Scénarios de manipulation du vote électronique en 4 phases

Phase 1 : Infection simple des systèmes utilisateurs non protégés

Si une puissance cybercriminelle décide de s'attaquer au système suisse de vote électronique, elle enverra à un moment donné des e-mails promettant un prix attrayant ou une lecture intéressante, de sorte que de nombreuses personnes cliqueront dessus. Vous obtenez une infection, qui est capable de recharger les programmes à un moment ultérieur. Celles-ci affecteront la procédure de saisie du vote électronique pour déjouer l'utilisateur. Ou bien ils infectent les sites Web fréquemment visités par les Suisses avec un cheval de Troie qui produit le même effet. L'attaque peut se produire de différentes manières dans le tuner utilisé :

#	Attaque d'un objet dans un téléphone mobile/PC	Avantages pour l'attaquant	Inconvénients pour l'attaquant
1	OS Kernel / root-kit	• L'utilisateur ne remarque rien s'il ne comprend pas la procédure de vérification. • Une mise à jour ne supprime pas l'infection. C'est permanent.	• N'est pas facile à programmer • Une analyse médico-légale détaillée peut déterminer l'infection
2	OS /Middleware(PC/Handy)	• L'utilisateur ne remarque rien s'il ne comprend pas la procédure de vérification.	• Une mise à jour pourrait supprimer l'infection • Une analyse médico-légale pourrait détecter l'infection.
3	Nouveau App	• Est pratique pour la programmation • L'utilisateur le trouve attrayant, • p. ex. s'occupe automatiquement des examens fastidieux en photographiant les codes de vote	• L'utilisateur doit accepter l'application • Des applications destructrices pourraient être dénoncées après un certain temps et dissuader de nombreux utilisateurs
4	Browser (intervention statique)	• L'utilisateur ne remarque rien s'il ne comprend pas la procédure de vérification.	• Une mise à jour pourrait supprimer l'infection • L'utilisateur peut utiliser un autre navigateur • Il faudrait infecter différents navigateurs • Une analyse médico-légale peut détecter l'infection
5	Browser (intervention dynamique)	• Est relativement simple et flexible • L'utilisateur ne remarque rien s'il ne comprend pas la procédure de vérification. • Une preuve est difficilement possible par la suite	• Une mise à jour pourrait supprimer l'infection • L'utilisateur peut utiliser un autre navigateur • Peut-être même un redémarrage du navigateur effacera l'infection. • L'infection doit être répétée encore et encore.

(Les attaques contre les systèmes d'évaluation ne sont pas traitées ici.)

Phase 2 : Vérification individuelle

La Chancellerie fédérale compte sur le fait que certains électeurs remarqueraient des manipulations des procédures et les signaleraient. Ils devraient si bien connaître la procédure avec les codes de cryptage qu'ils ne sont pas dépendants d'un guidage approprié de l'utilisateur. En cas d'attaque réussie d'un PC ou d'un téléphone portable non protégé, il n'est plus possible de compter sur un bon guidage de l'utilisateur. Des tests ont maintenant montré que 9 utilisateurs sur 10 suivent aveuglément les instructions (même manipulées) des ordinateurs. Il ne reste presque plus personne qui étudie les instructions et s'occupe des règlements. Supposons que ce 10e électeur remarque maintenant qu'il n'a pas vu de "code de finalisation", par exemple, et qu'il ne sait donc pas quoi faire maintenant. Il a les options suivantes, laquelle choisira-t-il ?

Que se passe-t-il s'il y a une attaque contre le vote électronique ?

	Option	Pour?	Contre?	Que se passe-t-il alors ?
1	Il appelle la hotline.	L'avis officiel des autorités est probablement le meilleur.	Tu sais déjà ce qu'ils diront là-bas: Allez à l'urne ou à la poste.	Il va à l'urne ou à la poste quand il le peut, rien d'autre. S'il rate le vote, il sera affecté par la manipulation.
2	Il va directement à la poste ou à l'urne, s'il n'est pas indisposé.	Le problème est tellement résolu pour lui	Le sens civique du devoir	Rien, parce que l'affaire n'est pas rendue publique.
3	Il se renseigne auprès d'amis ou autour de lui sur	Peut-être qu'ils ont aussi le problème.	S'ils ne l'ont pas, il ne comprendra pas grand-chose.	Rien, car la probabilité que le phénomène en ait plusieurs dans le petit cercle est assez faible. Si c'est le cas, il choisira une autre option.
4	Il le signale officiellement et demande une enquête.	Le sens civique du devoir	La (1) gêne et (2) le temps qu'il se met lui-même dans le pétrin, (3) l'absence de perspectives que son intervention implique, (4) la charge de la preuve que les autorités peuvent exiger, y compris la soumission de son instrument de vote électronique pour une durée indéterminée et éventuellement la (5) réprimande parce que lui-même a pu faire une erreur. En outre, il dispose (6) de données à caractère personnel, y compris les bulletins de vote, qu'il ne souhaite pas divulguer. Enfin, (7) les coûts des procédures et les frais peuvent également être prévus. Un argument particulier contre cela est que (8) il n'y a pas de processus définis et (9) aucune expérience de ce type de la part des autorités.	La probabilité que cette procédure soit choisie et mène au succès est extrêmement faible. Personne ne veut être le premier, et c'est seulement quand il y a un mouvement médiatique comme #Meetoo que tout le monde est soudainement là. Les autorités sont immédiatement à la limite de leur capacité, même si elles ne veulent faire le suivi que des échantillons individuels. Il faut donc faire preuve de scepticisme à cet égard. En outre, il n'est pas garanti qu'un résultat positif dans ces échantillons soit dû à une manipulation (ce qui pourrait également être un prétexte dans des cas individuels) et même un résultat négatif ne donne pas lieu à un soulagement absolu de la suspicion de manipulation. Même dans le meilleur des cas, le résultat acheté à un prix élevé n'est donc rien de plus qu'un durcissement d'une suspicion de manipulation sans en déterminer l'ampleur et la signification.
5	Il le rapporte aux journaux et/ou aux médias sociaux.	Le sens civique du devoir, beaucoup moins de colère qu'avec (4), L'utilisation du pouvoir des médias, qui ne doit pas être sous-estimée.	Ces rapports n'ont aucun caractère probatoire.	Les autorités sont obligées de prendre position. Cependant, ils n'ont ni preuve ni contre-preuve de la suspicion de manipulation dans le résultat final. Selon le volume du scandale médiatique, ils décideront d'un choix de répétition, ou en minimiseront l'ampleur et ne feront rien.

