla sua valutazione. Nei casi in cui la segnalazione riguardava una possibile vulnerabilità, la società SCRT ne informava il comitato di gestione e la Posta. A intervalli regolari la società SCRT e la Posta sottoponevano al comitato di gestione la loro valutazione delle segnalazioni. Non c'è stato disaccordo nella valutazione di queste segnalazioni né tra la società SCRT e la Posta, né con il comitato di gestione.

6 Risultati

Fino al 24 marzo 2019, giorno in cui si è concluso il test, si erano registrati 3186 partecipanti provenienti da 137 Paesi[8]. Alla piattaforma PIT si sono però effettivamente connesse 1090 persone o gruppi di persone e 822 persone hanno richiesto carte di legittimazione per il voto nell'ambito del test. Per finire, 80 persone hanno inoltrato in totale 173 segnalazioni attraverso la piattaforma PIT. Per 16 di esse la società SCRT ha potuto constatare una violazione delle buone prassi in materia di sicurezza da parte della Posta[9]. Quest'ultima ha quindi versato ai partecipanti in questione ricompense per un totale di 2000 franchi. Nell'ambito del PIT non sono state constatate intrusioni nell'infrastruttura, manipolazioni dei voti o violazioni della segretezza del voto.

Tuttavia, i ricercatori che, pur non partecipando al PIT, hanno analizzato la documentazione relativa al sistema fornita nell'ambito della pubblicazione del codice sorgente hanno individuato tre importanti lacune del sistema[10]. Una delle lacune riguardava anche il sistema con verificabilità individuale già in uso. A seguito di questa scoperta la Posta ha deciso di non utilizzare il proprio sistema in occasione della votazione del 19 maggio 2019. La Cancelleria federale ha inoltre annunciato che farà il punto della situazione allo scopo di prevenire tempestivamente in futuro errori di questo tipo. Non sono stati constatati attacchi al sistema che abbiano sfruttato una di queste lacune. Poiché tali lacune non sono state scoperte mediante un attacco al sistema testato, queste segnalazioni non rientravano nel campo d'applicazione del PIT.

7 Conclusioni

La partecipazione attiva di un gran numero di persone competenti provenienti da tutto il mondo è da considerarsi un successo. Il loro lavoro ha permesso di eliminare lacune nella categoria delle buone prassi e dunque di migliorare ulteriormente la sicurezza dell'intero sistema. Queste persone potrebbero mettere a disposizione anche in futuro l'esperienza che hanno acquisito

[6] https://www.bk.admin.ch/bk/it/home/diritti-politici/e-voting/oeffentlicher_intrusionstest.html
[7] https://www.bk.admin.ch/bk/it/home/diritti-politici/e-voting/oeffentlicher_intrusionstest.html
[8] In base alla dichiarazione dei partecipanti
[9] Numero 4.3 dell'allegato e https://www.onlinevote-pit.ch/stats/
[10] https://www.bk.admin.ch/bk/it/home/documentazione/comunicati-stampa.msg-id-74508.html

nell'ambito del voto elettronico in Svizzera ad esempio occupandosi nuovamente di questioni di sicurezza oppure partecipando al dibattito pubblico.

È probabile che non tutti i partecipanti fossero degli esperti ma che tra loro vi fossero anche cittadini interessati. Il PIT ha dato loro la possibilità di familiarizzarsi con un sistema di voto elettronico che in futuro forse sarà utilizzato nel loro Cantone.

La Posta ha soddisfatto la maggior parte dei requisiti posti da Confederazione e Cantoni. Grazie all'impiego di considerevoli risorse e di personale qualificato ha organizzato un PIT dal quale sono stati tratti molti insegnamenti. Il test ha dimostrato la necessità di agire nel campo della preparazione e della pubblicazione del codice sorgente.

In futuro dovranno essere sfruttate le numerose critiche espresse riguardo al campo d'applicazione del PIT. Il punto della situazione che effettuerà la Cancelleria federale, in particolare per quanto riguarda gli aspetti legati alla sicurezza che non possono essere trattati nell'ambito di un PIT, dovrà concentrarsi sulle misure atte a promuovere e strutturare un dialogo costruttivo con esperti indipendenti. Questi ultimi dovranno essere maggiormente coinvolti anche in vista dello sviluppo del sistema e dei test di garanzia della qualità.

