Mémoire sur le vote par Internet déposé dans le cadre de la consultation publique menée par Élections Québec

Présenté par Brian Lack le 7 octobre 2019

Contexte

1. Simple Vote Inc. est un prestataire de services spécialisé dans le vote par internet basé à Montréal. L'entreprise travaille au service de plus de 2000 clients dans de nombreux secteurs tels que des universités, des associations, des syndicats, des partis politiques, des municipalités et des collectivités de Premières Nations. À tout moment, elle héberge plus d'une centaine d'élections ou référendums simultanés sur ses serveurs, et n'a à ce jour subit aucun incident de sécurité.

2. En ce qui concerne plus particulièrement cette consultation, Simple Vote a fourni sa solution de vote par Internet et par téléphone à 28 municipalités lors des élections municipales de 2018 en Ontario. De plus, le plébiscite de 2016 sur le renouveau démocratique à l'Île du Prince-Édouard s'est déroulé sur sa plateforme de vote; il s'agit de la première utilisation du vote par Internet dans un scrutin provincial en Amérique du Nord.

3. Le président et fondateur de Simple Vote Inc., Brian Lack, a développé le système de vote par Internet de Simple Vote en 2003. Il est titulaire d'un B.Sc. en informatique de l'Université McGill.

Usages appropriés du vote par Internet

4. À l'heure actuelle, le vote par Internet est utilisé au Canada pour les élections municipales et des conseils scolaires en Ontario et en Nouvelle-Écosse. Cette application de la technologie au domaine électoral rencontre de plus en plus de succès, et un nombre grandissant de municipalités se dotent d'outils de vote par Internet à chaque cycle électoral. D'autres provinces pourraient autoriser le vote par Internet aux niveaux municipal et scolaire dans un avenir proche.

5. L'approche adoptée dans ces juridictions consiste à permettre à chaque municipalité de choisir son mode de scrutin, qui peut consister en une combinaison de vote en personne (par papier), du vote par correspondance, du vote par Internet, ou encore du vote par téléphone. La technologie de vote par téléphone offre une avenue aux électeurs qui ne peuvent ou ne veulent pas utiliser Internet ou se rendre à une borne dédiée au vote par Internet.

6. La plupart des municipalités desservies par Simple Vote ont décidé d'utiliser notre mode de vote par Internet et par téléphone et d'éviter totalement le papier. Les électeurs qui votent par téléphone ou par Internet s'identifient à l'aide d'un NIP unique et aléatoire, qui est envoyé par la poste à chaque électeur dans une enveloppe sécurisée. Ils doivent également fournir leur date de naissance. Lors du vote, chaque électeur reçoit un code de reçu aléatoire enregistré avec le bulletin de vote de manière

anonyme. À la fin d'une élection, la municipalité reçoit une liste de tous les bulletins enregistrés avec les codes de reçu associés. Cette liste peut être partagée avec le public afin de permettre aux électeurs de vérifier que leur vote a été correctement enregistré et comptabilisé.

7. Si le vote par Internet est utilisé en complément du vote par papier, tel que suggéré dans la présente consultation publique, Élections Québec pourrait considérer la possibilité d'utiliser clicSÉQUR pour l'identification des électeurs, ce qui éliminerait les coûts d'impression et d'envoi de lettres contenant des NIP pour tous les électeurs.

8. Le Québec aurait avantage à autoriser le vote par Internet à ce niveau de gouvernement, car il s'agit d'offrir aux électeurs une méthode de vote pratique et peu coûteuse pour les municipalités et les commissions scolaires. Les enjeux dans ces types d'élections sont raisonnablement faibles, et les fournisseurs desservant ce marché bénéficient d'une sécurité suffisamment élevée pour protéger leurs systèmes de vote. Ainsi, le risque de réussite d'une cyberattaque est très faible dans ce contexte.

Une menace élevée

9. Cependant, plus les enjeux d'un scrutin sont élevés, plus le danger d'une attaque augmente. Les pouvoirs économiques et politiques des gouvernements provinciaux sont bien plus importants que ceux des gouvernements municipaux. Les budgets de campagne pour les élections provinciales se chiffrent en millions de dollars[1], ce qui est largement supérieur à ceux des campagnes municipales. Avec des enjeux beaucoup plus importants, les candidats, les partis, les partisans, les groupes d'intérêts et même le crime organisé mobilisent beaucoup plus de ressources pour influer sur les résultats et pourraient être tentés d'attaquer le système de vote.

10. Au niveau provincial, les acteurs étrangers peuvent également s'intéresser au résultat. Le crime organisé international, des groupes de pirates informatiques tels que Anonymous, la Russie, la Chine et même l'Agence de sécurité nationale des États-Unis (NSA) possèdent tous de puissantes capacités en matière de cyberguerre. Les systèmes d'inscription en ligne des électeurs de l'Arizona et de l'Illinois ont récemment été piratés, apparemment par des acteurs étrangers. Cet exemple nous montre que la menace est bien réelle[2].

