Risiken von E-Voting

Sicherheit und Probleme elektronischer Wahlen

Barbara Ondrisek

Der Entschluss der Politik, bei den kommenden Wahlen der Österreichischen HochschülerInnenschaft im Frühling 2009 E-Voting einzusetzen, alarmiert Kritiker wie Rechtsexperten. Die Transparenz des Wahlvorganges ginge verloren und die Grundsätze des freien, geheimen und persönlichen Wahlrechts seien gefährdet. Zudem gäbe es eine Reihe von weiteren Risiken und Sicherheitsproblemen bei elektronischen Wahlen.

E-Voting und Wahlrecht

Elektronische Wahlen sind ein sehr umstrittenes Gebiet. Eine Reihe von Fehlern und Schwachstellen in E-Voting-Systemen wurden vor allem in den USA gefunden [11, 13]: Es gibt nur schwache oder unvollständige Standards zur Implementierung von elektronischen Wahlsystemen [1] und viele (wissenschaftliche) Experten wie M. Bishop und D. Wagner sprechen sich explizit gegen den Einsatz von E-Voting aus. Dennoch gibt es weitreichende Bestrebungen, E-Voting in Staaten einzusetzen, in denen bisher Urnenwahlen stattfanden, wie z. B. in Österreich.

Mit E-Voting (engl. für „elektronische Wahlen") ist jene Wahlmethode gemeint, mit der Stimmen auf elektronischem Weg repräsentiert oder gesammelt werden können. Die verschiedenen Arten von elektronischen Wahlen reichen von Internetwahlsystemen über Wahlmaschinen bis hin zu optischen Scannern, die Papierstimmzettel automatisiert auswerten.

Die Wahlrechtsgrundsätze, auf denen jede Wahlform basiert, sind in der (österreichischen) Verfassung verankert und besagen, dass jeder Bürger oder jede Bürgerin das Recht auf eine allgemeine, freie, gleiche, persönliche, unmittelbare und geheime Ausübung seines oder ihres Wahlrechts hat. Bei elektronischen Wahlen sind allerdings die Grundsätze des freien, geheimen und persönlichen Wahlrechts, besonders in Hinblick auf Stimmenkauf und Wahlzwang, umstritten, worauf später näher eingegangen wird.

Vorteile von E-Voting

Trotz der Kontroversen, die dieses Thema hervorbringt, gibt es durchaus Vorteile des E-Votings, die von den Befürwortern immer wieder hervorgehoben werden: Schnellere Auszählungen, Modernisierung und Zukunftsorientierung, das Verhindern unabsichtlich ungültiger Stimmen (besonders bei speziellen Auswertungsformen wie Panaschieren oder Kumulieren) und Vorteile für körperlich benachteiligte Personen (Stichwort: barrierefreies Wählen). Weiters werden finanzielle Ersparnisse, Steigerung der Wahlbeteiligung, leichtere Einbindung von Wählern aus dem Ausland wie auch Anwendung der direkten Demokratie genannt [14].

Wo liegen die Probleme?

Der Einsatz elektronischer Wahlen hat, Kritikern zufolge, allerdings nicht nur positive Aspekte. Zum Einen ergibt sind bei E-Voting das generelle Problem der Transparenz. Die Maschine – eine Blackbox – macht etwas, das selbst für Techniker nicht direkt

DOI 10.1007/s00287-009-0341-x

Barbara Ondrisek
Technische Universität Wien,
Karlsplatz 13, 1040 Wien, Österreich
E-Mail: barbara.ondrisek@gmx.net

Published online: 03 April 2009

Zusammenfassung
E-Voting ist ein sehr kontroverses Gebiet. Die Wahlbeteiligung nimmt kontinuierlich ab, weshalb einige Politiker meinen, ein Allheilmittel entdeckt zu haben: Internetwahlen als zusätzliche Wahlmethode. Obwohl IT-Experten und Datenschutzrechts-Spezialisten sich gegen elektronische Wahlen aussprechen, wird es in Österreich bei der kommenden Wahl der Österreichischen HochschülerInnenschaft im Frühling 2009 dennoch einen Echtwahlversuch mit Internetwahlen geben. Die Vorteile von E-Voting wie Erhöhung der Wahlbeteiligung durch zusätzliche Wahlkanäle und Kostenersparnis wurden allerdings durch Studien bereits entkräftet: Durch elektronische Verfahren seien vielmehr die Wahlrechtsgrundsätze gefährdet und die Transparenz des Wahlvorgangs ginge verloren, meinen Kritiker.

