Verifizierbarkeit elektronischer Wahlen

Lucie Langer I Axel Schmidt I Melanie Volkamer

abstract

Am 3. März 2009 hat das Bundesverfassungsgericht die bei der letzten Wahl des Deutschen Bundestages verwendeten Wahlcomputer für verfassungswidrig erklärt, weil sie dem Grundsatz der Öffentlichkeit der Wahl nicht ausreichend entsprechen. Das Urteil wirft hinsichtlich des zukünftigen Einsatzes elektronischer Wahlsysteme folgende Fragen auf: Wie kann die rechtliche Forderung nach Öffentlichkeit durch technische Verifizierungsmechanismen erfüllt werden? Erfordern entsprechende Maßnahmen tiefere Sachkenntnis seitens des Wählers? Der Beitrag untersucht exemplarisch zwei elektronische Wahlsysteme, die Verifizierbarkeit bieten, hinsichtlich ihrer Konformität mit dem Urteil. Dabei stellt sich heraus, dass der Aspekt der Benutzerfreundlichkeit bei elektronischen Wahlsystemen künftig stärker berücksichtigt werden muss.

Gesetzliche Forderungen. Die im deutschen Grundgesetz Art. 38 verankerten Wahlrechtsgrundsätze gebieten, dass eine Wahl allgemein, unmittelbar, frei, gleich und geheim sein muss. Das Urteil des Bundesver¬fass-ungsgerichts stellt heraus, dass dazu bei Bundestagswahlen auch der Grundsatz der Öffentlichkeit der Wahl kommt. Dieser lässt sich aus dem in Art. 20 Abs. 1 und 2 des Grundgesetzes verankerten Demokratieprinzip ableiten: Der Wähler delegiert die Staatsgewalt an die gewählten Vertreter und muss sich daher zuverlässig von der Rechtmäßigkeit des Übertragungsaktes überzeugen können (1, Rn.108). Daher müssen alle wesentlichen Schritte der Wahl, insbesondere Wahlhandlung und Ergebnisermittlung, öffentlicher Überprüfbarkeit unterliegen. Der Wähler muss selbst nachvollziehen können, ob seine Stimme unverfälscht erfasst und ausgezählt wurde, und zwar „ohne besondere Sachkenntnis“ (1, Rn.118, siehe auch Rn.119, 122). Die Kontrollierbarkeit des Wahlvorgangs kann nicht dadurch ersetzt werden, dass die Wahlgeräte vor ihrem Einsatz „auf ihre Übereinstimmung mit bestimmten Sicherheitsanforderungen und auf ihre technische Unversehrtheit hin“ überprüft werden, wie im Falle der in Deutschland eingesetzten Wahlgeräte angenommen (1, Rn.123). Eine reine Evaluierung und Zertifizierung reicht demnach nicht aus (2).

Dieser rechtlichen Forderung nach Öffentlichkeit der Wahl entspricht die technische Anforderung der Verifizierbarkeit. Dabei wird zwischen individueller Verifizierbarkeit durch den Wähler und universeller Verifizierbarkeit durch die interessierte Öffentlichkeit (inkl. Wähler) unterschieden. Beide Formen der Verifizierbarkeit können unterschiedlich stark umgesetzt werden: Im Fall der individuellen Verifizierbarkeit wird beispielsweise unterschieden, ob der Wähler nur feststellen kann, ob seine Stimme berücksichtigt wurde, oder zusätzlich feststellen kann, dass sie so gezählt wurde wie beabsichtigt. Im Fall der universellen Verifizierbarkeit wird zum Beispiel unterschieden, ob es lediglich möglich ist, die Stimmen erneut auszuzählen, oder ob zusätzlich verifiziert werden kann, dass im Ergebnis nur Stimmen von berechtigten Wählern berücksichtigt wurden.

