Szenarien einer E-Voting Manipulation in 4 Phasen

1. Phase: Einfache Infektion der ungeschützten Benutzersysteme

Wenn sich eine cyberkriminelle Macht entschliesst, das Schweizerische E-Voting System anzugreifen, so wird sie zu irgendeinem Zeitpunkt Mails verschicken welche einen attraktiven Gewinn oder eine interessante Lektüre versprechen, so dass viele Leute das anklicken werden. Sie holen sich damit eine Infektion, welche in der Lage ist, zu einem späteren Zeitpunkt Programme nachzuladen. Diese werden die E-Voting Eingabe-Prozedur beeinflussen, um den Benutzer zu überlisten. Oder sie infizieren von Schweizern häufig besuchte Webseiten, mit einem Trojaner, der denselben Effekt erzeugt.

Der Angriff kann auf vielfältige Weise im benutzten Abstimmgerät geschehen:

#	**Angriffsobjekt im Handy/PC**	**Vorteile für den Angreifer**	**Nachteile für den Angreifer**
1	OS Kern / root-kit	• Benutzer merkt nichts, wenn er die Verifikations-Prozedur nicht versteht • Ein Update löscht die Infektion nicht. Sie ist permanent.	• Ist nicht einfach zu programmieren • Eine ausführliche forensische Analyse kann die Infektion feststellen
2	OS /Middleware(PC/Handy)	• Benutzer merkt nichts, wenn er die Verifikations-Prozedur nicht versteht	• Ein Update könnte die Infektion löschen • Eine forensische Analyse kann die Infektion evtl. feststellen
3	Neue App	• Ist bequem zum Programmieren • Benutzer findet es attraktiv, erledigt z.B. die mühsamen Prüfungen automatisch durch Fotographie der Stimmunterlagen	• Benutzer muss die App akzeptieren • Destruktive Apps könnten nach einiger Zeit denunziert werden und viele der Benutzer abhalten
4	Browser (statischer Eingriff)	• Benutzer merkt nichts, wenn er die Verifikations-Prozedur nicht versteht	• Ein Update könnte die Infektion löschen • Der User könnte einen anderen Browser nehmen • Man müsste verschiedene Browser infizieren • Eine forensische Analyse kann die Infektion evtl. feststellen
5	Browser (dynamischer Eingriff)	• Ist relativ einfach und flexibel • Benutzer merkt nichts, wenn er die Verifikations-Prozedur nicht versteht • Ein Nachweis ist nachträglich kaum möglich	• Ein Update könnte die Infektion löschen • Der User könnte einen anderen Browser nehmen • Vielleicht löscht schon ein Neustart des Browsers die Infektion • Die Infektion muss immer wieder neu erfolgen

(Auf die Angriffe gegen die Auswertungssysteme wird hier nicht eingegangen.)

2. Phase : Die individuelle Verifizierung

Die Bundeskanzlei zählt darauf, dass einige Stimmbürger Ablaufmanipulationen merken und das melden würden. Sie müssten die Ablaufprozedur mit den Krypto-Codes so gut kennen, dass sie nicht auf eine ordentliche Benutzerführung angewiesen sind. Mit einer ordentlichen Benutzerführung kann bei einem erfolgreichen Angriff auf den ungeschützten PC oder das Handy nämlich nicht mehr gerechnet werden. Testversuche haben nun aber gezeigt, dass 9 von 10 Benutzern den (auch manipulierten) Anweisungen von Computern blind folgen. Kaum noch gibt es Leute, die Anleitungen studieren und sich mit Reglementen herumschlagen.

Nehmen wir mal an, diesem 10. Stimmbürger fällt nun auf, dass er z.B. einen „Finalisierungscode“ nicht gesehen hat und er deshalb unsicher ist, was nun zu tun ist. Folgende Handlungs-Optionen hat er, welche wird er wohl wählen?

Was passiert, wenn ein Angriff auf E-Voting stattfindet?

