SocietyByte
Wissenschaftsmagazin des BFH-Zentrums Digital Society
https://www.societybyte.swiss

Schwachstellen im E-Voting-System der Post entdeckt

Autor : Eric Dubuis

Datum : 25. März 2019

Der in den letzten Wochen durchgeführte, öffentliche Intrusionstest des E-Voting-Systems der Schweizerischen Post hat in Fachkreisen und der Öffentlichkeit ein grosses Interesse geweckt, insbesondere als die Entdeckung schwerwiegender Schwachstellen bekannt wurde. Diese Vorfälle zeigen, wie wichtig Zusammenarbeit und Transparenz bei der Einführung von E-Voting sind.

Mitte Februar hat die Schweizerische Post die Spezifikation und den Quelltext ihres E-Voting-Systems veröffentlicht. Dies geschah im Vorfeld des Intrusionstest, der grosse mediale Aufmerksamkeit auf sich zog. Die nun bekannt gewordenen schwerwiegenden Schwachstellen sind aber bereits in der Spezifikation des Systems ersichtlich; der Quelltext und der Intrusionstest spielen dabei eine untergeordnete Rolle. Die Spezifikation ist der eigentliche Bauplan des Systems. Sie beschreibt, aus welchen Komponenten das System aufgebaut ist und wie diese zusammenarbeiten. Wenn dieser Bauplan einen Fehler aufweist, so handelt es sich um ein grundlegendes Problem.

Universelle Verifizierbarkeit fehlt

Die entdeckten Schwachstellen sind deshalb schwerwiegend, weil sie zeigen, dass die sogenannte universelle Verifizierbarkeit des Postsystems nicht gegeben ist. Die universelle Verifizierbarkeit ist die zentrale Sicherheitsanforderung, welche die Bundeskanzlei an alle neuen E-Voting-Systeme stellt, welche für politische Wahlen in der Schweiz eingesetzt werden sollen. Sie erlaubt unabhängigen Stellen, nach einer Wahl oder Abstimmung das Resultat anhand der angefallenen Daten zu überprüfen. Diese Verifizierung kann mit dem Nachzählen der Stimmen bei papierbasierten Wahlsystemen verglichen werden. Damit wird verhindert, dass irgendjemand das Resultat einer Wahl oder Abstimmung unbemerkt manipulieren kann.

Die Bundeskanzlei hat Ende 2013 eine erste Verordnung über den Einsatz von E-Voting Systemen für politische Wahlen in der Schweiz erlassen, in welcher zum ersten Mal die universelle Verifizierbarkeit gefordert wurde. Zudem wurde ein Prozess für die Zertifizierung von E-Voting-Systemen definiert, mit welcher die universelle Verifizierbarkeit nachgewiesen werden muss. Dieser Zertifizierungsprozess entsprach dem damaligen Wissensstand.

Ende 2018 konnte die Wissenschaft aber aufzeigen, dass der Nachweis der Verifizierbarkeit eines E-Voting-Systems allein nicht genügt, sondern dass die einzelnen Verifizierungsschritte konkret als Teil der Spezifikation definiert werden müssen. Denn erst so können unabhängige Expertengruppen die Verifizierung auf ihre Vollständigkeit überprüfen. Ungeachtet dieser neuen Erkenntnisse wurde der Zertifizierungsprozess des Postsystems auf den aktuellen gesetzlichen Grundlagen durchgeführt. So war es überhaupt möglich, dass ein nicht universell verifizierbares System den Zertifizierungsprozess erfolgreich durchlaufen konnte.

Fazit der BFH-Forschenden

All dies zeigt, wie wichtig bei der Entwicklung von E-Voting-Systemen und der Definition der zugehörigen Prozesse eine enge Zusammenarbeit der politischen Institutionen, der Hersteller und der Wissenschaft ist. Zudem muss im Sinne grösstmöglicher Transparenz auch die Öffentlichkeit frühzeitig miteinbezogen werden. Dazu gehört eine offene Diskussion der Vertrauensannahmen, auf welchen die universelle Verifizierbarkeit basiert. Die Nicht-Manipulierbarkeit einer Wahl oder Abstimmung ist beispielsweise nur garantiert, wenn bestimmte Komponenten des Systems von unabhängigen Organisationen betrieben werden, damit keine die alleinige Kontrolle über das System erhält. Eine andere wichtige Annahme ist die Vertrauenswürdigkeit der Druckerei, welche die Wahlunterlagen druckt und damit zu Beginn einer Wahl oder Abstimmung eine kritische Rolle spielt. Aus Sicht der E-Voting-Gruppe der BFH ist es wichtig, dass alle Annahmen hinterfragt werden, um bewusst entscheiden zu können, ob das Restrisiko, das sie bergen, für unsere Demokratie tragbar ist.