

Gutachten

e-Voting mit Open Source

Information Rules 1, Gruppe 12
Dinçel Ataç, Birol Kayapinar, Wolfram Riedel

TU Berlin WS0304
11. Feb 2004

Inhaltsverzeichnis

1	Demokratie in Europa	3
2	e-Voting	3
2.1	Neue Wege zur Demokratie	3
2.2	Frappierende Sicherheitslücken und Fehler	4
2.3	Gefahren der Manipulation	5
3	Lösung Papier?	5
4	Lösung Open Source	6
4.1	Transparenz und Vertrauen	6
4.2	Nicht auf Kosten der Sicherheit	6
4.3	e-Voting mit Open Source ist bereits Realität	7
5	Empfehlung	8
6	Informationen	8

1 Demokratie in Europa

Seit 1979 wird in allgemeinen und direkten Wahlen das Europa-Parlament alle fünf Jahre gewählt. Fast 400 Millionen freie Bürger werden nach der EU-Ost-Erweiterung 2004 wahlberechtigt sein, viele zum ersten mal. (Wikipedia N.d.b)

Der Begriff „Demokratie“ stammt aus dem Griechischen und bedeutet soviel wie „Herrschaft des Volkes“. Das Volk ist der Souverän und bestimmt selber über seine Regierung. Die wichtigste Errungenschaft der Demokratie sind freie Wahlen. Eine Wahl gilt als demokratisch wenn sie allgemein, frei, gleich und geheim ist. Durch sie übt der freie Bürger das Recht aus, seine Meinung mit dem Abgeben seiner Stimme zu bekunden, sei es für eine Partei oder einzelne Personen. (Wikipedia N.d.a)

Wahlen finden traditionell auf Papier statt. Stimmzettel werden angekreuzt und ausgezählt. Die Prozedur ist langwierig, aufwendig und sehr kostenintensiv. Um die hohen Kosten und den enormen Aufwand von Wahlen, insbesondere in der Größenordnung einer Europawahl anzugehen, möchte man in Zukunft auf Technik statt Papier setzen.

Die Wahlen müssen von einer Kontrollinstanz überwacht werden, damit alles korrekt abläuft und der freie Bürger dem Wahlsystem vertrauen kann. Bis heute wird die Kontrolle durch Wahlhelfer ausgeübt. Sie sind eine Sicherheitsgarantie für den Wähler, dass seine Stimme korrekt gezählt wird. (Wikipedia N.d.a)

Aber wie vertrauenswürdig oder demokratisch ist ein Wahlsystem, bei dem die Wahlhelfer nun nicht mehr mitverfolgen können, daß jede Stimme korrekt gezählt wird?

2 e-Voting

2.1 Neue Wege zur Demokratie

Elektronisches Wählen bringt viele Vorteile. Sobald die Infrastruktur für elektronische Wahlen einmal aufgebaut ist, sind die Folgekosten gering. Nicht wie bei den bisher langwierigen Auszählungen von Hand kann mit e-Voting das Ergebnis innerhalb weniger Minuten zur Verfügung stehen.

Mit e-Voting lässt sich auch der Ablauf der Wahl flexibler gestalten. Beibehalten wird die Urne im Wahllokal, die sich zukünftig in elektronischer Form präsentiert. Eine entsprechende Verschlüsselung vorausgesetzt, lässt sich alternativ die Wahl auch vom heimischen PC aus tätigen oder von einem anderen Computer aus, der sich beispielsweise auch im Ausland befinden kann – ein Bequemlichkeitsfaktor, der die schwächelnden Wahlbeteiligungen deutlich ansteigen lassen könnte.

Die neuen Möglichkeiten klingen sehr verlockend, aber leider wirft die Technik auch neue Probleme auf.

2.2 Frappierende Sicherheitslücken und Fehler

Computertechnik ist sehr komplex und sehr viel schwieriger abzusichern als einige Stapel mit Stimmzetteln. Dieser Umstand wird von vielen derzeit unterschätzt.

