Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Chancellerie fédérale ChF

Section des droits politiques

Test public d'intrusion

Fiche d'information du comité de gestion de la Confédération et des cantons

25 février 2019

Exigences fixées par la Confédération et les cantons

La Confédération et les cantons ont décidé en 2017 que les systèmes de vote électronique proposant la vérifiabilité complète seraient soumis à un test public d'intrusion.

Ils mettent ainsi à l'épreuve l'élément infrastructurel qui assure la conservation des suffrages et auquel on pourra accéder pendant quatre semaines à partir d'Internet.

La Confédération et les cantons ont fixé des exigences communes qui s'appliquent à la réalisation du test public d'intrusion. Il s'agit notamment des exigences suivantes :

- Le fournisseur du système de vote électronique met ce dernier à disposition pendant quatre semaines pour la réalisation du test ;
- La documentation relative au système et le code source doivent être publiés pour que les participants au test y aient accès ;
- Les participants ont le droit de publier les informations que le test leur permettra de collecter, mais le fournisseur du système est autorisé à fixer un délai d'attente avant la publication ;
- En donnant son accord, le fournisseur du système protège les participants contre d'éventuelles poursuites judiciaires ;
- Cet accord englobe les attaques lancées contre le système de vote électronique, l'objectif étant de tenter de manipuler des suffrages, de lire des suffrages exprimés, de violer le secret du vote et de mettre hors-service ou de contourner les dispositifs de sécurité qui protègent aussi bien les suffrages que les données inhérentes à la sécurité.

Déroulement

Un comité de gestion composé de spécialistes de la Confédération et des cantons surveillera et encadrera la réalisation du test public d'intrusion.

La Confédération et les cantons ont confié la réalisation du test public d'intrusion à la société SCRT, qui est chargée des relations avec les participants. Cette société a pour tâches d'enregistrer les participants, de recueillir leurs réponses et d'évaluer ces dernières. Pour ce faire, elle a mis en place une plateforme Internet[1].

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

La société SCRT communiquera à La Poste Suisse les découvertes plausibles qui lui auront été signalées. À cet égard, la Poste a laissé entendre qu'elle verserait une indemnité financière à tout participant qui aura identifié une vulnérabilité (entre 100 et 50 000 francs suisses par communication, mais au maximum 150 000 francs au total). Les critères d'indemnisation et les montants des indemnités ont été définis au préalable ; les participants peuvent les consulter sur la plateforme Internet précitée.

Dès que toutes les évaluations seront terminées, le comité de gestion rédigera à l'attention du comité de pilotage Vote électronique un rapport qui fera la synthèse de toutes les informations recueillies à la faveur du test public d'intrusion. Le comité de pilotage publiera le rapport en question durant l'été 2019.

Sécurité et transparence

Un test public d'intrusion ne peut pas apporter la preuve que le vote électronique est sûr, mais il constitue une occasion d'identifier des vulnérabilités inconnues et de les élimer si besoin est. De surcroît, il permet à des milieux supplémentaires, qui regroupent de nombreux spécialistes, de participer au débat public. Ce dernier peut lui aussi contribuer, indirectement, à accroître la sécurité.

Le droit fédéral contient des exigences élevées qui s'appliquent à la sécurité des systèmes et à leur fonctionnement. Ces exigences portent sur toute la chaîne des processus qui interviennent dans le cadre de l'exécution des scrutins. Dans le présent test public d'intrusion, les exigences fixées par la Confédération et les cantons s'appliquent à dessein au système de vote électronique, dans le souci de garantir la sécurité des suffrages. Les attaques présentées ci-après, dirigées contre des éléments de la chaîne des processus, n'ont pas leur place dans le test public d'intrusion.

