Vote électronique
Requisiti posti da Confederazione e Cantoni per dei test di intrusione pubblici

Conformemente alla decisione del comitato direttivo Vote électronique del 29 ottobre 2018, i seguenti requisiti si applicano ai test di intrusione pubblici:

1. I fornitori dei sistemi consentono di effettuare un test di intrusione pubblico sul loro sistema.

2. Il test dura almeno quattro settimane (durata di uno scrutinio).

3. Partecipanti da tutto il mondo possono testare il sistema.

4. I partecipanti devono poter attaccare il sistema: devono essere consentiti tentativi di manipolare i voti, leggere i voti espressi, violare il segreto del voto e mettere fuori uso o aggirare le misure di sicurezza che proteggono i voti e i dati rilevanti per la sicurezza.

5. I partecipanti possono pubblicare le conoscenze acquisite durante i test.

6. La documentazione relativa ai sistemi e il codice sorgente devono essere pubblicati previamente su Internet (al riguardo si applicano le disposizioni di cui all'art. 7*a* seg. OVE). Come materiale di prova i partecipanti ricevono un numero sufficiente di legittimazioni al voto, che possono essere recapitate loro per via elettronica.

7. I riscontri dei partecipanti al test pervengono a un fornitore di servizi stabilito da Confederazione e Cantoni, che li valuta ed esprime il prima possibile il proprio parere in proposito. In questa fase è supportato dai fornitori dei sistemi.

8. I fornitori dei sistemi possono subordinare la partecipazione al test all'accettazione di un codice di comportamento. Il codice potrebbe comprendere i seguenti obblighi:

    a. evitare gli attacchi esclusi dal test;
    b. annunciare tempestivamente i difetti riscontrati;
    c. aspettare di pubblicare la descrizione dei difetti riscontrati finché il fornitore del sistema non abbia definito come comportarsi con il difetto.

9. Sono esclusi dal test:

   a. attacchi volti a impedire l'espressione del voto con attacchi DDoS (Distributed Denial of Service), ossia che provocano un'interruzione del servizio con origine da più fonti;
   b. attacchi volti a costringere gli attori, mediante notizie fasulle, a discostarsi dai processi previsti (ingegneria sociale);
   c. attacchi volti a manipolare i voti, sempre che tali attacchi possano essere riconosciuti con l'aiuto della verificabilità individuale;
   d. attacchi volti a leggere i voti diffondendo malware negli apparecchi utilizzati per votare;
   e. attacchi ai servizi dei fornitori del sistema non associati al voto elettronico;
   f. attacchi al sistema d'invio elettronico delle legittimazioni al voto.

10. Un consenso alla partecipazione al test espresso dai fornitori dei sistemi tutela i partecipanti dal perseguimento penale, sempre che gli attacchi non siano esclusi dal test.