Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Chancellerie fédérale ChF

Test public d'intrusion

La Poste Suisse a mis à disposition son futur système de vote électronique – le premier en Suisse à proposer la vérifiabilité complète – pour un test public d'intrusion qui a eu lieu **du 25 février au 24 mars 2019**. La vérifiabilité complète permet un recours au vote électronique à plus grande échelle. Elle garantit l'identification des dysfonctionnements systématiques à la suite d'erreurs logicielles, d'erreurs humaines ou de tentatives de manipulation.

Le droit fédéral exige que ce système soit certifié avant sa première utilisation et que le code source soit publié. De plus, 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. Un test d'intrusion sert à éprouver la sécurité d'un système en le soumettant à une attaque. Un test de ce type est déjà réalisé dans le cadre de la procédure de certification menée par un organe accrédité. En organisant de surcroît un test public d'intrusion, on donnera à un grand nombre de personnes dans le monde entier la possibilité de tester la sécurité du système.

Les personnes désireuses de participer au test pouvaient s'inscrire sur un site Internet, où elles trouvaient toutes les informations concernant les modalités du test.

Communiqué de la Chancellerie fédérale du 07 février 2019

Questions et réponses

La Confédération a-t-elle le droit de verser des indemnités financières aux hackeurs qui ont lancé des attaques ?

> La Poste Suisse était chargée d'indemniser les personnes qui signalaient des failles de sécurité dans le cadre du test public d'intrusion. Elle fixait le montant des indemnités et procédait à leur versement. La Confédération et les cantons ont alloué un montant de 250 000 francs suisses pour la réalisation du test public d'intrusion, conformément au plan stratégique de la cyberadministration suisse.

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.

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.

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.

Quel devait être le degré de gravité d'une vulnérabilité pour que la personne qui la signalait reçoive une indemnité financière ?

Ce n'était pas la gravité de la vulnérabilité qui était déterminante, mais le respect des règles par les participants au test d'intrusion. En principe, toutes les attaques qui pouvaient faire émerger de nouvelles connaissances sur la sécurité des suffrages étaient autorisées et même souhaitées. Les attaques destinées uniquement à mettre en évidence des vulnérabilités connues ne donnaient pas droit à une indemnisation. Quelques attaques sont même interdites, bien qu'elles présentaient 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.

Quelles étaient les attaques qu'il était interdit de lancer ?

Les attaques autorisées qui donnaient lieu à une indemnisation financière étaient les attaques réussies qui étaient lancées contre l'infrastructure de vote électronique de La Poste Suisse. Il était 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 participaient pas au test public d'intrusion. Étaient aussi interdites les attaques par saturation (déni de service distribué) étant donné qu'elles n'apportaient pas de connaissances nouvelles à la faveur du

test public d'intrusion, qu'elles pouvaient faire l'objet de tests par d'autres moyens et qu'elles perturbaient de surcroît le déroulement du test. Les attaques lancées contre les plateformes utilisateur des électeurs ne donnaient 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 (un « oui » est transmis, et c'est un « non » qui s'affiche) de telle sorte que les votants n'aient aucune possibilité d'identifier la manipulation, il recevait une indemnité financière.

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 était 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.

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 a soumis 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.

Exigences de la Confédération et des cantons

Afin de promouvoir la sécurité et la transparence, la Confédération et les cantons se sont mis d'accord en 2017 sur la conduite d'un projet pilote de test public d'intrusion. C'est à cet effet qu'ils ont émis les exigences suivantes à l'attention des fournisseurs de système:

Exigences fixées par la Confédération et des cantons pour les tests d'intrusion publics (PDF, 217 kB, 07.02.2019)

Fiche d'information de la Chf - PIT (PDF, 382 kB, 25.02.2019)

Fiche d'information du comité de gestion - PIT (PDF, 237 kB, 25.02.2019)

Rapports finals

Dans le cadre d'un mandat du comité de pilotage Vote électronique, le test public d'intrusion était accompagné et encadré d'un comité de gestion de la Confédération et des cantons. Le comité de gestion a établi un rapport final à l'attention du comité de pilotage Vote électronique.

Rapport final PIT (PDF, 850 kB, 02.09.2019)

Annexe rapport final PIT (PDF, 714 kB, 02.09.2019)

Liens

Communiqué de la Chancellerie fédérale du 07 février 2019

E-Voting blog de la Poste

Sécurité du vote électronique

Documents

Ordonnance de la ChF sur le vote électronique OVotE

Annexe OVotE (PDF, 600 kB, 29.06.2018)

https://www.bk.admin.ch/content/bk/fr/home/droits-politiques/groupe-experts-vote-electronique/oeffentlicher_intrusionstest.html