

Le Soleil, Samedi 19 novembre 2005, p. A30.

## **Un système excessivement préoccupant**

Gagnon, Clément

En tant que citoyen, je suis sensible à la fragilité de notre système démocratique et en tant que spécialiste en sécurité informatique, je suis au fait des faiblesses qu'un système informatique peut comporter. Ce que j'ai constaté avec le système de vote électronique lors de la dernière élection municipale dans la ville de Québec est excessivement préoccupant.

En sécurité informatique, il faut préserver trois choses : la disponibilité, l'intégrité et la confidentialité. Les élections de nature politique requièrent ces trois qualités à un niveau très élevé. Le système de vote et le traitement des votes se doivent d'être disponibles durant toute la durée du scrutin, le résultat du geste de voter doit être intègre (non altéré, ni perdu) et, évidemment, le vote du citoyen doit rester confidentiel.

La disponibilité du système de votation semble présenter de sérieuses lacunes. Selon le fournisseur du système de vote, les serveurs de compilation des votes sont tombés en panne à la suite d'une surcharge des données. Est-ce que la capacité de traitement du système a été évaluée selon les règles de l'art ? La charge maximale a-t-elle été estimée de façon minutieuse ? Des essais réalistes de charge ont-ils été réalisés ? Est-ce que la continuité de service et la relève informatique ont été prévues ?

À mon grand étonnement, j'ai constaté que les ordinateurs dans les bureaux de vote pour le suivi des listes électorales et l'activation des cartes à puce pour le vote étaient dotés de cartes de réseau sans fil. Il est très facile de paralyser ce type de réseau avec des jammers et par conséquent de perturber le vote. Certains des manuels du système de vote de PG Élections inc. sont accessibles dans leur site Web. La description des mécanismes de sécurité dans le système est très superficielle. Une rapide consultation de ces manuels et l'expérience de mon vote suscitent de sérieuses interrogations sur les mécanismes de conservation de l'intégrité et de la confidentialité des données de vote.

Le citoyen qui se présente au bureau de scrutin doit présenter une carte d'identité. Par la suite, une carte à puce est programmée et cette carte lui est remise. Cette carte est utilisée pour activer le terminal de vote et ensuite elle est retirée par un responsable pour permettre le vote du citoyen. Cette carte est non numérotée ou marquée ! Un pirate pourrait la substituer par une autre carte lors de son vote et cette carte pourrait provoquer un comportement anormal du terminal de vote. La cause serait difficile à retracer. De plus, quelles sont les informations qui sont inscrites sur cette carte à puce ? Est-il possible de faire un lien entre mon vote et mon identité avec cette carte dans le terminal de vote ?

Le système permet l'envoi des résultats du vote entre les bureaux de scrutin et le centre de traitement de vote du fournisseur par différents moyens, notamment par courriel. Est-ce que ce courriel est sécurisé ? De plus, le système de courriel d'Internet n'offre aucune garantie de livraison de courriel... Les autres moyens de transmission sont-ils sécurisés ?

Si un des éléments de ce système est relié à Internet, est-il protégé ? Comment ? Est-ce vérifié ? Le réseau sans fil dans les bureaux de scrutin est-il sécurisé, est-il protégé contre l'écoute ?

Selon les manuels disponibles dans le site de PG Élections, le système de compilation de vote offre le choix d'utiliser deux types de bases de données Microsoft. Une de ces bases de données (MS-Access) présente des lacunes majeures pour le support de la sécurité.

Signalons qu'une saine pratique de la sécurité informatique commande des audits et des vérifications externes de la conformité et de la sécurité d'un système. Est-ce que ceci a été fait ? Par qui ? Aucune mention sur ce point... Quels sont les lois et les règlements, les principes et les normes qui ont encadré la conception de l'ensemble de ce système ?

Pour terminer, l'échange et la conservation d'informations nominatives et confidentielles par un tiers exigent que ce tiers signe une entente de confidentialité. PG Élections a offert le service et le traitement du vote. Est-ce qu'il y a une entente de confidentialité qui été signée entre lui et la municipalité ? Qu'arrive-t-il avec les données après l'élection, combien de temps sont-elles conservées, comment sont-elles détruites ?

Je crois que ces questions exigent des réponses et que ces réponses soient publiques afin de rétablir la confiance.

En tant que citoyen, je n'ose imaginer les conséquences du système actuel dans le cas d'une élection ou d'un référendum avec un enjeu majeur comme la souveraineté du Québec.

*Conseiller en architecture de sécurité, consultant auprès d'organismes publics et privés, l'auteur est détenteur de la certification en sécurité informatique CISSP. Il a enseigné les technologies d'Internet dans plusieurs collèges de la région de Québec.*