	Option	Was spricht dafür?	Was spricht dagegen?	Was passiert dann?
1	Er ruft die Hotline an	Der offizielle Ratschlag der Behörden ist wohl der beste	Man weiss schon, was die dort sagen werden: Geh an die Urne oder zur Post.	Er geht an die Urne oder zur Post, wenn er kann, sonst nichts. Evtl. verpasst er die Abstimmung, dann ist er von der Manipulation betroffen.
2	Er geht direkt zur Post oder an die Urne, falls er nicht verhindert ist	Das Problem ist für ihn so gelöst	Das staatsbürgerliche Pflichtbewusstsein	Nichts, denn der Fall wird nicht bekannt.
3	Er frägt im Umfeld oder bei Freunden nach	Vielleicht haben die das Problem auch	Wenn sie es nicht haben, wird er auf wenig Verständnis treffen	Nichts, denn die Wahrscheinlichkeit, dass das Phänomen mehrere im kleinen Kreis haben, ist eher klein. Falls doch wird er noch eine andere Option wählen.
4	Er meldet es amtlich und verlangt eine Untersuchung	Das staatsbürgerliche Pflichtbewusstsein	Der (1) Ärger und (2) Zeitaufwand den er sich einhandelt, die (3) mangelnden Aussichten, die seine Intervention beinhalten, (4) die Beweispflicht, die die Behörden möglicherweise verlangen, beinhaltend Abgabe seines elektronischen Wahlinstruments für eine unbestimmte Zeit und evtl. den (5) Tadel, weil er womöglich doch einen Fehler selber gemacht hat. Zudem hat er ja (6) persönliche Daten darauf, inkl. Abstimmungseingaben, die er nicht preisgeben will. Schliesslich sind ja möglicherweise auch noch (7) Kosten für Verfahren und Gebühren zu erwarten. Dagegen spricht insbesondere auch, dass es (8) keine definierten Prozesse und (9) keinerlei Erfahrungen dieser Art auf Seiten der Behörden gibt damit.	Die Wahrscheinlichkeit ist äusserst klein, dass dieses Vorgehen gewählt wird und zum Erfolg führt. Niemand will wohl der erste sein, und erst wenn es eine mediale Bewegung gibt wie #Meetoo ist plötzlich jedermann dabei. Die Behörden sind sofort an der Grenze ihrer Kapazitäten, auch wenn sie nur einzelnen Stichproben nachgehen wollen. Man muss dort darum mit einer skeptischen Haltung rechnen. Bei diesen Stichproben ist zudem ein positiver Befund nicht garantiert auf eine Manipulation zurückzuführen (könnte im Einzelfall auch eine Vortäuschung sein) und auch ein negativer Befund ergibt keinen Anlass für eine absolute Entlastung des Manipulationsverdachtes. Das teuer erkaufte Resultat ist also auch im besten Falle eine nichts weiter als eine Erhärtung eines Manipulationsverdachtes ohne Bestimmung von Ausmass und Bedeutung.
5	Er meldet es Zeitungen und/oder sozialen Medien	Das staatsbürgerliche Pflichtbewusstsein, viel weniger Ärger als bei (4), Nutzung der Medienmacht, die nicht zu unterschätzen ist.	Solche Meldungen haben keinen Beweischarakter.	Die Behörden sind gezwungen Stellung zu nehmen. Sie haben aber weder Beweise noch Gegenbeweise für den Manipulationsverdacht im Endergebnis. Sie werden je nach Lautstärke des Medienskandales auf eine Wahl Wiederholung entscheiden oder aber das Ausmass kleinreden und nichts tun.

Man kann getrost davon ausgehen, dass ca. 80-90% dieser Leute die Optionen 1-3 wählen, ca. 10-20% die Option 5 und vielleicht weniger als 1% nimmt den schwierigen Weg 4. Treffen diese Annahmen zu, so wird höchstens jedes 1000. der manipulierten Opfer den Weg wählen, der zu einer forensischen Untersuchung – zu Gunsten des gesamten Stimmvolkes - führen könnte. Beträgt die Stimmendifferenz also nur ca. 1000 Stimmen, so müsste man – um auf der sicheren Seite zu sein - auch einen einzigen Melder so ernst nehmen, dass man die Wahl für ungültig erklärt.