erkennbar ist. Das Speichern und das Berechnen der Wahlergebnisse bleibt dem Wähler verborgen [18]. Es könnten sich beabsichtigte wie auch unbeabsichtigte Fehler oder Schwachstellen eingeschlichen haben, die auch durch strenge Qualitätskontrollen schlüpfen können. So wurden bei vergangenen Wahlen oft Unregelmäßigkeiten im Wahlergebnis gefunden [23, 24], bei Untersuchungen der eingesetzten Wahlmaschinen wurden sogar gravierende Sicherheitsmängel entdeckt [3, 8, 13] sowie mögliche Attacken nachgewiesen, wie etwa ein Tempest-Angriff oder die Manipulation des Boot-Loaders der Maschine. Zudem beharren Hersteller von E-Voting-Systemen meist auf proprietärer Soft- und Hardware, die nicht offen gelegt werden, da sie fürchten, dass Sicherheitslücken oder Betriebsgeheimnisse ausspioniert werden könnten.

Bei Wahlsystemen muss eine Unterscheidung zwischen sogenanntem Retail bzw. Wholesale Fraud gemacht werden [20, S. 37]: Bei einem Wholesale-Angriff kann schon eine einzige Person das gesamte Wahlergebnis manipulieren. Auf diese Art kann mit kleinem Aufwand [4] großer Schaden entstehen. Im Vergleich dazu können bei einem dezentralen Retail-Angriff nur einige wenige Maschinen in kurzer Zeit manipuliert werden, wie auch bei der Papierwahl.

Zum Anderen konnte das Argument der Kosteneinsparung durch E-Voting durch konkrete Zahlen aus Belgien (parlamentarische Anfragen belegen, dass sich die Kosten pro Wählerstimmer verdreifacht haben) und durch Studien in Quebec (Steigerung der Kosten um 25%) [10] widerlegt werden. Ebenfalls wurde gezeigt, dass diese These in England nicht belegt werden konnte, als bei fünf Pilotversuchen bei Kommunalwahlen Anfang Mai 2007 die Kosten pro Wählerstimme nach offiziellen Angaben umgerechnet zwischen 150 und 900 € gelegen haben [22]. Eine Papierstimme kostet im Vergleich dazu etwa 1,5 €.

Zusätzlich sind aus Schweden [9] wie auch aus England Entkräftungen des Arguments für die Steigerung der Wahlbeteiligung bei *Multi-Channel-Voting* bekannt, da sich die von der Regierung erwartete höhere Wählerbeteiligung bei den Pilotversuchen nicht eingestellt hat [18]. Eine Steigerung des politischen Interesses scheint somit nicht durch alternative Möglichkeiten der Stimmabgabe, sondern nur durch eine Änderung der demokratischen Kultur möglich zu sein.

Papierbelege bei E-Voting

Ein weiteres Problem bei Wahlcomputern sind fehlende Papierbackups für erneute, aussagekräftige Auszählungen [6]. Eine von vielen Seiten [8, 12, 13, 15] geforderte Maßnahme ist der Einsatz von Kontrollbelegen, die von Wählern überprüfbar sind – der sogenannte Voter-Verified Paper Trail (VVPT). Zusätzlich zur elektronischen Speicherung wird die Stimme hier auch auf einem Papierbeleg gesichert, mit dem gezeigt wird, dass die Stimme, die abgegeben wurde, auch tatsächlich der entspricht, die man abgeben wollte. Mit diesen Papierbelegen kann mittels sogenannter Bulletinboards überprüfbar sein, dass die Stimme im Ergebnis enthalten ist. Ein Kontrollbeleg kann für spätere geräteunabhängige Nachzählungen verwendet werden und dient ebenfalls zur Überprüfung der Korrektheit einzelner Maschinen. Dieses Verfahren ermöglicht bedeutungsvolle Neuzählungen und Audits und stichprobenartige Überprüfungen der Maschinen [5].

