

Pro und Contra elektronischer Wahlsysteme

1. Wahlbeteiligung:

- + Steigende Wahlbeteiligung bei Jungwählern durch Internetbegeisterung und durch Bequemlichkeit auch bei anderen Wählergruppen
- Hat sich bei bisherigen Internetwahlen nicht bestätigt, Briefwahl ähnlich bequem

2. Kostensenkung:

- + langfristig
- hohe Anfangsinvestition (ca 100€pro Wahlberechtigten)

3. Effizienz:

- + schnellere Stimmauszählung und Vermeidung von Zählfehlern
- Sicherheit und Korrektheit der Technik

Sonstige Nachteile:

- Wahlprüfung nur mit **Spezialwissen** und nur bei **Open Source** Software
- **Unsicherheit** des Internet (Denial of Service Attacken, Viren etc.)
- Unsicherheit von derzeitiger Hard und Software der Endgeräte
Daraus folgend **Vertrauensverlust** bei Bevölkerung
- Fragwürdige Verbindung von Wahlwerbung und Wahlort (§32 BWG)
- Sichere **Wählerauthentifizierung** bei gleichzeitiger **Anonymität** seiner Stimme

Sonstige Vorteile:

- + **Prestigegewinn** durch erste großflächige Elektronische Wahl
- + **Keine ungültigen Stimmen**
- + **Postlaufzeit** der Briefwahl entfällt
- + **Weniger Wahlbetrug** in „gefährdeten“ Ländern
- + Blinde könnten ohne Hilfspersonen wählen

Technische Universität Berlin
Informatik und Gesellschaft



Gutachten

**zur Benutzung elektronischer Wahlsysteme
für die Europaparlamentswahl 2009
unter Verwendung von Open Source Software**

erstellt von: Ulviye Tandogan
Lars Schröder
René Schmutzler

Elektronische Wahlsysteme:

Wir wollen unter diesem Begriff sowohl die Benutzung des Heim PC zur Stimmabgabe als auch die Verwendung von Wahlmaschinen im Wahllokal verstehen.

Unter der Zielsetzung der Erhöhung der Wahlbeteiligung werden wir uns hauptsächlich mit der Internet - Wahl von zu Hause beschäftigen und nur an einigen Stellen auf Wahlmaschinen wie sie heute schon in den USA benutzt werden eingehen.

Anforderungen an Wahlsysteme:

Das EuWG fordert in §1 dass die Wahl **allgemein, unmittelbar, frei, gleich** und **geheim** sein muss und die Rechtsprechung fordert eine Gleichgewichtung aller fünf Eigenschaften.

Wir werden jetzt die Probleme aufführen, die die Übertragung auf elektronische Wahlverfahren mit sich bringt:

Um den Grundsatz der **Allgemeinheit** zu wahren muss ein elektronisches Wahlverfahren ausfallsicher sein, was PC und Internet basierende Systeme nicht bisher nicht sind.

Die Gewährleistung der **Unmittelbarkeit** ist bei Closed Source Systemen unmöglich, da hier die Überprüfbarkeit für den Wähler ausgeschlossen ist. Selbst bei Verwendung von Open Source Systemen ist die geforderte **leichte** Überprüfbarkeit für den Wähler nicht gewährleistet.

Die **Freiheit** der Wahl ist höchstens in Bezug auf das Verbot von Wahlwerbung am Wahlort eingeschränkt, denn diese Werbung ist nur durch einen Mausklick von der Wahlseite entfernt. Gegenüber der Briefwahl besteht kein Unterschied bezüglich eventuellem privaten Druck.

Um die **Gleichheit** zu gewährleisten, muss sichergestellt werden, dass jeder Wähler nur eine Stimme abgeben kann und dies muss auch überprüfbar sein was wieder die Problematik der Unmittelbarkeit aufwirft. Des Weiteren müssen für alle Wähler die gleichen Bedingungen gelten, was schon bei der digitalen Darstellung des Wahlzettels mit unterschiedlichen Bildschirmauflösungen sehr schwierig umzusetzen ist.

Das **Geheimnisprinzip** ist ähnlich gefährdet wie bei der Briefwahl, da der Wähler seine Stimme nicht in einer Wahlkabine abgibt. Eine Weitere Schwierigkeit besteht darin, zu verhindern, dass der Stimmzettel auf den Wähler zurückverfolgt werden kann.

