Elektronische Wahlen: Verifizierung vs. Zertifizierung

Melanie Volkamer[1], Guido Schryen[2], Lucie Langer[1], Axel Schmidt[1], Johannes Buchmann[1]

[1]CASED
Technische Universität Darmstadt
volkamer@cased.de
langer,axel,buchmann@cdc.informatik.tu-darmstadt.de

[2]International Computer Science Institute, Berkeley
schryen@winfor.rwth-aachen.de

Der Beitrag diskutiert die kontroversen Ansätze – Verifizierung versus Evaluation/Zertifizierung – zur Sicherung elektronischer Wahlen mit Wahlgeräten. Dazu werden zunächst beide Ansätze definiert. Es werden insbesondere die verschiedenen Implementierungsformen für die Verifizierung vorgestellt.

Das Urteil des Bundesverfassungsgerichts spielt bei der weiteren Diskussion eine zentrale Rolle. Hierin wird entschieden, dass die Zertifizierung des Wahlgerätes nicht ausreicht und es werden Verifizierungsfunktionen gefordert, die den Wählern die Möglichkeit geben sich von der Integrität des Wahlergebnisses zu überzeugen, um so das Öffentlichkeitsprinzip umzusetzen. Allerdings lässt das Urteil die Ausgestaltung und Stärke der Verifizierungsfunktionen offen.

Dabei wird begründet, dass die individuelle und universelle Verifizierbarkeit nur einen Teil der Anforderungen an Wahlgeräte abdeckt und insbesondere nicht sicherstellt, dass das Gerät das Wahlgeheimnis sichert. Daher ist es mindestens für diese Anforderungen erforderlich, das Wahlgerät außerdem zu zertifizieren. Daher wird eine Kombination beider Techniken diskutiert, die das Vertrauen in die Integrität einzelner Komponenten reduziert. Es wird außerdem die Frage diskutiert, warum der Zertifizierung hinsichtlich dieser zusätzlichen Anforderungen vertraut werden kann, während dies nicht der Fall bei der Integritätsanforderung ist. Der Beitrag wirft abschließend hierzu die Frage auf, ob das Urteil die Verifizierbarkeit nicht nur für die Integrität sondern auch für die anderen Anforderungen wie das Wahlgeheimnis fordert. Dieses Thema stellt eine offene Forschungsfrage dar, die nicht abschließend geklärt wurde. Allerdings wird dieses Thema auch weitere Forschungsfragen auf, beispielsweise hinsichtlich der Ausgestaltung der Verifizierungsfunktionen und deren Benutzerfreundlichkeit.