Robert Donovan
Edmonton
Alberta

Le 20 septembre 2016

Mes 30 ans de développeur de systèmes informatiques m'ont appris deux choses très simples : d'abord, si vous ne pouvez pas évaluer un événement, c'est qu'il ne s'est pas produit et ensuite, si le pire peut, en théorie, se produire, il se produira. Par conséquent, quand je développe des systèmes informatiques, j'y laisse diverses traces, fichiers et pistes de vérification qui me permettront ainsi qu'à mes clients de découvrir ce qui s'est exactement passé lors du passage des données dans le système.

Pourtant, ces systèmes ne sont généralement pas parfaits. L'idéal, c'est que mon procédé d'évaluation cerne et fasse ressortir toutes les erreurs, ce qui me permet de traiter le problème de manière proactive et rapidement. Des erreurs se produisent quand même, et ce sont habituellement mes clients ou leurs clients qui détectent le problème. Pour vous expliquer, je vais utiliser l'exemple d'une organisation dont le fonctionnement est presque entièrement fondé sur les données, la banque.

Les clients d'une banque vérifient généralement l'intégrité des données de leur institution financière en consultant simplement le solde de leur compte. La plupart des clients de banques ont une relativement bonne idée de ce que leur solde devrait être. C'est quand ils s'aperçoivent qu'il n'est pas ce qu'il devrait être, selon eux, qu'ils commencent à passer en revue leurs relevés d'opération afin de remonter à la source du problème.

Il s'agit souvent d'une transaction oubliée ou d'un autre problème simple. Parfois, cependant, il peut s'agir d'une erreur du système ou même d'une fraude. Une intervention simple de la banque à la demande du client contribue souvent à résoudre le problème rapidement.

Cet exemple de la banque m'amène à soulever deux points essentiels en lien directement avec la faisabilité du vote en ligne. En premier lieu, étant donné la nature même du système de vote en ligne, quel qu'il soit, les votes sont absorbés par le système. Un électeur ne peut pas « vérifier » plus tard l'état final de son vote. Il disparaît simplement dans un bassin, un peu comme une banque monstrueuse qui n'a pas maintenu séparés les comptes de ses clients, mais a simplement laissé tous ces derniers déposer leur argent dans un seul compte géant. Et comme si cela ne suffisait pas, il n'y a pas de relevés de transactions, seulement un solde sous la forme d'un immense méli-mélo informe.

En second lieu, les banques sont des institutions incroyablement sûres. Les banques utilisent d'énormes ressources pour prévenir, contrer et limiter les attaques d'une extrême sophistication qu'une telle richesse attire. Mais, très souvent, les banques sont vaincues. De l'argent est volé, s'égare ou bien est récupéré en quantité énorme par différents acteurs malveillants. On peut dire la même chose de toutes les grandes entreprises du numérique dans le monde. Facebook, Google, eBay, PayPal, Microsoft et ainsi de suite sont régulièrement piratées, et souvent victimes de graves infractions. Ces entreprises comptent parmi leurs employés certaines des personnes les plus intelligentes de la planète.

Encore une fois, doublement pertinent est le fait que c'est souvent l'utilisateur final qui décèle ces attaques parce qu'il peut vérifier lui-même ses données : un compte bancaire où de l'argent

manque, un compte de courrier électronique Google qui reçoit d'étranges messages, un compte PayPal qui indique de mystérieux achats.

En tant que développeur de systèmes informatiques comptant des décennies d'expérience, je peux dire que le vote en ligne présente deux grandes faiblesses : d'abord, c'est un système qui, comme les banques, peut être piraté. Seuls un escroc ou un fou diraient l'inverse. Si les banques et les entreprises comme Google ne peuvent pas empêcher le piratage, c'est simple, personne ne le peut. La première conclusion inévitable est que le système de vote en ligne sera piraté, un point, c'est tout. La seconde est que les utilisateurs victimes de piratage ne pourront pas faire une vérification du système en s'assurant par la suite que leur vote a bel et bien été pris en compte. De par sa nature même, un piratage réussi est une attaque qui est parvenue à contourner les éléments de sécurité du système. Par conséquent, on ne peut se fier aux systèmes de détection du système, quels qu'ils soient, pour représenter les millions de parties intéressées. Un système de vote en ligne vraiment compromis répondra sans hésiter à quiconque vérifie son exactitude et son intégrité que tout va bien.

Le très petit nombre de personnes qui peuvent être les acteurs malfaisants ou être potentiellement conduites à devenir des acteurs malfaisants constitue un second problème pour le vote en ligne. N'importe lequel des programmeurs en chef peut trafiquer le système afin que le résultat soit déterminé par le pirate ou un petit groupe de conspirateurs. Il y a un concours destiné aux programmeurs appelé *The Underhanded C Contest* dans le cadre duquel les programmeurs doivent créer un programme qui effectue apparemment une certaine opération, alors qu'en fait il en effectue une autre néfaste. Dans le cadre d'un récent concours, il s'agissait de tromper des inspecteurs relativement à l'état des matières nucléaires. De tels programmes passeraient haut la main la plupart des contrôles de codes visant à repérer les codes malveillants. Plus important encore, un petit groupe de conspirateurs pourrait facilement « vérifier » les codes des uns des autres, évitant ainsi complètement tous les dispositifs de protection. Cet argument peut s'appliquer à tous les acteurs malfaisants de l'extérieur : ils n'ont en effet pas besoin d'être nombreux. Ce genre d'actions est souvent réalisé par de petits groupes de personnes.