Im Urteil wird nicht festgelegt, welche Stärke der Verifizierbarkeit gefordert wird. Es wird lediglich darauf hingewiesen, dass es nicht ausreicht, wenn der Wähler „ausschließlich durch eine elektronische Anzeige darüber unterrichtet wird, dass seine Stimmabgabe registriert worden ist“ (1, Rn.119). Laut Urteil sind insbesondere Wahlgeräte geeignet, die eine „von der elektronischen Stimmerfassung unabhängige Kontrolle“ bieten, indem sie die Stimme neben der elektronischen Speicherung noch anderweitig erfassen, z.B. in Form eines Ausdrucks, der durch den Wähler überprüft werden kann (1, Rn.121). Es ist allerdings fraglich, auf die Korrektheit eines Ausdrucks zu vertrauen, der aus einem Wahlgerät stammt, dem man misstraut: Ein manipuliertes Wahlgerät kann auch manipulierte Papierausdrucke erzeugen (3).

Technische Umsetzung. Verifizierbarkeit kann auf der Basis kryptographischer Verfahren oder auf der Basis von Papierstimmzetteln mit technischen Hilfsmitteln realisiert werden. Im Folgenden betrachten und diskutieren wir

zwei entsprechende Vorschläge aus der Literatur für die Umsetzung der Verifizierbarkeit in elektronischen Wahlsystemen.

Andrew Neff hat 2004 ein Verfahren vorgeschlagen, das sowohl individuelle als auch universelle Verifizierbarkeit bietet und dazu kein Vertrauen in das Wahlgerät erfordert (4). Nachdem der Wähler seine Stimme am Gerät eingegeben hat, generiert dieses den verschlüsselten Stimmzettel, der für jeden Kandidaten eine Zeile mit mehreren Bit-Paaren enthält. Während diese Paare in der Zeile des gewählten Kandidaten von der Form (0,0) oder (1,1) sind, haben die Paare in allen anderen Zeilen die Form (0,1) oder (1,0). Die Bit-Paare sind jedoch verschlüsselt, so dass ihre Form nicht erkennbar ist. Das Wahlgerät bekennt sich nun zu den Bits, die für den gewählten Kandidaten gesetzt wurden, d.h. es gibt eine 1 für jedes verschlüsselte Paar (1,1) an und eine 0 für jedes Paar (0,0). Der Wähler fordert das Gerät daraufhin auf, für jedes Bit-Paar entweder das linke oder das rechte Bit aufzudecken. Da das Wahlgerät vorher nicht weiß, welches Bit es für jedes Paar nun aufdecken muss, kann es keine Stimme für einen anderen Kandidaten abgeben als vom Wähler beabsichtigt, ohne dass dieser den Betrugsversuch mit großer Wahrscheinlichkeit entdeckt. Würde das Wahlgerät z.B. die Bit-Paare der Zeile des gewählten Kandidaten, welche die Form (0,0) oder (1,1) haben, durch Paare der Form (0,1) oder (1,0) ersetzen, um so die Stimme zu fälschen, so würde der Wähler diesen Betrug mit großer Wahrscheinlichkeit entdecken. Hätte das Wahlgerät z.B. aus (0,0) das Paar (0,1) gemacht und sich zu „0“ bekannt, und der Wähler würde nun fordern, die rechte Seite aufzudecken, so käme eine „1“ zum Vorschein und der Betrug des Wahlgeräts wäre entlarvt. Diese Überprüfung erfolgt für jedes Bit-Paar der Zeile. Aufgrund der hohen Anzahl von Bit-Paaren ist die Wahrscheinlichkeit sehr groß, dass eine solche Manipulation entdeckt wird. Die einzelnen Schritte dieser Interaktion werden in Form eines Papierausdrucks festgehalten.
Neffs Ansatz ist vielversprechend und bietet ein hohes Maß an Verifizierbarkeit, setzt allerdings beim Wähler Sachkenntnis voraus. Es stellt sich daher die Frage, wie man derartige Verfahren für den Wähler verständlicher und benutzbarer machen kann.