Ein sehr unpassender Vergleich ist der mit Online-Shopping, wie er unlängst auf der Webseite des experimentellen Online-Wahlsystems SERVE¹ gezogen wurde. (Krüger 2004) Denn für e-Commerce gelten andere Anforderungen. So können auftretende Probleme bei Versandbestellungen immer im Nachhinein geklärt und einer Transaktion auch immer zwei bekannte Teilnehmer zugeordnet werden. Beim e-Voting gibt es nur genau einen Stichtag, an dem die Wahl stattfindet, und die geheime Stimme darf dem Wähler nach der Abgabe nicht mehr zugeordnet werden können. (Gerck, Neff, Rivest, Rubin & Yung 2002, p. 246)

Auf dem Markt befinden sich bereits einige kommerzielle Wahlsysteme, deren Quellcode nicht offenliegt. Leider häufen sich seit einiger Zeit die negativen Berichte über diese.

Die Hersteller scheinen schon die elementarsten Regeln zu missachten, die zum Bau von sicheren Geräten notwendig sind. Aus internen Dokumenten eines Herstellers geht hervor, dass seine Geräte die eigentlich einfachste Aufgabe, das Zählen der Stimmen, nicht richtig beherrscht und schonmal Stimmen abzieht anstatt sie immer nur zu addieren. (Krugman 2004)

Durch ein Sicherheitsproblem der Firma Diebold gelang Quellcode ihrer Wahlmaschinen an die Öffentlichkeit. Das Urteil von zahlreichen Experten ist erschreckend, sie entdeckten viele schwerwiegende Sicherheitslücken. Obwohl dieser und andere Hersteller beteuern, sie täten alles, um die Sicherheit und Fehlerfreiheit zu gewährleisten, zum Beispiel durch Testlabore und logische Überprüfungen des Codes, kann nicht davon ausgegangen werden, dass diese Systeme fehlerlos sind. (Dill, zitiert bei Jonietz 2004)

Ein weiterer, beunruhigender Vorfall geschah bei einer Wahl in Broward, Florida. Anscheinend wurden mit den brandneu angeschafften, elektronischen Wahlurnen ganze 134 Stimmen nicht gezählt. Die Wahl erfolgte rein elektronisch, es existieren somit keine Belege auf Papier und man kann im Nachhinein nur noch spekulieren. Dass sich die Wähler nicht für einen der ausschließlich republikanischen Kandidaten entscheiden konnten ist genauso vorstellbar wie ein Funktionsproblem der Software. Aber auch die Bedienung könnte das Problem verursacht haben, denn das Gerät ließ zu es, Stimmen abzugeben, ohne zuvor einen Kandidaten ausgewählt zu haben. (Bolstad 2004)

¹Secure Electronic Registration and Voting Experiment, <http://www.serveusa.gov>

2.3 Gefahren der Manipulation

Herkömmliche Wahlen werden von Wahlhelfern oder manchmal auch ausländischen Wahlbeobachtern verfolgt. Ihre Kontrolle ist bisher ein wesentlicher Sicherheitsfaktor. Mit papierlosen, elektronischen Wahlgeräten kann eine Auszählung der Stimmen aber nicht mehr beobachtet werden. Schlimmer noch, mit einem Wahlsystem ohne Zugriff auf den Programmcode wird selbst informationstechnisch ausgebildeten Fachleuten verwehrt, den Ablauf der Stimmzählung nachzuvollziehen. Die Wahlurne wird so zur Black-Box, bei der man nicht weiß, ob hinten auch wieder herauskommt was man vorne reingesteckt hat.