11. Lorsqu'une quantité importante de ressources technologiques est déployée, un acteur peut tirer parti des vulnérabilités mentionnées ci-dessous. Ces vulnérabilités sont attribuables aux limitations de la technologie Web en général, et ne sont pas le propre du vote par Internet.

[1] https://www.electionsquebec.qc.ca/documents/pdf/DGE-6355-18-07.pdf
[2] http://www.lefigaro.fr/elections-americaines/2016/08/30/01040-20160830ARTFIG00143-le-fbi-detecte-des-vols-de-donnees-d-electeurs-en-arizona-et-dans-l-illinois.php

Logiciels malveillants ciblés

12. Un logiciel malveillant (« malware » en anglais) est un programme destiné à nuire à un système informatique en infectant un appareil à l'insu et contre la volonté de son propriétaire. Certains logiciels malveillants, tels que le ver informatique Stuxnet qui a détruit les centrifugeuses iraniennes d'enrichissement d'uranium[3], sont conçus pour viser une cible et un objectif en particulier. Les logiciels malveillants peuvent être conçus spécifiquement pour détourner un vote particulier sur un système de vote Internet particulier, et peuvent être aussi simples dans leur conception qu'une extension de navigateur Chrome, par exemple. Lorsque l'électeur se connecte au système de vote par Internet à partir d'un ordinateur infecté et clique sur le candidat A, le logiciel malveillant soumet silencieusement un vote pour le candidat B. L'électeur ne saura jamais la différence (à moins qu'il ne vérifie son reçu de vote, après le fait accompli).

13. Pour qu'un logiciel malveillant ait une incidence sur l'issue du vote, il doit être installé sur un nombre suffisant d'appareils utilisés par les électeurs. Le logiciel peut se propager de lui-même, ou un pirate seul peut prendre le contrôle de tous les ordinateurs grâce à un « botnet », un réseau composé de nombreux ordinateurs personnels infectés par un certain virus informatique. On sait que des « botnets » importants comprenant des centaines de milliers d'ordinateurs existent réellement[4]. Souvent, ils sont utilisés à des fins de pollupostage, d'attaques par déni de service (DoS) et d'activités frauduleuses. L'exploitant d'un « botnet » pourrait facilement installer le programme malveillant de son choix sur les ordinateurs infectés.

14. Quelle que soit le niveau de sécurité offert par le système de vote par Internet choisi, les ordinateurs à partir desquels sont enregistrés les votes ne peuvent pas être sécurisés. Ce type d'attaque est très difficile à détecter et encore plus à arrêter.

Vulnérabilités aux attaques « zero-day »

15. Les principaux fournisseurs de vote par Internet adhèrent aux meilleures pratiques en matière de sécurité sur Internet et sont de manière générale protégés contre les techniques de piratage connues. Le véritable danger vient des techniques de piratage inconnues : les vulnérabilités parfois appelées « zero-day ». Les cybercriminels et les services du renseignement découvrent, recueillent et exploitent les vulnérabilités « zero-day » qui pourraient être utilisées pour accéder à des serveurs ou à décrypter des données chiffrées[5]. À titre d'exemple, le ver informatique Stuxnet mentionné précédemment a tiré parti de plusieurs vulnérabilités « zero day » pour attaquer efficacement sa cible.

16. Il est extrêmement difficile pour tout service en ligne de se protéger contre des menaces inconnues, et aucun serveur Internet ne peut être sécurisé à 100%. Lorsqu'une vulnérabilité de type « zero day »

[3] https://fr.wikipedia.org/wiki/Stuxnet
[4] https://fr.wikipedia.org/wiki/Botnet
[5] https://fr.wikipedia.org/wiki/Vulnérabilité_zero-day

est exploitée, elle devient connue de la communauté de la sécurité et devient par le fait moins puissant. Les acteurs malveillants ne gaspilleront donc pas un piratage de type « zero day » sur une cible de faible valeur. Cependant, une élection ou référendum provinciale peut être considérée comme une cible de grande valeur pour des raisons économiques ou politiques.

Conclusion

17. Bien que Simple Vote soit l'un des principaux fournisseurs canadiens de vote par Internet, l'entreprise **recommande de ne pas utiliser le vote par Internet dans les élections et les référendums provinciaux**. Le degré élevé de menaces lors d'une élection provinciale nécessite un niveau de sécurité que le vote par Internet ne peut offrir. Les enjeux sont donc trop grands.

18. Cependant, il convient de noter que **le vote par Internet est une excellente solution pour les plébiscites, les élections des conseils scolaires, les élections municipales et les élections des Premières Nations**, puisque les mesures de sécurité existantes sont extrêmement élevées par rapport au niveau de la menace. Si Élections Québec devait conclure que le vote par Internet n'est pas suffisamment sûr pour les élections provinciales, il serait important de nuancer cette recommandation et de ne pas caractériser la technologie comme défectueuse ou inutilisable en général.