25.09.2018, René Droz

3. Phase : Die forensische Untersuchung im Einzelfall

Die BK hat in so einem Fall eine Untersuchung in Aussicht gestellt. Die einzige Aussicht auf ein aussagekräftiges Resultat bedingt ein Team von gut ausgerüsteten IT-Forensikern, die

1. sofort aufgeboten und eingesetzt werden können, damit innerhalb der 6-tägigen Beschwerdefrist gegen die Stimmauszählung noch ein aussagekräftiges Resultat möglich ist,
2. Zugang haben zu den Auswertungscomputern in der Zentrale und dem betroffenen Kanton, um die Resultate zu verifizieren und zu vergleichen,
3. das benutzte Gerät zur Stimmabgabe untersuchen können, was auch gleichzeitig die Aufhebung des Abstimmgeheimnis in diesem Fall bedeutet,
4. die Erlaubnis vom Benutzer dafür bekommen haben (Datenschutz, Verfügbarkeitsverlust für einen kurzen Zeitraum)
5. die Resultate von anderen Forensiker Teams innerhalb der Beschwerdefrist auch noch synchronisieren und abgleichen können,
6. die diese Untersuchungen und Abgleiche auch noch dokumentieren und den Behörden in einer verständlichen Sprache zur Verfügung stellen können.

Eine forensische Untersuchung beinhaltet eine Analyse des gesamten Datenspeichers auf diverse Muster. Da diese Speicher heute riesig sind und der verdächtigen Muster immer mehr werden, dauert alleine dieser Vorgang oft mehrere Tage.

Allein die juristischen Prämissen, die hier eingehalten werden müssten, lassen so eine Aktion als unrealistisch erscheinen. Abgesehen davon, dass es solche Forensiker Teams nur bei den Polizei-Korps (und 1 bei der Armee) gibt und diese bereits mehr als genügend ausgelastet sind (Ressourcenproblem), sind auch die Zeitbedingungen nicht dazu geeignet, erfolgreich zu sein bei der rasch notwendigen Entdeckung von Abstimmungsmanipulationen.

4. Phase: Die politische Bewertung des Vorfalles

Die politische Bewertung wird voraussichtlich so enden, dass öffentlich die Frage gestellt wird, ob es „berechtigte Zweifel“ an der Stimmenauszählung gibt. Bereits heute ist klar, dass es Zweifel geben wird. Ob sie aber „berechtigt“ sind, ist eine Frage des Standpunktes und der dannzumal verfügbaren belastbaren Argumenten. Wie oben gezeigt wird, werden letztere mit ziemlicher Sicherheit sehr dünn ausfallen. Die Standpunkte werden sich der dann medialen Stimmung anpassen. Der Entscheid, eine Wahl/Abstimmung zu wiederholen wird zwar irgendwie demokratisch legitimiert sein, hat aber eine deutliche emotionale und irrationale Komponente. Ich gehe davon aus, dass für die Wiederholung E-Voting nicht mehr zugelassen sein dürfte. Das wird wiederum die Stimmung nicht nur bei den Abstimmungssiegern, sondern auch bei E-Voting Befürwortern und der Verwaltung/Regierung selbst gegen die Wiederholung beeinflussen. Zu gross wäre die Angst, bei einem erneuten, nächsten Vorfall auf E-Voting ganz verzichten zu müssen. Gesichtsverluste drohen allen, die jahrelang trotz seriöser Bedenken von Fachleuten das Prestigeprojekt durchgeboxt und allen Widerständen getrotzt haben.

5. Schlussfolgerung

Manipulationen an der E-Voting –Auswertung hätten – wegen der Verifizierbarkeit- nur dann keine Auswirkungen, wenn sie so massiv sind, dass eine gewaltige mediale Stimmung keine andere Wahl lässt als eine Wahl/Abstimmungs-Wiederholung ohne E-Voting. Kleinere Manipulationen mit wenigen Meldern und nur einigen 10000 Stimmen haben aber unter diesen Umständen ausgezeichnete Erfolgsaussichten.