„Wahlen lassen sich manipulieren, Wahlbetrügereien sind bereits oft genug vorgekommen. Und mit dem Übergang zu digitalen Wahlmaschinen scheinen die Manipulationsmöglichkeiten zuzunehmen.“ Diese könnten nicht nur von den Herstellern, sondern auch von Außenstehenden vorgenommen werden, sogar von den Wählern selbst. (Rötzer 2003)

Die Gesetzgeber in den USA haben begonnen, elektronische Wahlurnen einzuführen, ohne die Herstellung und Funktionsweise ausreichend zu kontrollieren. Kritiker ermahnen zurecht, dass für die Erhaltung der heimischen Demokratie nur ein Bruchteil dessen ausgegeben wird, was für die Demokratisierung des Irak aufgewendet wird. (Krugman 2004)

Offenbar mangelt es noch an gesetzlichen Standards für elektronische Wahlen. Und so kommt es wohl, dass amerikanische Spielautomaten vermutlich sicherer sind als elektronische Wahlurnen, da sie vorgeschriebene Verfahren durchlaufen, die Manipulationen verhindern sollen. (Rubin, zitiert bei Damon 2003) Hier muss der Gesetzgeber aktiv werden bevor eine Infrastruktur aufgebaut wird.

3 Lösung Papier?

In der jüngsten Entwicklung, in der die Gefahren von e-Voting bereits diskutiert werden, ist man auf den Gedanken gekommen, einen Papierausdruck von jeder Stimme anzufertigen, die der Wähler überprüfen kann bevor er sie abgibt. Durch eine Nachzählung der Ausdrücke kann man auch noch lange nach der Wahl Klarheit über das Ergebnis bekommen. (Stone 2003)

Wir halten diese Maßnahme für unterstützenswert. Jedoch kann sie leider nicht das eigentliche Problem beseitigen, das durch eine nicht offene Wahlsoftware weiterhin besteht.

Sofern kein Verdacht auf Unkorrektheit besteht, könnten Papierausdrücke sogar eine trügerische Sicherheit vermitteln. Eine Fälschung der elektronischen Er-

gebnisse könnte weiterhin stattfinden und würde wohlmöglich nicht entdeckt. Eine obligatorische Nachzählung ausgedruckter Stimmen könnte das Wahlergebnis mit Sicherheit bestätigen, Aufwand und Kosten wären dadurch aber ähnlich hoch wie bei herkömmlichen Wahlen.

Nach der papiergebundenen Präsidentschaftswahl 2000 in den USA, der ehemaligen Vorzeigedemokratie, wurde ein Kandidat trotz äußerst knapper Mehrheit faktisch zum Präsidenten ernannt bevor eine erneute Auszählung der Stimmen die tatsächlichen Wählerzahlen an den Tag brachte. Es scheint daher umso bedeutender, dass die Auszählung einer elektronischen Wahl schon beim ersten Anlauf korrekt funktioniert und nicht auf Nachzählungen angewiesen ist.

4 Lösung Open Source

4.1 Transparenz und Vertrauen

Ein Kerngedanke der Demokratie ist das Recht auf Information. Man könnte sagen, je transparenter ein Wahlprozess ist, umso demokratischer ist er. Deshalb sollten sich Bürger einer demokratisch organisierten Gesellschaft ein eigenes Urteil darüber bilden können, ob ein elektronisches Wahlsystem auch das tut was es verspricht. Werden jedoch dem Wähler systematisch Informationen zum Wahlhergang vorenthalten, so wird die Demokratie untergraben.

Open Source garantiert politische Unabhängigkeit und Neutralität. Jedes Land, jede Gemeinde oder Organisation, die Closed Source Wahlmaschinen kauft, begibt sich in eine vollkommene Abhängigkeit vom Hersteller und seinen Strategien. Die Firma könnte ihr Produkt in eine Richtung entwickeln, die den gewünschten Eigenschaften für eine demokratische Wahl zuwiderläuft oder bestimmte Anforderungen gar nicht erst ermöglicht. (Kitcat 2001)

Allein die Offenlegung des Quellcodes gewährleistet das Vertrauen der Wähler in e-Voting, da jeder Bürger den Code auf Manipulationen und Fehler persönlich überprüfen kann. Die Kontrolle der Software gehört in die Hände der wählenden Bevölkerung. Ein Gerät ohne Open Source könnte sich früher oder später als Büchse der Pandora entpuppen.