On peut supposer avec confiance qu'environ 80 à 90 % de ces personnes choisissent les options 1 à 3, environ 10 à 20 % choisissent l'option 5 et peut-être moins de 1 % choisissent la voie difficile 4. si ces hypothèses augmentent, au plus tous les 1000e des victimes manipulées choisiront la voie qui pourrait mener à une enquête judiciaire en faveur de tous les électeurs. Donc, si la différence de votes n'est que d'environ 1000 votes, il faudrait - pour être sûr - prendre un seul déclarant tellement au sérieux que l'on déclare l'élection invalide.

27.09.2018, René Droz

Phase 3 : L'enquête médico-légale dans l'affaire individuelle

Le CF a promis une enquête dans un tel cas. La seule perspective d'un résultat significatif nécessite une équipe d'experts médico-légaux en TI bien équipés qui:

1. sont convoqué et déployé immédiatement afin qu'un résultat significatif puisse encore être obtenu dans le délai de 6 jours contre le décompte des voix,
2. ont accès aux ordinateurs d'évaluation à la centrale et dans le canton concerné afin de vérifier et de comparer les résultats,
3. peuvent examiner l'équipement utilisé pour le vote, ce qui implique en même temps la levée du secret du vote dans ce cas,
4. ont reçu l'autorisation de l'utilisateur de le faire (protection des données, perte de disponibilité pour une courte période de temps)
5. savent synchroniser et comparer les résultats des autres équipes médico-légales dans les délais impartis,
6. savent également documenter ces enquêtes et comparaisons et les mettre à la disposition des autorités dans un langage compréhensible.

Une enquête médico-légale comprend une analyse de l'ensemble de la mémoire de données pour différents modèles. Comme ces stockages de données sont immenses aujourd'hui et que les schémas suspects deviennent de plus en plus nombreux, ce processus prend souvent à lui seul plusieurs jours.

Les seules prémisses juridiques, qui doivent être respectées ici, rendent une telle action irréaliste. Outre le fait que ces équipes médico-légales n'existent qu'avec les corps de police (et une avec l'armée) et qu'elles sont déjà plus que suffisamment occupées (problème de ressources), les conditions de temps ne sont pas non plus réunies pour réussir la découverte rapidement nécessaire des manipulations de vote.

Phase 4: L'évaluation politique de l'incident

L'évaluation politique se terminera probablement par une question publique sur l'existence de "doutes légitimes" quant au décompte des voix. Il est déjà clair aujourd'hui qu'il y aura des doutes. La question de savoir s'ils sont "justifiés" est cependant une question de point de vue et d'arguments résilients alors disponibles. Comme on l'a vu plus haut, cette dernière sera presque certainement très mince. Les points de vue s'adapteront alors à l'accord des médias. La décision de répéter une élection/un vote sera en quelque sorte démocratiquement légitimé(e), mais aura une composante émotionnelle et irrationnelle distincte. Je suppose que le vote électronique ne devra plus autorisé pour la répétition. Ceci, à son tour, affectera l'accord non seulement parmi les vainqueurs du vote, mais aussi parmi les partisans du vote électronique et l'administration/le gouvernement lui-même contre la répétition. Il y aurait trop de crainte d'avoir à renoncer complètement au vote électronique en cas d'un autre incident. Face à la perte menace tous ceux qui, malgré de sérieuses réserves de la part des experts, ont fait avancer le projet de prestige pendant des années et ont défié toute résistance.

Conclusions:

Les manipulations de l'évaluation du vote électronique n'auraient d'effet, en raison de son caractère vérifiable, que si elles sont si massives qu'une formidable atmosphère médiatique ne laisse d'autre choix qu'un vote/révote sans vote électronique. De plus petites manipulations avec peu de détecteurs et seulement quelques 10000 votes ont d'excellentes chances de succès dans ces circonstances.