Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundeskanzlei BK

Sektion Politische Rechte

Dialogo con gli esperti del mondo scientifico 2020

Sintesi del riassunto

1. Contesto e modo di procedere

Nel quadro del mandato del Consiglio federale del 26 giugno 2019 la Cancelleria federale (CaF), in collaborazione con diversi Cantoni, ha incontrato degli esperti del mondo scientifico. Il dialogo era finalizzato a servire come base per il sottogruppo di lavoro della Cancelleria e dei Cantoni per l'elaborazione di raccomandazioni. La CaF ha affrontato insieme a 23 esperti del mondo della ricerca e dell'industria questioni legate al sistema di voto elettronico[1]. Il dialogo era incentrato su questioni tecniche. La maggior parte degli esperti avevano conoscenze in un settore delle scienze esatte, mentre tre esperti disponevano di conoscenze nel campo delle scienze sociali.

In una prima fase il 14 febbraio 2020 la CaF ha sottoposto agli esperti un questionario con circa 60 domande[2]. Sulla base delle risposte ottenute, tra il 5 maggio e il 17 luglio 2020 la CaF ha condotto un dialogo online moderato in forma scritta. Per ciascun blocco di discussione il moderatore ha fornito un riassunto agli esperti partecipanti. Il riassunto dei blocchi di discussione e delle risposte al questionario sono inseriti nel documento concernente il riassunto del dialogo con gli esperti (« Summary of the Expert Dialog »).

2. Valutazione generale

Gli esperti vedono margine di manovra concernente la sicurezza, la trasparenza e l'esame indipendente. Allo stesso tempo sono dell'opinione che negli ultimi 15 anni sono stati raggiunti notevoli risultati. Raccomandano di analizzare le questioni legate alla sicurezza anche in merito agli altri canali di voto e di approfondire ulteriormente quelle relative alla creazione di un clima di fiducia.

Inoltre sottolineano l'importanza di includere sempre gli specialisti, in particolare quelli del mondo scientifico, nelle fasi di concezione, sviluppo ed esame dei sistemi di voto elettronico. È stato più volte suggerito di incaricare un comitato scientifico.

3. Allestimento di un sistema sicuro

3.1 Le autorità devono continuare a garantire la sicurezza

Gli esperti ritengono che valutare i rischi e se necessario prevedere delle misure debba rimanere compito delle autorità. Un comitato scientifico potrebbe assumere una funzione a questo proposito.

[1] Cfr. Lista degli esperti incaricati all'indirizzo www.bk.admin.ch > Diritti politici > Voto elettronico
[2] Cfr. Questionario all'indirizzo www.bk.admin.ch > Diritti politici > Voto elettronico

3.2 Standardizzazione della cifratura a blocchi

Le verifiche di sicurezza già richieste nell'ambito crittografico sono importanti ed è sempre necessario adattarle in base allo stato attuale delle conoscenze scientifiche. Inoltre gli esperti consigliano alle autorità di puntare sulla standardizzazione della cifratura a blocchi.

3.3 Garantire la qualità e la verificabilità del codice sorgente

È necessario assicurarsi che la documentazione di sistema e il codice sorgente siano accessibili in modo tale da permettere di verificare in modo efficiente la conformità con i requisiti legali. Gli esperti hanno menzionato diversi standard come possibile base per i processi di sviluppo. La semplicità deve essere il principio alla base dell'allestimento del sistema.

3.4 Maggiore diversità come presupposto fondamentale per l'affidabilità

La diversità tra le componenti che sono importanti per la verificabilità (le cosiddette componenti di controllo e verifica) costituisce per gli esperti un presupposto fondamentale per l'affidabilità del sistema: grazie alle altre componenti con un corretto funzionamento, gli errori nelle singole componenti non devono avere effetti negativi sulla verificabilità (guadagno esponenziale in termini di sicurezza). Tra gli elementi per la diversificazione è incluso anche il software. Gli esperti hanno individuato del potenziale di miglioramento anche nel generare parametri di sistema (ad es. il codice di controllo per la verificabilità individuale), cosa che deve essere realizzata separatamente e in maniera verificabile. Per stampare la carta di legittimazione hanno delineato delle soluzioni per un processo di stampa suddiviso. Agli esperti non sfuggono i costi e la maggiore complessità di funzionamento, quest'ultima dovuta all'introduzione di più diversità, ma ne sottolineano il valore aggiunto.