4.2 Nicht auf Kosten der Sicherheit

Viele Hersteller von Wahlsystemen verbreiten die Auffassung, daß das Verstecken von Informationen der Sicherheit dient. Das ist nicht korrekt, vielmehr führt die Geheimhaltung des Quellcodes dazu, daß viele Fehler und Schwachstellen unentdeckt bleiben, jedoch ohne daß das Programm dadurch sicherer wird.

Erst mit dem Open Source Modell ist eine ausreichende Sicherheit gegeben. Und zwar dann wenn möglichst viele Sicherheitsexperten und Programmierer aus den unterschiedlichsten Ländern und Fachrichtungen sich schon während der Entwicklungsphase persönlich davon überzeugen können, daß das elektronische Wahlsystem keine Fehler enthält. Bei der Open Source Entwicklung ist eine gute und ausführliche Dokumentation üblich, ein weiterer Faktor, der zu Sicherheit und Vertrauen führt. Nur mit dem Open Source Modell können Sicherheitslücken schnell gefunden und Angriffe auf das System frühzeitig abgewendet werden.

Enorme Kosteneinsparungen sprechen ebenfalls für ein Open Source Wahlsystem, da man frei von Lizenzkosten ist. Denn der Open Source Quellcode ist „copylefted“, das heißt er steht unter einer freien Lizenz. Es ist jedem erlaubt, den Code zu verwenden, weiterzugeben und weiterzuentwickeln solange der Quellcode offen bleibt. Open Source bringt somit auch Investitionssicherheit. Und durch die Unabhängigkeit von einzelnen Unternehmen wird der Markt der mittelständischen Betriebe durch mehr Wettbewerb belebt.

4.3 e-Voting mit Open Source ist bereits Realität

Eine Wahlsoftware auf Basis von Open Source existiert bereits. Im Oktober 2001 fanden im australischen ACT-Distrikt² elektronische Wahlen statt. Anders als die davor gescheiterten elektronischen Wahlen, setzte man auf Open Source. Es stellte sich heraus, dass Open Source die bessere Lösung war. (Baader 2001)

Obwohl das Wahlsystem von einer australischen Firma entworfen wurde, basierte es auf Spezifikationen, die von unabhängigen Wahlhelfern festgelegt wurden. Der Sourcecode wurde ins Internet gestellt und kann seitdem von jedem interessierten begutachtet und selber verwendet werden. Das System läuft auf einer kostengünstigen Standard-Hardware auf dem ebenfalls unter einer freien Lizenz stehenden Betriebssystem Linux. (Zetter 2003)

„Die einzige Plattform, die Robustheit und Vertrauen der Wähler gewährleistet, war Debian GNU/Linux, mit all seinem Quellcode, der unter der General Public License (GPL) lizenziert ist.“ (IT-News, zitiert bei Baader 2001)

Mittlerweile gibt es eine „non profit“ Organisation (Open Vote Foundation) in Californien, die das australische System eVACS³ als Grundlage genommen hat, mit dem Ziel, die optimierte Software bei amerikanischen Wahlen einzusetzen. (Zetter 2004)

Erwähnenswert ist auch das „Open Voting Consortium“, eine nicht profitorientierte Organisation, die zur Zeit die Entwicklung einer offenen Wahlsoftware koordiniert.

²Australian Capital Territory

³Electronic Voting and Counting System

5 Empfehlung

Alle Fakten zusammen betrachtet, stellt die Überführung in die elektronische Form einen großen Fortschritt für die Durchführung von Wahlen dar. Jedoch müssen wir warnen vor überstürzter Euphorie. Angesichts der existierenden Sicherheitsprobleme muß viel Energie aufgewendet werden, um bis 2009 eine funktionierende und vor allem sichere Infrastruktur aufzubauen. Vor allem müssen zunächst verbindliche Standards festgelegt werden, die die Sicherheit gewährleisten und vor Manipulationen schützen.