VVPT-Verfahren werden allerdings oft kritisiert, da sie versuchen, Transparenz in einen von Haus aus nicht transparenten Prozess zu bringen. Daher ist der Einsatz von VVPT, besonders bei nachträglicher Installation in einem bereits eingesetzten E-Voting-System, umstritten. Zudem kann der VVPT das geheime Wahlrecht untergraben, da man so einen Beleg für die Stimme erhält. Ein weiterer

Abstract

E-Voting has become a very controversially discussed topic during the last few years. Primarily caused by the fact of decreasing voter participation, some politicians regard e-voting as the magic bullet. Although IT experts and data privacy specialists disapprove of it, e-voting will be introduced during the upcoming Austrian Students' Union polls in early 2009.

All advantages of e-voting, like an increased turnout of voters due to additional voting channels or cost reduction, have already been rebutted by a number of studies. Critics also strongly emphasize the disadvantages of electronic elections, such as violating the principles of electoral law as well as the loss of transparency of the voting process.

Kritikpunkt ist, dass es durch den Einsatz von VVPT nur zu höherer Komplexität und zu zusätzlichen Kosten kommen würde [2].

Internetwahlen

Wählen über das Internet, auch I-Voting genannt, als Spezialfall elektronischer Wahlen ist ein Beispiel für Distanzwahlen und birgt durch die Verknüpfung zum Internet weit höhere Sicherheitsrisiken in sich als andere E-Voting-Verfahren. Den Vorteilen von Internetwahlen wie Wählen „im Pyjama", höhere Wahlbeteiligung, Steigerung der Mobilität für Wähler (vor allem für Auslandswähler), Kostenersparnisse, breiterer Zugang und weitere Zugriffsmöglichkeiten [16] werden schwerwiegende Nachteile von Kritikern entgegengehalten.

Zunächst sind diese zusätzlichen Sicherheitsrisiken des E-Votings mit den allgemeinen Sicherheitsproblemen des Internets eng verbunden, speziell der Möglichkeit verschiedener Angriffe wie z. B. Hacker_Attacken, Phishing, Viren, Trojaner, Lauschangriffe, Malware, Spyware, Rückverfolgbarkeit, vor allem aber *(Distributed) Denial-of-Service*-Attacken, gegen die es beim heutigen Stand der Technik keinen hinreichenden Schutz gibt. Das geheime Wahlrecht könnte durch Vorratsdatenspeicherung, Online-Durchsuchungen (etwa mittels Bundestrojaner), *Deep Packet Inspection* oder das Ausspionieren von IP-Adressen nicht gewährleistet werden, da eine Zuordnung von Stimmen zu Wählern möglich wäre.

Zusätzlich beherbergen Internetwahlen (wie auch jede andere Form von Distanzwahlen) ein weiteres großes, nicht-technisches Problem: Den Stimmenkauf. Der Wähler gibt seine Stimme in einer nicht von der Wahlkommission kontrollierten Umgebung ab. So werden bei Distanzwahlen Methoden der unzulässigen Wählerbeeinflussung erleichtert, wie Erpressung (etwa Anordnungen im Familienkreis, auch Family Voting genannt, oder Andere) [7]. Bereits bei den erst kürzlich in Österreich eingeführten Briefwahlen, für die die Österreichische Bundeswahlbehörde bei den Big Brother Awards 2008 nominiert wurde, gab man dem allgemeinen Wahlrecht zugunsten des freien, geheimen und persönlichen Wahlrechts den Vorzug.

Weiters befinden sich die Möglichkeiten der Verbrechensverfolgung von Tätern über das Internet – zu deren Gunsten – in einem rechtlichen Graubereich. So sind etwa Angriffe über ausländische Server aus strafrechtlichen Gründen nicht nach österreichischem Recht verfolgbar. Auch stellen Internetwahlen die Gleichberechtigung der Bürger (Bevorzugung von Personen mit Internet, Technologieverständnis älterer Mitbürger, eventuelle Kosten zusätzlicher Geräte, wie etwa Chipkartenlesegeräten, etc.) vor ein Problem.

Wahlen über das Internet bieten zudem weder eine Möglichkeit für aussagekräftige Audit-Verfahren (Audits bezeichnen allgemeine Untersuchungsverfahren), noch für authentische, erneute Auszählungen, da keine Papierbelege verwendet werden können. Die Stimmauszählung entzieht sich vollständig den Augen der Wahlkommission und Wahlbeobachtern, was in Widerspruch zum Öffentlichkeitsprinzip und zum Transparenzgebot steht und den Nachweis von Manipulationsfreiheit unmöglich macht. Damit ist es bei E-Voting-Verfahren äußerst schwierig, Transparenz und die Überprüfbarkeit der Richtigkeit des Wahlergebnisses sicherzustellen, wodurch auch das Vertrauen in diese Systeme schwindet. Solche Probleme haften allen Distanzwahlverfahren, wie auch der Briefwahl, an.