Ziele und Vorteile elektronischer Wahlsysteme:

Die Wahlbeteiligung ist in den letzten Jahren stetig gesunken. Durch die Verwendung von Internetwahlen erhofft man sich diesen Trend umzukehren. Denn insbesondere Erst- und Jungwähler fühlen sich vom Internet angezogen und würden aufgrund der „Nähe zur Wahl“ so auch eher daran teilnehmen.

Durch die Reduzierung der Briefwähler lassen sich die Kosten stark senken. Außerdem braucht man bei der Benutzung von Wahlmaschinen weniger ehrenamtliche Wahlhelfer. Auch das digital geführte Wählerverzeichnis spart Kosten.

Die Maschinelle Auszählung der Stimmen geht wesentlich schneller, als das von Hand möglich wäre. Außerdem sind bei einer korrekten Implementierung Zählfehler ausgeschlossen. Menschliche Fehler werden auf ein Minimum reduziert.

Es wird keine ungültigen elektronischen Stimmzettel geben, da der Wähler durch automatische Kontrolle daran gehindert wird einen solchen abzusenden.

Der Wahlbetrug in dafür gefährdeten Ländern lässt sich bei geeigneten Wahlsystemen, die für jedermann offen sind, eindämmen.

Für Behinderte bietet die Wahl über das Internet eine Erweiterung der Teilnahme an der Demokratie, so können zum Beispiel Blinde ohne Hilfsperson ihre Stimme abgeben.

Auch für kurzfristig Erkrankte ist es eine einfache Möglichkeit doch noch an der Wahl teilzunehmen, denn Briefwahlen haben den Nachteil der langen Postlaufzeit.

Zuletzt bleiben noch der Prestigegewinn, den ein flächendeckend eingesetztes und stabil funktionierendes Wahlsystem mit sich bringt und die damit verbundenen Verkaufschancen.

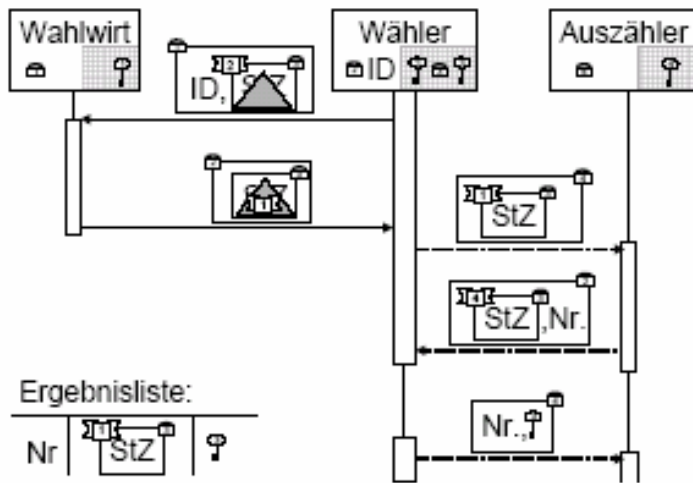
Nachteile und Risiken elektronischer Wahlsysteme:

Bisherige Experimente mit Internetwahlen haben keine merklichen Steigerungen der Wahlbeteiligung gezeigt. So stieg die Beteiligung bei der Studentschaftswahl an der Uni Wien von ca. 26% auf ca. 36% wobei jedoch ein Gewinnspiel an die Wahl angeschlossen war[Led 2003]. Außerdem sind viele elektronische Wahlen bisher unter Jugendlichen durchgeführt worden, die tendenziell eine geringere Hemmschwelle gegenüber modernen Techniken haben. Sollten Internetwahlen das Ziel haben die Briefwahl abzulösen, wären viele ältere Menschen, die sich nicht mehr mit modernen Techniken beschäftigen wollen oder auch können, von der Teilnahme an der Demokratie ausgeschlossen. Da wir jedoch einer Verschiebung der Alterspyramide von jung nach alt [destatis 2001] unterliegen, kann es nur der falsche Weg sein, die Älteren von der Demokratie auszuschließen.

Um die Sicherheit der Internetwahlen zu gewährleisten sind Maßnahmen, wie die Erstellung von Signaturkarten und das Bereitstellen von Lesegeräten notwendig. Diese verursachen naturgemäß sehr hohe Investitionskosten die sich erst bei vielfach wiederholter Benutzung rentieren[Phil 2001].