3.5 Il Public Bulletin Board per una maggiore verificabilità

Come approccio complementare per consolidare la verificabilità e renderla più indipendente si è discusso in merito all'impiego di una cosiddetta bacheca pubblica (public bulletin board) che è conosciuta dalla letteratura scientifica sul voto elettronico. Gli esperti considerano questa bacheca pubblica come uno strumento adatto per instaurare fiducia, ma temono che quest'ultima possa essere compromessa se nelle fasi di messa a punto o di attuazione sono commessi errori. Si rende necessario analizzare e tenere in considerazione anticipatamente le necessità dei votanti, in particolare in merito alla comunicazione, all'interfaccia grafica e alla facilità di impiego.

4. Esame su mandato ed esame pubblico

4.1 Esame su mandato

Alla certificazione dei sistemi non è attribuita un'importanza decisiva. Tuttavia una certificazione potrebbe rivelarsi utile nel quadro dell'esame relativo al funzionamento (certificazione secondo lo standard ISO27001). Al posto delle certificazioni, le autorità devono basarsi su esami indipendenti condotti da persone con le competenze necessarie. I crittografici devono essere coinvolti anche nell'esame del codice sorgente e del funzionamento. Al fine di evitare falle nel sistema è necessario che l'esame segua un concetto olistico. L'esame deve essere commissionato da parte della Confederazione o da un comitato indipendente.

4.2 Esame pubblico

Gli esperti conferiscono grande importanza all'esame pubblico. Per questo motivo sono favorevoli a sostituire il test pubblico d'intrusione condotto nel 2019 con un programma «bug bounty» (PBB) permanente con indennità finanziaria. Il PBB non dovrebbe limitarsi ad individuare gli attacchi all'infrastruttura del fornitore, ma anche scoprire gli errori nella documentazione del sistema e nel codice sorgente. Si

ritiene spetti alla Confederazione o ad un comitato indipendente decidere gli obiettivi, le modalità e l'alta vigilanza sul PBB.

Oltre al PBB, possono essere esaminate anche altre misure per la partecipazione dell'opinione pubblica, come ad esempio gli hackathon. Anche il coinvolgimento di persone senza conoscenze pregresse in ambito scientifico può dimostrarsi significativo, ad esempio nel quadro di un progetto di scienza partecipativa in merito alla facilità di impiego o alla comunicazione.

4.3 Trasparenza e pubblicazione del codice sorgente

La trasparenza costituisce una prerogativa per un esame pubblico efficace. Secondo gli esperti nella pubblicazione del codice sorgente è necessario rinunciare alla dichiarazione di riservatezza.

Oltre al codice sorgente devono essere pubblicati tutti i documenti necessari per capire il funzionamento e l'impiego del sistema. Inoltre deve essere possibile testare il sistema anche sul proprio computer. Nel caso in cui le modifiche al codice sorgente non siano direttamente pubblicate, gli esperti consigliano di effettuare una serie di esami per evitare errori inutili e la conseguente perdita di fiducia.

È necessario rendere noti i difetti e rispondere alle indicazioni emerse dal pubblico. Le relative disposizioni di dettaglio devono essere determinate dalla Confederazione. Inoltre la maggior parte degli esperti consiglia di pubblicare rapporti d'esame. Tuttavia, alcuni esperti fanno notare che rapporti d'esame di qualità carente possono portare alla perdita di fiducia.

Gli esperti sono dell'avviso che una pubblicazione non dotata di una licenza Open Source[3] possa permettere un esame pubblico mirato al raggiungimento degli obiettivi. Tuttavia ritengono la pubblicazione con una licenza Open Source più promettente.

4.4 Trattamento delle non conformità

Idealmente l'esame è svolto con un anticipo talmente largo da permettere di individuare le non conformità con un ampio margine in modo che possano essere corrette in tempo. Per il trattamento delle non conformità individuate in un secondo momento è necessario avviare dei processi decisionali.

L'impiego del sistema di voto elettronico non deve essere interrotto per ciascuna non conformità individuata. Gli esperti ritengono ragionevole accettare rischi di entità esigua. La difficoltà consiste nel valutare correttamente ciascuno di essi. Il confronto con quelli già accettati può essere d'aiuto. Un altro aspetto da considerare è che di fatto parte dei cittadini svizzeri residenti all'estero perde il proprio diritto di voto e che la rinuncia al sistema di voto elettronico comporta il ricorso al voto per corrispondenza, canale che risulta ugualmente rischioso. Maggiore è l'impatto di una non conformità sul sistema e meno è circoscritta ai relativi processi, più sarà necessario eliminarla in tempi brevi. Generalmente gli errori nel protocollo crittografico o in merito alla sua attuazione nel codice sorgente non devono essere accettati.

5. Valutazione del dialogo da parte degli esperti

Per gli esperti questo dialogo con il mondo scientifico costituisce una pietra miliare. Ritengono abbia portato a notevoli risultati e propongono di considerarlo una base per uno scambio continuo.

[3] Le licenze Open Source permettono di utilizzare il software per qualunque tipo di obiettivo.