Die bewiesene Unsicherheit

Nun ist es also bewiesen. Im E-Voting System der Post, hatte, es trotz gegenteiliger Beteuerungen solche kritischen Fehler, dass die vielgepriesene „Verifizierbarkeit“ gar nicht funktioniert hätte, wenn ein Insider entsprechende Manipulationen vorgenommen hätte. Die Post nimmt ihr System temporär aus dem Markt.

Kein IT –Spezialist wird sich ob so einer Feststellung wundern, denn er weiss es aus eigener Erfahrung, dass es nur eine Frage des Aufwandes ist, bis man einen solchen Fehler entdeckt. Und es wird nie der letzte sein.

Was der Politik und uns Stimmbürgern aber am meisten zu denken geben muss, ist, dass die Post ja offenbar ihr System gar nicht genügend gut versteht, als dass sie selbst in der Lage gewesen wäre, solche kritischen Fehler selbst zu finden. Man hat sich also darauf verlassen, dass irgendjemand in der Welt mit mehr Kompetenz sich die Zeit nimmt, um Fehler zu finden. Es ist bezeichnend, dass alle die bezahlten Firmen und auch die auf einen Gewinn spekulierenden Hackergruppen gerade nicht in der Lage waren, diese 2 kritischen Fehler zu finden, währenddessen eine Idealistin und 2 ihrer Kollegen ohne Bezahlung auf einem andern Kontinent der Welt dies zustande brachte.

Was ist das für eine Sicherheits-Strategie, die darauf abzielt, per so einem Zufall eine Schwachstelle zu finden, um nachher grossartig verkünden zu können, dass diese jetzt behoben sei? Es ist keine Sicherheits-Strategie, sondern eine reine Medienstrategie. Es geht darum, der Bevölkerung den guten Willen zu demonstrieren. Aber reicht das wirklich aus für den Anspruch eines E-Voting-Systems an Sicherheit?

Der nun überprüfte Quellcode ist mit Sicherheit nicht der, der am Ende implementiert wird, denn dieser hat ja Fehler. Wenn man weiss, dass solche Quellcodes nicht nur bei dieser Runde, sondern ganz generell permanent einem laufenden Neuerungsprozess unterliegen, so ist eine einmalige statische Feststellung, ob Fehler gefunden wurden und wenn ja welche, nur wenig wert, wenn es gilt, Prognosen für einen künftigen sicheren Betrieb zu stellen. Ausserdem bedarf es einer kleinen Manipulation, um den Anschein zu geben, der geprüfte Code sei auch der implementierte, währenddessen der manipulierte Compiler zusätzlichen Code installiert.

Unsere Gruppe der E-Voting Gegner haben diesem Test mit höchsten Bedenken entgegengesehen. Zunächst war nicht klar, ob die spanische Firma überhaupt den gesamten Code (der Applikation) veröffentlicht. Nun war zumindest ein Teil dabei, der Fehler zeitigte. Aber die ganze Quellcode Frage, die ja, wie erwähnt, nie sauber beurteilt werden kann, stellt nur eine von ca. 10 konzeptionellen Bereichen[1] mit Schwachstellen und Manipulationspotential dar. Die Nichtzulassung von ca. 8 dieser Bereiche für den Hacker-Test sehen wir nach wie vor als eine fragwürdige Art, Vertrauen schaffen zu wollen.

Was aber zeigt dieser Intrusion Test dennoch? Er zeigt die Leichtfertigkeit und Überheblichkeit, mit der unsere Behörden Zertifikate ausstellen lassen und die Unverfrorenheit, mit der man dem Stimmbürger Sicherheit und Professionalität vorgaukelt.

[1] S. https://noevoting.ch/file/system

29.03.2019/dr