Zwar lässt sich durch die elektronische Verwaltung der Wahldaten, der Mensch als Fehlerquelle fast vollständig ausschalten, doch jeder, der schon einmal mit einem PC gearbeitet hat, weiß, wie unzuverlässig diese sein können.

Um die Problematik der Einhaltung der Wahlrechtsgrundsätze zu illustrieren, werden wir kurz ein recht komplexes elektronisches Wahlsystem, wie es Prof. Dr. Phillipsen vorstellt, einführen. Einfachere Systeme haben noch gravierendere Probleme und werden von uns daher nicht weiter behandelt.



Quelle: Michael Phillipsen 2001 FZI Karlsruhe – Internetwahlen: Demokratische Wahlen über das Internet S.6

Bei diesem Verfahren kommen mehrere Paare von Öffentlichen und privaten Schlüsseln zum Einsatz. Der Wähler verschickt seinen verschlüsselten Stimmzettel und ein Identifikationsmerkmal an einen Wahlwirt (eine Art Wahllokal). Das gesamte Paket wird noch einmal mit dem Öffentlichen Schlüssel des Wahlwirtes verschlüsselt, so dass dieser es mit seinem privaten Schlüssel öffnen kann. Wenn der Wähler wahlberechtigt ist, dann signiert der Wahlwirt dessen Stimmzettel mit einer Blindsignatur, wozu er den Stimmzettel nicht zu öffnen braucht, und sendet das Paket zurück an den Wähler. Dieser kann Manipulation feststellen, da der Stimmzettel noch immer mit seinem privaten Schlüssel verschlüsselt sein muss. Jetzt wird der Stimmzettel über einen anonymisierten Kanal, der keine Rückverflung erlaubt, an den Auszähler gesendet. Dieser sendet eine Kopie zusammen mit einer fortlaufenden Nummer über den Rückkanal an den Wähler.

Damit der Stimmzettel vom Auszähler gelesen werden kann, ist es notwendig, dass der Wähler seinen privaten Schlüssel zur Verfügung stellt. Und damit fangen die Probleme an:

Wird nämlich der Schlüssel vor dem Ende der Wahl übermittelt, so kann der Auszähler das Wahlgeheimnis verletzen oder die Wahl sogar manipulieren. Aber welcher Wähler möchte schon bis zum Ende der Wahl warten, um sich dann noch einmal ins Internet zu begeben damit er dann seinen Schlüssel übermitteln kann. Wenn das auch noch Millionen weitere Wähler zeitgleich tun, dann wird auch der modernste Wahlserver seinen Dienst verweigern. Unterlassen das dann auch noch einige Wähler ganz, verzögert sich die Ergebnisbestimmung erheblich. Also muss die Auszählsoftware Open Source sein, um zu gewährleisten, dass der Auszähler seine theoretische Manipulationsmöglichkeit nicht ausnutzen kann.

Ein weiteres Problem ist die Quittung, die beim Wähler verbleibt und mit der dieser seine Wahlentscheidung beweisen kann, was eindeutig dem Grundsatz der geheimen Wahl widerspricht, es sind bisher auch noch keine annähernd sicheren Wahlverfahren bekannt, die Quittungsfreiheit garantieren.

Die 5 Nachrichten, die zwischen allen Beteiligten versandt werden bieten eine große Angriffsfläche auf die wir im Folgenden genauer eingehen werden.

Da alle Wahlsysteme, die eine breite Öffentlichkeit erreichen sollen, PC und Internet -basiert sein sollten, ergeben sich eine große Anzahl fundamentaler Sicherheitsprobleme die wir anhand eines Prüfberichts der Security Peer Review Group [SPRG 2004] vom Januar diesen Jahres aufzeigen werden. Diese Gruppe von Wissenschaftlern ist vom US-Verteidigungsministerium beauftragt worden das SERVE Projekt zu untersuchen, welches Internetwahlen für US-Bürger im Ausland über das Internet ermöglichen soll und ebenfalls vom Verteidigungsministerium in Auftrag gegeben wurde. Die Gruppe kam zu einem vernichtenden Urteil, was dazu führte, dass das Pentagon am vergangenen Freitag die Benutzung für die Präsidentschaftswahl 2004 ausschloss[AFIS 2004].