Zahlreiche Wissenschaftler, Techniker und Gruppierungen, wie etwa Peter G. Neumann, der Chaos Computer Club in Deutschland oder Ronald L. Rivest vom MIT sowie viele andere [15, 19] sprechen sich ebenfalls explizit gegen Internetwahlen aus.

Internetwahlen werden häufig fälschlicherweise mit E-Banking oder anderen Online-Anwendungen verglichen. Allerdings hinkt der Vergleich stark, da bei E-Voting im Gegensatz zu allen anderen Internet-Applikationen eines gewährleistet werden muss: Auf der einen Seite Kontrolle über den Benutzer (Identifikation, Authentifizierung etc.) und auf der anderen Seite Anonymität (geheimes, freies Wahlrecht). Beim Online-Banking ist der Benutzer bekannt und man kann jederzeit den Geldfluss nachverfolgen, beim E-Voting gibt es keine direkte Nachvollziehbarkeit, da die Stimme anonym abgegeben und gespeichert wird.

Papierwahlen

Das heutige Papierwahlsystem überzeugt und besticht durch seine Einfachheit. Man kann die Schritte, die für jeden verständlich sind, selbst einem Volksschüler erklären. Es ist ein durchdachtes, bewährtes System mit einem bestimmten Ablauf mit mehreren Kontrollfunktionen. Es ist transparent, da es auch Wahlbeisitzer und Wahlbeobachter einbezieht. Jeder, auch Leute ohne technisches Wissen, können sich vor, während und bei der Wahl von der Korrektheit überzeugen. Bei E-Voting-Systemen ist die Kenntnis des genauen Ablaufes nur wenigen Experten vorbehalten, in technischen Details kann sich allerdings auch der beste Programmierer verstricken, zumal Fehler niemals hundertprozentig ausgeschlossen werden können.

Eine weitere Frage ist die generelle Motivation, warum E-Voting überhaupt eingesetzt werden soll. Wieso ein bestehendes, vertrauenswürdiges System ersetzen, das funktioniert? Vertreter von E-Voting argumentieren in diesem Zusammenhang, dass traditionelle Wahlverfahren ebenfalls Sicherheitslücken enthalten (etwa Stimmenkauf mit Briefwahl, Kameras in Wahlzellen), die teilweise mit elektronischen Verfahren gesichert werden könnten.

Sicherheit

Neben den bereits erörterten aktuellen Problemen bei elektronischen Wahlen stellt sich auch die Frage, ob die derzeit verfügbare Soft- und Hardware überhaupt schon sicher genug ist, um für ein derartig kritisches Szenario wie elektronische Wahlen eingesetzt zu werden. Einige Kritiker behaupten, Sicherheitskonzepte und Sicherheitsmechanismen seien mit dem heutigen Stand der Technik überhaupt nicht möglich und heutige elektronische Systeme inhärent fehlerhaft [7].

So erwartet auch der Sicherheitsexperte Klaus Brunnstein eine markante Steigerung der Sicherheit in der IT-Branche erst in 20 Jahren, wenn „die Unfälle so gravierend geworden sind, dass man die Sicherheitsdefizite nicht mehr akzeptiert“ [21]. Die Computertechnik durchläuft die gleichen Zyklen wie jede andere technologische Veränderung: Zuerst gibt es Hoffnung, dass die neue Technologie Probleme lösen wird, dann Verzweiflung, weil die Technologie die hohen Erwartungen nicht erfüllt, und letztendlich greift ein regulierendes Element (etwa eine staatliche Behörden) ein, um die neue Technologie in die Gesellschaft zu integrieren.

Die größten Probleme von E-Voting sind der Mangel an Vertrauen und Akzeptanz, die fehlende Transparenz des Vorganges, keine oder unzulängliche Papierbackups für erneute Auszählungen, fehlende Nachweisbarkeit über die Manipulationsfreiheit des Systems, schlechte Handhabbarkeit sowie fehlende Kontrolle für die Wahlkommission vom Source-Code bis zum Transfer der Stimme. Zusätzlich dazu gibt es den großen Widerspruch, der im E-Voting steckt: Die Stimmabgabe soll einerseits geheim, andererseits aber auch kontrollierbar bleiben, um Manipulationen auszuschließen. Mit E-Voting wird blindes Vertrauen in die Technik vorausgesetzt und somit die Sicherheit des gesamten demokratischen Prozesses gefährdet.