Le segnalazioni più utili sono state quelle riguardanti importanti lacune nel codice sorgente. Non sono stati segnalati tentativi riusciti di penetrare nel sistema. In futuro bisognerà valutare la possibilità di incentivare le persone a comunicare osservazioni utili sul codice sorgente e sulla documentazione. Le esperienze fatte aprono inoltre la via per istituire una cultura della qualità e dell'errore nell'ambito del voto elettronico.

È probabile che la mediatizzazione del PIT abbia anche contribuito ad aumentare il numero di persone che ha partecipato all'analisi del codice sorgente.

Il test svolto quest'anno è stato il primo nel suo genere per quanto riguarda il voto elettronico. L'esperienza acquisita sarà utile per eventuali nuovi test.

8 Documentazione complementare, rapporti, rimandi

Informazioni della Confederazione, dei Cantoni e della società SCRT (fornitore di servizi incaricato del test) sul test pubblico d'intrusione:

Documento / rapporto / link	Link
Sito Internet della Confederazione con informazioni relative al test pubblico d'intrusione 2019	https://www.bk.admin.ch/bk/it/home/diritti-politici/e-voting/oeffentlicher_intrusionstest.html
Requisiti posti da Confederazione e Cantoni per dei test di intrusione pubblici	https://www.bk.admin.ch/dam/bk/de/dokumente/pore/Anforderungen%20von%20Bund%20und%20Kantonen_%C3%96ffentliche%20Intrusionstests.pdf.download.pdf/Anforderun-

	gen%20von%20Bund%20und%20Kantonen_%C3%96ffentliche%20Intrusionstests.pdf
Scheda informativa della Cancelleria federale sul test pubblico d'intrusione	https://www.bk.admin.ch/dam/bk/it/dokumente/pore/PIT_Factsheet%20BK_IT.pdf.download.pdf/PIT_Factsheet%20BK_IT.pdf
Scheda informativa del Comitato di gestione di Confederazione e Cantoni sul test pubblico d'intrusione	https://www.bk.admin.ch/dam/bk/it/dokumente/pore/PIT_Factsheet%20Leitungsausschuss_IT.pdf.download.pdf/PIT_Factsheet%20Leitungsausschuss_IT.pdf
Piattaforma di registrazione al test pubblico d'intrusione per interessati e partecipanti	https://www.onlinevote-pit.ch/
Domande e risposte sul test pubblico d'intrusione (FAQ) per interessati e partecipanti	https://www.onlinevote-pit.ch/faq/
Risultati accettati e pubblicati sul test pubblico d'intrusione	https://www.onlinevote-pit.ch/stats/

Informazioni sul test pubblico d'intrusione fornite dal gestore del sistema, la Posta:

Documento / rapporto / link	**Link**
Rapporto tecnico finale dettagliato del gestore del sistema (Posta CH SA)	https://www.post.ch/-/media/post/evoting/dokumente/abschlussbericht-oeffentlicher-intrusionstest-post.pdf?la=en&vs=1
Terms, Conditions and Code of Conduct Public Intrusion Test (PIT)	https://www.onlinevote-pit.ch/conduct/
Sito Internet della Posta con informazioni sul test pubblico d'intrusione 2019	https://www.post.ch/it/soluzioni-commerciali/e-voting/pubblicazioni-e-codice-sorgente#test-publico-di-intrusione-2019
Articolo sul blog della Posta sul test pubblico d'intrusione	https://www.evoting-blog.ch/fr/pages/2019/test-de-piratage-public-du-systeme-de-vote-electronique-de-la-poste
Articolo sul blog della Posta sulla pubblicazione del codice sorgente	https://www.evoting-blog.ch/fr/pages/2019/la-poste-divulgue-le-code-source-de-son-systeme-de-vote-electronique

Link al portale informativo per gli elettori incluso il sistema di dimostrazione della Posta	https://www.evoting.ch/it
Accesso al codice sorgente dal sito Internet della Posta	https://www.post.ch/it/soluzioni-commerciali/e-voting/pubblicazioni-e-codice-sorgente#pubblicazionecodicesorgente

9 Allegato

Public Intrusion Test, Final Report, SCRT SA, 2019