1. Insider Angriffe

Bei geschlossener Software wäre es für die Entwickler möglich, bestimmte Hintertüren einzubauen, die dann zu Sabotage oder Manipulation genutzt werden können. Open Source ließe dieses Risiko gegen Null gehen, da dieses Projekt sicherlich sehr viele Programmierergruppen auf den Plan rufen würde und so solche Art Fehler mit höchster Wahrscheinlichkeit gefunden werden.

2. Denial of Service (DoS) Angriffe

sind Angriffe, bei denen von vielen Rechnern aus gleichzeitig anfragen an einen Server gesendet werden, worauf dieser seinen Dienst verweigert. Sie lassen sich über so genannte Mailwürmer, wie zuletzt MyDoom, gezielt vorbereiten aber was noch viel schwerwiegender ist sie können auch in beliebter Free und Shareware versteckt werden, die häufige Updatezyklen haben.

3. Viren

könnten zum Beispiel gezielt am Wahltag die Rechner von Millionen Wählern außer Gefecht setzen

Weitere Gefahren gehen von installierter Standardsoftware aus, die gezielt in den Wahlablauf eingreifen könnte um so einen Kandidaten oder eine Partei zu unterstützen. Hier ließe sich durch ein spezielles offenes Mini – Betriebssystem auf Basis von Linux Abhilfe schaffen. Dieses dürfte bis auf die benötigten Treiber und die Wahlsoftware keine weiteren Komponenten enthalten.

Wenn wir nun noch einmal einen Blick in Richtung USA werfen, dann sehen wir auch in der New York Times vom 23.01.2004 einen Artikel von Paul Krugmann [Krug 2004] der elektronische Wahlen als Risiko für die Demokratie sieht. Er führt an, das bereits bei mehreren Wahlen Fehler aufgetreten sind, dass zum Beispiel Wahlmaschinen ausfielen und bereits abgegebene Stimmen verloren gingen.

Weiterhin verweist Krugmann auf einen Gesetzentwurf des Republikaners Rush Holt vom Mai 2003 [Holt 2003] Der einige Minimalforderungen an Elektronische Wahlsysteme stellt. So fordert er zusätzliche Papieraufzeichnungen, die eine Überprüfung gewährleisten, keine geschlossene Software, rechtzeitige Fertigstellung der Software, Zugangsmöglichkeiten für behinderte und Stichprobenartige Zufallskontrollen.

Diesem Entwurf ist selbst aus Sicht des eher demokratisch eingestellten Krugmann nichts hinzuzufügen

Abschließend können wir nur zu der Empfehlung gelangen zum gegenwärtigen Zeitpunkt auf Elektronische Wahlsysteme ganz zu verzichten. Aber jegliche weitere Bemühungen sollten in Richtung von Open Source gehen um das Vertrauen der Bevölkerung in diesen so wichtigen Bestandteil der Demokratie nicht zu gefährden. Denn noch immer klingen die Gerüchte nicht ab, George W. Bush habe die Wahl gegen Al Gore nicht gewonnen, denn auch bei dieser Wahl kamen elektronische Wahlsysteme zum Einsatz.

[Led 2003] Lederer, Andreas 18.08.2003 E-Voting Premiere in Österreich URL: <http://www.politik-digital.de/edemocracy/evoting/oesterreich.shtml> -zuletzt gesehen: 02.02.2004

[Phil 2001] Phillipsen, Michael 08.10.2001: Internetwahlen: Demokratische Wahlen über das Internet?
Karlsruhe Forschungszentrum Informatik (FZI)

[destatis 2001] Statistisches Bundesamt 2001: Alterspyramiden URL:
<http://www.destatis.de/basis/d/bevoe/bevoegra2.htm> – zuletzt gesehen: 02.02.2004

[SPRG 2004] Security Peer Review Group 21.01.2004: A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE) URL : <http://www.servesecurityreport.org/paper.pdf> - zuletzt gesehen: 03.02.2004

[AFIS 2004] American Forces Information Service 06.02.2004: Pentagon Decides Against Internet Voting This Year URL: http://www.pentagon.gov/news/Feb2004/n02062004_200402063.html - zuletzt gesehen: 08.02.2004

[Krug 2004] Krugman, Paul: Democracy at Risk: in der New York Times vom 23.01.2004 S.23

[Holt 2003] Holt, Rush: ON ELECTION DAY 2004, Voter Confidence and Increased Accessibility Act of 2003 22.03.2003 URL: <http://thomas.loc.gov/cgi-bin/query/D?c108;1:./temp/~c108Y9jMH0::> zuletzt gesehen: 08.02.2004