End-to-End verifizierbare Wahlverfahren in Hinblick auf den Grundsatz der Öffentlichkeit der Wahl

Katharina Hupf, Anastasia Meletiadou

Universität Koblenz-Landau
Universitätsstraße 1
56070 Koblenz
hupfi@uni-koblenz.de
nancy@uni-koblenz.de

Laut dem Urteil des Bundesverfassungsgerichts für den Einsatz elektronischer Wahlgeräte muss gelten, dass "die wesentlichen Schritte der Wahlhandlung und der Ergebnisermittlung vom Bürger zuverlässig und ohne besondere Sachkenntnis überprüft werden können". Daraus resultiert die Notwendigkeit der Überprüfung der Integrität der Stimmabgabe und der Stimmauszählung seitens des Wählers. Bei der papierbasierten Wahl wird dem Wähler diese Überprüfung durch physische Anwesenheit bei allen Wahlhandlungen ermöglicht. In der elektronischen Variante von Wahlen liegt die Herausforderung darin, geeignete Verfahren zu identifizieren, die die Grundsätze der Öffentlichkeit und der geheimen Wahl gleichzeitig realisieren. Ein Ansatz hierfür sind die sogenannten End-to-End verifizierbaren e-Voting-Protokolle. In diese Kategorie gehören die Protokolle ThreeBallot, Punchscan, Bingo Voting und Prêt-à-Voter. Im vorliegenden Beitrag werden diese Protokolle mit dem Ziel untersucht, diejenigen Verfahren zu identifizieren, welche den Anspruch des Urteils auf die Nachvollziehbarkeit der Wahl durch den Bürger erfüllen. Nachdem ein kurzer Überblick über die Funktionsweise der Protokolle entlang der Wahlphasen gegeben wird, werden Kriterien für eine weitere systematische Betrachtung definiert. Es sind folgende Fragestellungen zu beantworten: Inwiefern gewährleisten die genannten Wahlverfahren die Integrität der Stimmen sowie der Stimmauszählung und welche Verifikationsmethoden nutzen sie dafür? Wie ist die Benutzerfreundlichkeit der Wahlverfahren bzgl. der Verifikation zu bewerten? Wie ergonomisch ist der Wahlzettel gestaltet? Wie einfach kann der Wähler die Richtigkeit der Ergebnisse und die Existenz des eigenen Votums überprüfen? Es lässt sich zusammenfassend festhalten, dass bzgl. der Integrität von Stimmzettel und Stimmauszählung vielfältige korrekte Lösungen angeboten werden, deren Überprüfbarkeit und Nachvollziehbarkeit für den Wähler jedoch nicht möglich ist. Eine weitere Konsequenz aus dem Urteil des BVerfG ist, die erneute Durchführung von Sicherheitsanalysen bzgl. der Integrität und Verifizierbarkeit bestehender Protokolle. Der Grund liegt darin, dass bei den Wahlprotokollen Annahmen getroffen wurden, welche den Anforderungen, die sich aus dem Urteil des BVerfG ergeben, nicht genügen. Aufgrund des Umfangs des Papers wird nur das Bingo Voting dementsprechend analysiert und ein Angriff auf die Integrität der Stimme durch die Manipulation des verwendeten Zufallszahlengenerators samt einer Gegenmaßnahme vorgestellt.