J'aime comparer une telle situation au processus électoral traditionnel faisant appel à des bulletins en papier : comment peut-on perpétrer une fraude dans un tel contexte au milieu de milliers d'urnes électorales, de dizaines de milliers de membres du personnel électoral, de scrutateurs et de candidats aux élections? Il y a tout simplement trop de témoins et le complot devrait être bien trop vaste pour pouvoir vraiment faire basculer des élections. Il faudrait que les comploteurs réussissent leur tour de passe-passe dans des milliers de bureaux de vote, qu'ils parviennent tous à faire l'échange des bulletins de vote sans qu'aucun d'entre eux ne se fasse attraper et qu'aucun d'entre eux ne vende la mèche.

Par ailleurs, pour rendre tout cela encore plus intéressant, je peux vous donner un exemple tout à fait d'actualité de piratage hors norme. La National Security Agency (NSA) a récemment été piratée (non pas par Edward Snowden, mais par un pirate de l'extérieur) et de nombreux outils de piratage lui ont été dérobés. Les voleurs sont en train d'essayer de les vendre pour une somme faramineuse à la Dr Terreur, ce qui prouve que même la renommée NSA mettait partiellement en scène une aura de sécurité. D'après ce que j'ai vu, tous les systèmes de vote électronique sont aussi protégés que des secrets industriels. Tous les systèmes de vote électronique sans exception qui ont été étudiés par d'authentiques chercheurs indépendants dans le domaine de la sécurité ont été complètement discrédités parce que considérés comme inutiles, peu sûrs et susceptibles d'être les victimes d'un grand nombre d'attaques mineures. C'est de la foutaise que prétendre qu'un système est sûr. Prouver qu'il l'est à un groupe d'experts contradicteurs est mieux, mais comme les experts dans toutes les banques vous le diront, ce n'est toujours pas suffisant. En soumettant

un système à l'analyse des experts, on prouvera probablement que c'est de la foutaise. Mais, si des experts prétendent qu'un tel système est sûr, cela signifie simplement qu'ils sont biaisés ou que ce ne sont pas des experts.

Mais le pire dans tout cela, c'est que le genre de personne qui sera (et non « pourrait » être) élue en raison de ce genre de fraudes est exactement le genre de personnes que nous ne voulons pas voir titulaires d'une charge publique. On peut en arriver à ce résultat électoral catastrophique de trois manières : dans le premier cas, l'individu concerné s'engage dans la voie de la fraude en raison de sa soif du pouvoir qui s'appuie, au mieux, sur le principe rationalisé selon lequel la fin justifie les moyens; dans le deuxième cas, un parrain du parti ou en coulisse appuie le candidat fraudeur et la fraude, et dans le troisième cas, quelque État-Nation ou société commanditaire empêche un candidat qui lui est hostile d'être élu ou soutient un candidat qui lui est favorable. Dans ces deux derniers cas, le politicien vainqueur n'est peut-être, sans en avoir conscience, qu'un pion.

Il y a, sans aucun doute, différentes personnes dans les catégories nommées ci-dessus qui, ne connaissant aucun problème en matière de ressources, n'auront aucun scrupule à commettre une telle fraude électorale.

On ne peut tout simplement pas l'empêcher et de par la nature même du système de vote électronique, on ne peut pas la déceler si elle est perpétrée correctement. Il peut y avoir des « statistiques » aberrantes, mais qui ne sont pas suffisantes pour permettre à un juge d'annuler un résultat.

Gardez en tête l'idée que le vote en ligne est une erreur irrémédiable. Une fois les élections gagnées frauduleusement, les élus conserveront certainement le système qui leur aura permis de gagner. À ce stade-là, les seuls qui peuvent, au mieux, se saisir du pouvoir sont encore plus sournois que ceux d'avant.

Pourquoi risquerions-nous l'une des plus importantes institutions qui tient à cœur à l'Occident? Pour faire l'économie de quelques bulletins de vote? Pour attirer quelques électeurs apathiques qui ne voudraient pas se donner la peine de se rendre à un bureau de vote? En tant qu'expert informatique, je ne considère pas cela comme un risque, mais comme une certitude. Google sera piraté, Apple sera piraté, Facebook sera piraté, la CIBC sera piratée et n'importe quel système de vote en ligne élaboré par des gens bien moins talentueux sera certainement piraté. Les autres actes de piratage me coûteront quelques dollars ou mon compte de courriel. Cet acte de piratage là me coûtera ma liberté.

Sincères salutations,

Robert Donovan