Keines der existierenden, kommerziellen Systeme kann als vertrauenswürdig gelten. Im Gegenteil, es bietet sich ein Bild klaffender Sicherheitslücken und die praktizierte Geheimhaltung der Wahlsoftware ist nicht akzeptabel. Ein Wahlsystem, bei der lückenlose Transparenz nicht gegeben ist, bringt demokratische Werte in Gefahr. Ein Wähler, der nicht darauf vertrauen kann, dass seine Stimme richtig gezählt wird, ist morgen schon kein Wähler mehr.

Open Source Wahlsysteme sind die einzige Möglichkeit, um diesen Bruch in der Transparenz gar nicht erst entstehen zu lassen und den Grundstein für das Vertrauen des Wählers in elektronische Wahlen zu legen. Unsere Empfehlung kann daher nur „Open Source“ lauten.

6 Informationen

Unter folgenden Internet-Adressen finden Sie weiterführende Informationen:

- <http://www.eff.org/Activism/E-voting>
Die Electronic Frontier Foundation gibt allgemeine Informationen zur Problematik des e-Voting.
- <http://www.blackboxvoting.com>
Black Box Voting untersucht die Manipulationsmöglichkeiten von elektronischen Wahlurnen, dazu gibt es auch ein Buch.
- <http://www.open-vote.org>
Die Open Vote Foundation widmet sich der Entwicklung und Implementierung von offenen, sicheren Standards für elektronische Wahlmaschinen.
- <http://www.openvotingconsortium.org>
Das Open Voting Consortium entwickelt eine offene Software für elektronische Wahlen.
- <http://www.verifiedvoting.org>
Verified Voting setzt sich für transparente, zuverlässige und durch die Öffentlichkeit verifizierbare Wahlen in den USA ein.

Literatur

- Baader, Hans Joachim. 2001. "Debian in Wahlsoftware." *Pro-Linux* .
URL: <http://www.pro-linux.de/news/2001/3302.html>
- Bolstad, Erika. 2004. "New system no easy touch for 134 voters in Broward." *The Miami Herald* .
URL: <http://www.miami.com/mld/miamiherald/news/politics/7660910.htm>
- Damon, Anjeanette. 2003. "Experts voice doubts about voting machines." *RENO GAZETTE-JOURNAL* .
URL: <http://www.rgj.com/news/stories/html/2003/12/02/58202.php>
- Gerck, Ed, C. Andrew Neff, Ronald L. Rivest, Aviel D. Rubin & Moti Yung. 2002. The Business of Electronic Voting. In *FC 2001, LNCS 2339*, ed. P. Syverson. Springer pp. 243–268.
- Jonietz, Erika. 2004. "Valid Voting?" *Technology Review* pp. 74–75.
- Kitcat, Jason. 2001. "Why Electronic Voting Software Should Be Free Software.".
URL: <http://www.free-project.org/writings/wfs.html>
- Krüger, Alfred. 2004. "Wählen ist wie Online-Shopping." *Telepolis* .
URL: <http://www.heise.de/tp/deutsch/inhalt/te/16615/1.html>
- Krugman, Paul. 2004. "Democracy at Risk." *New York Times* .
- Rötzer, Florian. 2003. "US-Wahlcomputer mit vielen Manipulationsmöglichkeiten." *Telepolis* .
URL: <http://www.heise.de/tp/deutsch/inhalt/te/15301/1.html>
- Stone, Adam. 2003. "E-Voting: Should We Pull the Lever?" *IEEE Software* .
- Wikipedia. N.d.a. Demokratie.
URL: <http://de.wikipedia.org/wiki/Demokratie>
- Wikipedia. N.d.b. Europäisches Parlament.
URL: http://de.wikipedia.org/wiki/Europ%EAisches_Parlament
- Zetter, Kim. 2003. "Aussies Do It Right: E-Voting." *Wired News* .
URL: <http://www.wired.com/news/ebiz/0,1272,61045,00.html>
- Zetter, Kim. 2004. "Open-Source E-Voting Heads West." *Wired News* .
URL: <http://www.wired.com/news/evote/0,2645,61968,00.html>