Literatur

1. Barr E, Bishop M, Gondree M (2007) Fixing Federal E-Voting Standards. In: Communications of the ACM, vol. 50. Emergency response information systems: emerging trends and technologies. Column: Viewpoint. ACM 3:19–24, ACM, New York, NY, USA
2. Castro D (2007) Stop the Presses: How Paper Trails Fail to Secure e-Voting. Report. The Information Technology & Innovation Foundation (18. September 2007), S 1–19
3. Chaos Computer Club (2006) Bericht der CCC-Wahlbeobachtergruppe von der Oberbürgermeisterwahl in Cottbus (24. Oktober 2006)
4. Di Franco A, Petro A, Shear E, Vladimirov V (2004) Small vote manipulations can swing elections. In: Communications of the ACM, vol. 47. Voting systems – SPECIAL ISSUE: The problems and potentials of voting systems 10:43–45
5. Dill D, Rubin A (2004) E-Voting Security. IEEE Security Priv Magazine 2(1): 1540–7993
6. Dill D, Schneier B, Simons B (2003) Voting and Technology: Who Gets to Count Your Vote? Communications of the ACM 46(8):29–31
7. Evans D, Paul N (2004) Election security: Perception and reality. IEEE Security Priv Magazine 2(1):24–31
8. Feldman A, Halderman J, Felten E (2006) Security Analysis of the Diebold AccuVote-TS Voting Machine. Princeton University, Princeton
9. Grönlund Å (2002) Private Sanctity – e-Practices Overriding Democratic Rigor in e-Voting. In: Traunmüller R, Lenk K (Hrsg) EGOV 2002. Lect Notes Comput Sci 2456:52–60
10. Gyulai L (2006) Plug pulled on electronic voting – High-tech balloting cost 25 per cent more. The Gazette (25. Oktober 2006)

11. Harris B (2004) Black Box Voting: Ballot-Tampering in the 21st Century. Talion Publishing, Renton, USA
12. Jones M (2005) The Pedagogic Opportunities of Touch-Screen Voting. In: ACM SIGCSE Bulletin, SESSION: E-voting, ethics, and infrastructure for computing education. ACM 37(3):223–226
13. Kohno T, Stubblefield A, Rubin A (2004) Analysis of an Electronic Voting System. In: Security and Privacy, 2004. Proceedings 2004 IEEE Symposium on 9–12 May 2004, S 27–40
14. Maidou A, Polatoglou H (2004) E-Voting and the architecture of virtual space. In: Proceedings of the 1st International Workshop on Electronic Voting. "Electronic Voting in Europe: Technology, Law, Politics and Society". GI, Bonn, S 133–142
15. Mercuri R (2002) A better ballot box? Spectr IEEE 39(10):46–50
16. Mohen J, Glidden J (2001) The case for Internet Voting. Commun ACM 44(1):72–85
17. Ondrisek B (2008) Sicherheit elektronischer Wahlen. Verlag Dr. Müller
18. Open Rights Group (2007) Election Report – Findings of the Open Rights Group Election Observation Mission in Scotland and England (20. Juni 2007)
19. Philippsen M (2002) Internetwahlen – Demokratische Wahlen über das Internet. Informatik-Spektrum 25(2):138–150
20. Rubin A (2006) Brave new ballot – the battle of safeguard democracy in the age of electronic voting. Morgan Road Books
21. Sagatz K (2004) Den sicheren PC gibt es erst in zwanzig Jahren. Interview geführt mit Kurt Brunnstein. Der Tagespiegel (12. Mai 2004)
22. Sietmann R (2007) Wähler-Selbstkontrolle – Experten ringen um Vertrauen in elektronische Wahlmaschinen. c't 19:84
23. USA Today (2004) More than 4,500 North Carolina votes lost because of mistake in voting machine capacity. The Associated Press (4. November 2004)
24. K Zetter (2004) E-Vote Snafu in California County. Wired Magazine, Politics: Security (31. September 2004)