Raisons pour lesquelles il est interdit de lancer des attaques par déni de service distribué

Une attaque par déni de service distribué (distributed denial of service) est une attaque dirigée contre des systèmes informatiques dont le but est de perturber leur disponibilité. Le test public d'intrusion ne porte pas sur les attaques de ce type pour deux raisons. Premièrement, ces attaques contre des systèmes basés sur Internet sont connues et elles ne présentent aucune caractéristique propre au vote électronique. En cas d'attaque d'une certaine durée, les électeurs ont toujours la possibilité de voter par correspondance ou à l'urne. La prescription du Conseil fédéral en vertu de laquelle l'urne électronique doit être fermée déjà le samedi à 12 heures constitue également une mesure destinée à contrecarrer les attaques par déni de service distribué. Deuxièmement, ces attaques rendraient impossible l'accès au système qu'il faut tester, perturbant par là même le déroulement du test proprement dit. Il est possible de tester l'efficacité des dispositifs de défense contre les attaques par déni de service distribué d'une façon bien meilleure en simulant ces attaques en dehors du cadre d'un test public d'intrusion.

Raisons pour lesquelles il est interdit de lancer des attaques dirigées contre les plateformes utilisateur des électeurs

Les attaques dirigées contre des infrastructures externes – en particulier contre les plateformes utilisateur de particuliers – sont illicites et donc exclues du champ d'application du test

public d'intrusion. Les mécanismes de vérification à la disposition des électeurs, notamment la vérifiabilité individuelle, et les instructions des cantons qui leur sont destinées servent à protéger ces plateformes utilisateur. La possibilité de déjouer le système de vérifiabilité individuelle, c'est-à-dire les mécanismes de vérification à la disposition des électeurs, fait partie intégrante du test.

Il va de soi qu'un participant pourrait accepter qu'un autre participant lance une attaque contre sa plateforme utilisateur. En cas d'attaque réussie, les organisateurs du test public d'intrusion seraient toutefois dans l'impossibilité de déterminer s'il s'agit d'une vraie attaque ou d'une attaque simulée. La réalisation d'un test public d'intrusion ne constitue dès lors pas une mesure appropriée pour tester la sécurité des plateformes utilisateur. Il n'est cependant pas interdit de simuler des démonstrations d'attaques. De telles démonstrations pourraient même se révéler tout à fait utiles dans le contexte des discussions consacrées à la sécurité du vote électronique.

Raisons pour lesquelles il est interdit de lancer des attaques d'ingénierie sociale

L'ingénierie sociale est un terme générique désignant les attaques visant à influencer le comportement des différents acteurs au moyen de messages falsifiés. Une stratégie pourrait consister notamment à pousser les électeurs à ne pas suivre les instructions des autorités qui s'appliquent au vote électronique (par ex. les amener à ne pas contrôler les codes de vérification), ou encore à tenter d'influencer les employés du fournisseur du système de vote électronique ou ceux du canton responsable. Néanmoins, comme les acteurs savent qu'un test public d'instruction est organisé, on peut s'attendre à ce qu'ils se préparent à faire face à des attaques d'ingénierie sociale. Par conséquent, les conditions du test ne refléteraient plus la réalité. La réalisation d'un test public d'intrusion n'est dès lors pas une mesure appropriée pour tester la résistance d'un système à des attaques d'ingénierie sociale.

Un test public d'intrusion pour les infrastructures des cantons

Le traitement des données destinées à l'exécution du scrutin et l'impression du matériel de vote, mais aussi le déchiffrement et le dépouillement des suffrages, se font dans les cantons. Les deux étapes sont effectuées sur des infrastructures soumises à une surveillance physique qui sont séparées physiquement de tous les réseaux. Ces procédures ne cadrent pas avec le système de vote électronique, auquel on pourra accéder pendant quatre semaines à partir d'Internet. Il est plus efficace de tester les mesures de protection au sein même des infrastructures. Un test réalisé dans le cadre d'un test public d'intrusion (à distance) ne va guère déboucher sur des résultats concluants.

Membres du comité de gestion de la Confédération et des cantons

Oliver Spycher, chef de Projet suppléant Vote éléctronique, Chancellerie fédérale

Philipp Egger, responsable de l'informatique et des infrastructures, Chancellerie d'État du canton de Saint-Gall

Nicolas Fellay, responsable des droits politiques, Chancellerie d'État du canton de Fribourg

Bruno Ledergerber, responsable suppléant des élections et des votations, Office de la statistique du canton de Zurich