Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Chancellerie fédérale ChF

Section des droits politiques

Vote électronique
Exigences fixées par la Confédération et des cantons pour les tests d'intrusion publics

Conformément à la décision du comité de pilotage Vote électronique du 29 octobre 2018, les exigences suivantes s'appliquent aux tests d'intrusion publics :

1. Les fournisseurs de système font en sorte que leur système puisse être soumis à un test d'intrusion public.

2. Ce test durera au moins 4 semaines (durée d'un scrutin).

3. Le système pourra être testé par des participants du monde entier.

4. Les participants devront pouvoir attaquer le système, et notamment tenter de manipuler des votes, d'identifier des votes émis, de briser le secret du vote, enfin de désactiver ou de déjouer les mesures de sécurité qui protègent les votes et les données de sécurité.

5. Les participants pourront publier les enseignements qu'ils auront tirés du test.

6. La documentation système et le code source devront préalablement être publiés en ligne (les art. 7, let. a à f, OVotE, étant applicables). Il sera remis aux participants un nombre suffisant de certificats de capacité civique en guise de matériel de test. Ces certificats pourront leur être remis sous forme électronique.

7. Les participants aux tests adressent leurs retours à un prestataire choisi par la Confédération et les cantons. Ce prestataire évalue les retours et les commente dans les meilleurs délais. Les fournisseurs de système lui apportent leur assistance.

8. Les fournisseurs de système peuvent prévoir que les participants doivent s'engager au préalable à respecter un code de conduite. Ce code pourrait comporter les obligations suivantes :

    a. s'abstenir de lancer des attaques qui sont exclues du test ;
    b. communiquer immédiatement toute faille de sécurité décelée ;
    c. s'abstenir d'exposer publiquement toute faille de sécurité qui aurait pu être décelée, jusqu'à ce que le fournisseur de système ait décidé de la procédure à suivre à cet égard.

9. Sont exclues du test les attaques suivantes :

   a. attaques par inondation destinées à empêcher le vote (attaques par déni de service) ;
   b. attaques consistant en l'envoi de fausses informations destinées à amener les acteurs à s'écarter des procédures prévues (ingénierie sociale) ;
   c. attaques qui visent à manipuler des voix, pour autant qu'il s'agisse d'attaques que la vérifiabilité individuelle permet de déceler ;
   d. attaques qui consistent à installer des logiciels malveillants sur les appareils de vote afin de pouvoir prendre connaissance des votes qui ont été émis ;
   e. attaques dirigées contre des prestations du fournisseur de système qui sont sans lien avec le vote électronique ;
   f. attaques dirigées contre le système d'envoi électronique des certificats de capacité civique.

10. Les participants sont protégés contre d'éventuelles poursuites judiciaires par l'accord que leur a donné le fournisseur de système, pour autant qu'ils ne lancent pas d'attaques exclues du test.