Einen anderen Ansatz schlägt Rivest mit seinem Three-Ballot-System vor (5). Hierbei gibt der der Wähler seinen Stimmzettel in Papierform ab und der Inhalt wird anschließend elektronisch erfasst. Das System verzichtet dabei völlig auf kryptographische Verfahren: Der Stimmzettel enthält in jeder Zeile einen Kandidaten und je Kandidat drei Spalten. Der Wähler macht für jeden Kandidaten in beliebigen Spalten zwei Kreuze, wenn er für diesen Kandidaten stimmen möchte, und ein Kreuz, wenn er gegen ihn stimmen will. (Bei der Zählung der Stimmen muss später bei jedem Kandidaten die Anzahl der Wähler abgezogen werden, um die tatsächliche Stimmenzahl zu erhalten.) Die drei Spalten werden daraufhin voneinander getrennt, und der Wähler sucht sich eine davon aus, deren Kopie er als Beleg behält. Anhand der eindeutigen ID, die auf jeder Spalte aufgedruckt ist, kann er sich später davon überzeugen, dass seine Stimme gezählt wurde.

Dieses Verfahren erfordert deutlich weniger technisches Verständnis vom Wähler. Auch hier wird die Verifizierbarkeit (unter Wahrung des Wahlgeheimnisses) jedoch durch eine erhöhte Komplexität erkauft: Es ist sicherlich verwirrend für den Wähler, wenn er auch Kandidaten ankreuzen muss, die er gar nicht wählen möchte. Daher sollte auch hier mehr Wert auf Benutzerfreundlichkeit gelegt werden.

Fazit. Dass Verifizierbarkeit eine zentrale Anforderung an elektronische Wahlsysteme ist, hat das Urteil des Bundesverfassungsgerichts deutlich herausgestellt. Diese Forderung ist allerdings nicht immer trivial in existierende Systeme zu integrieren, da sichergestellt werden muss, dass durch die Verifizierbarkeitsmechanismen nicht das Wahlgeheimnis gefährdet wird. Es ist weiterhin zu bedenken, dass die zu Grunde liegenden Wahlprotokolle durch die Integration von Verifizierungsmechanismen komplexer und damit auch fehleranfälliger werden (2). Eine Form der Verifizierbarkeit, die keinerlei Ansprüche an den Wähler stellt, erscheint kaum realisierbar. In technischer Hinsicht ist es somit eine Herausforderung, den bislang wenig beachteten Aspekt der Benutzerfreundlichkeit in verifizierbare Systeme zu integrieren. ■

literatur

(1) Urteil des Zweiten Senats vom 3. März 2009, 2 BvC 3/07, 2 BvC 4/07. URL: http://www.bundesverfassungsgericht.de/entscheidungen/cs20090303_2bvc000307.html

(2) Volkamer, M./ Schryen, G./ Langer, L./ Schmidt, A.;/ Buchmann, J. (2009): **Elektronische Wahlen: Verifizierung vs. Zertifizierung.** In: Informatik 2009: erscheint in Kürze.

(3) Buchmann, J./ Roßnagel, A. (2009): **Das Bundesverfassungsgericht und Telemedienwahlen. Zu den Auswirkungen des Urteils des Bundesverfassungsgerichts zu elektronischen Wahlgeräten für die Durchführung von „Internetwahlen“ in nicht-politischen Bereichen.** In: Kommunikation und Recht (K&R) 2009, Heft 7/8.

(4) Neff, C. A. (2004): **Practical high certainty intent verification for encrypted votes. VoteHere.** URL: http://www.votehere.com/old/vhti/documentation/vsv-2.0.3638.pdf.

(5) Rivest, R. L. (2006): **The ThreeBallot Voting System.** URL: http://people.csail.mit.edu/rivest/Rivest-TheThreeBallotVotingSystem.pdf

Dipl.-Math. Lucie LANGER
Technische Universität Darmstadt
Wissenschaftliche Mitarbeiterin am Fachgebiet Theoretische Informatik
langer@cdc.informatik.tu-darmstadt.de

Dipl.-Math. Axel SCHMIDT
Technische Universität Darmstadt
Wissenschaftlicher Mitarbeiter am Fachgebiet Theoretische Informatik
axel@cdc.informatik.tu-darmstadt.de

Dr. Melanie VOLKAMER
Technische Universität Darmstadt
Wissenschaftliche Mitarbeiterin und Koordinatorin des Arbeitsbereiches Sichere Daten von CASED
volkamer@cased.de