Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundeskanzlei BK

Sektion Politische Rechte

Questions et réponses

Vote électronique. Test public d'intrusion

1. En réalisant un test public d'intrusion, cherche-t-on à prouver que le système de vote électronique ne peut pas être hacké ?

Non. L'objectif consiste à identifier les vulnérabilités et, si besoin est, à les éliminer. Par ailleurs, la participation d'un maximum de spécialistes de la sécurité du vote électronique qui soient indépendants contribuerait à accroître la transparence. Le test public d'intrusion pourrait leur donner l'occasion de se pencher sur le système de vote électronique.

2. Quelles sont les attaques qu'il est interdit de lancer ?

Les attaques autorisées qui donneront lieu à une indemnisation financière seront les attaques réussies qui auront été lancées contre l'infrastructure de vote électronique de La Poste Suisse. Il sera interdit de mener des attaques contre les cantons, les imprimeries et les autres secteurs de la Poste qui fournissent des prestations, car ces entités ne participeront pas au test public d'intrusion. Seront aussi interdites les attaques par saturation (déni de service distribué) étant donné qu'elles n'apporteront pas de connaissances nouvelles à la faveur du test public d'intrusion, qu'elles peuvent faire l'objet de tests par d'autres moyens et qu'elles perturberaient de surcroît le déroulement du test. Les attaques lancées contre les plateformes utilisateur des électeurs ne donneront lieu à aucune indemnisation, pas plus – d'ailleurs – que les attaques visant à pousser les participants, par le biais de messages falsifiés, à s'écarter des procédures prévues (techniques d'ingénierie sociale). Les attaques réussies exploitent des comportements inappropriés qui ne peuvent pas être simulés de manière fidèle à la réalité dans le cadre d'un test public d'intrusion. Si quelqu'un réussit malgré tout à manipuler le système de vérifiabilité individuelle (l'électeur vote « oui », et c'est un « non » qui s'affiche) de telle sorte que les votants n'aient aucune possibilité d'identifier la manipulation, il recevra une indemnité financière.

3. C'est donc à des spécialistes indépendants qu'il incombe d'identifier toutes les vulnérabilités ?

Non. Le test public d'intrusion est une mesure de sécurité parmi de nombreuses autres. Chaque système informatique comporte des vulnérabilités ; ce sera le cas du système de vote électronique même après le test public d'intrusion. Ce qui est crucial, c'est qu'aucune vulnérabilité ne représente un risque plus ou moins élevé. Les vulnérabilités doivent être contrebalancées par des mesures de sécurité suffisamment efficaces. En proposant la vérifiabilité complète, le vote électronique dispose d'une mesure de sécurité globale et particulièrement efficace dont d'autres prestations sont dépourvues. Qui plus est, les systèmes sont vérifiés et certifiés à intervalles réguliers par un service accrédité.

4. L’établissement de la vérifiabilité complète nécessite aussi des ordinateurs. Ces ordinateurs ne présentent-ils donc aucune vulnérabilité ?

La vérifiabilité complète signifie pour l’essentiel qu’il ne suffit pas de manipuler un seul composant pour falsifier des suffrages sans que quelqu’un s’en aperçoive. Si un seul composant est manipulé, d’autres composants permettent d’identifier toute tentative de falsification.

5. Le test public d’intrusion ne va-t-il pas permettre à des assaillants d’apprendre aussi comment hacker le système de vote électronique ?

Quelqu’un pourrait signaler une vulnérabilité à un assaillant potentiel au lieu de le faire aux organisateurs du test public d’intrusion. Cela ne constitue pas un problème si les organisateurs sont aussi informés de la vulnérabilité et s’ils l’éliminent en cas de besoin. L’indemnité financière proposée par la Poste est une incitation à signaler les vulnérabilités (également) aux organisateurs. Par ailleurs, il est possible de tenter de découvrir des vulnérabilités par des moyens illégaux même en dehors du cadre du test public d’intrusion. En revanche, le test permettra aussi à des personnes bien intentionnées d’analyser le système en détail pour tenter d’y déceler des vulnérabilités.

6. La Confédération a-t-elle le droit de verser des indemnités financières aux hakkeurs qui auront lancé des attaques ?

En sa qualité de fournisseur du système de vote électronique, la Poste est chargée d’indemniser les personnes qui signaleront des failles de sécurité. Elle fixera le montant des indemnités et procédera à leur versement. La Confédération et les cantons alloueront un montant de 250 000 francs suisses pour la réalisation du test public d’intrusion, conformément au plan stratégique de la cyberadministration suisse.

7. Quel devra être le degré de gravité d’une vulnérabilité pour que la personne qui la signalera reçoive une indemnité financière ?

Ce n’est pas la gravité de la vulnérabilité qui est déterminante, mais le respect des règles par les participants au test d’intrusion. En principe, toutes les attaques qui pourraient faire émerger de nouvelles connaissances sur la sécurité des suffrages sont autorisées et même souhaitées. Les attaques destinées uniquement à mettre en évidence des vulnérabilités connues ne donneront pas droit à une indemnisation. Quelques attaques sont même interdites, bien qu’elles présentent indubitablement un lien avec un risque à prendre en considération. Pour garder ces risques sous contrôle, on dispose toutefois de moyens plus efficaces que le test public d’intrusion.

8. Pourquoi recourt-on déjà au vote électronique alors que le système n’a encore été soumis à aucun test d’intrusion ?

Le système que l’on va soumettre à un test public d’intrusion est le premier système proposant la vérifiabilité complète. Les systèmes utilisés à l’heure actuelle proposent la vérifiabilité individuelle, mais pas encore la vérifiabilité complète. Étant donné que la vérifiabilité complète permettra un recours au vote électronique à plus grande échelle, tout système proposant cette vérifiabilité devra répondre à des exigences de sécurité encore plus élevées, au nombre desquelles figurent notamment une certification et la publication du code source. Qui plus est, la Confédération et les cantons ont décidé que les systèmes de vote électronique proposant la vérifiabilité complète devraient passer un test public d’intrusion avant leur première utilisation.