E-Voting – kritische Erfolgsfaktoren

Alexander Prosser

Abteilung Produktionsmanagement, Wirtschaftsuniversität Wien
A-1090 Wien, Augasse 2-6
alexander.prosser@wu-wien.ac.at

Schlagworte: E-Voting, e-Democracy, Wahlen

Abstract: Ausgehend von ausgewählten, für e-Voting relevanten Wahlrechtsgrundsätzen versucht der Beitrag kritische Erfolgsfaktoren für e-Voting-Systeme herauszuarbeiten. Er greift dabei auf die in den folgenden Beiträgen dargestellten Zustandsberichte zum Thema aus Deutschland, Österreich und der Schweiz zurück, wobei das Internationale Rechtsinformatiksymposion (IRIS) 2003 die Möglichkeit bot, die Voraussetzungen, den gegenwärtigen Stand der Diskussion und das Umfeld für Implementierungen in diesen drei Ländern unmittelbar zu vergleichen.

1. E-Democracy

Zahlreiche Applikationen nutzen das Internet für die Abwicklung von Geschäfts- und administrativen Transaktionen, sei es im privaten oder im öffentlichen Sektor (e-Government). Es stellt sich die Frage, wie das Internet auch für die Unterstützung demokratischer Entscheidungsprozesse (also „e-Democracy") eingesetzt werden kann. Dies hat neben rein technischen vor allem rechtliche und soziologische Aspekte.

Zum einen beeinflussen diese das Design bzw. überhaupt die Machbarkeit eines technischen Systems. Andererseits ist ein Informationssystem mehr als nur die „Elektrifizierung" eines bestehenden Prozesses. Das Informationssystem verändert den Prozess, so wie dies auch bei Geschäftsprozessen im privaten Sektor der Fall ist.[1]

Abbildung 1 versucht eine Kategorisierung von e-Democracy-Systemen nach dem Maß an Beteiligung des Bürgers und der technischen Komplexität des entsprechenden Systems.

---

[1] Vgl. dazu *Malone, Thomas W.; Yates, JoAnn; Benjamin, Robert I.:* Electronic Markets and Electronic Hierarchies. In: Communications of the ACM 30 (1987) 6, S. 484–497.

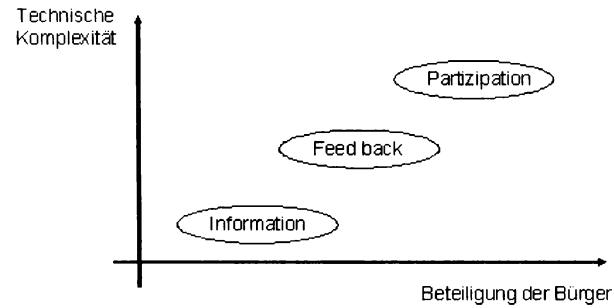

Abbildung 1: e-Democracy Systeme

Systeme zur reinen Information des Bürgers bzw. zum Feedback des Bürgers an den Mandatar sind technisch relativ einfach in der Realisierung; so können beispielsweise virtuelle Sprechtage oder virtuelle politische Diskussionen mit vorhandenen Technologien rasch realisiert werden. Dennoch sind sie als Basis für eine informierte Entscheidung des Bürgers nicht zu unterschätzen. Noch relativ wenig Erfahrung besteht hingegen mit Formen der elektronischen Stimmabgabe, sei es elektronischen Unterschriftenlisten oder der anonymen elektronischen Stimmabgabe (e-Voting). Vor allem beim e-Voting kommen zur Diskussion von Gestaltung und Wirkungsanalyse auch grundsätzliche Fragen der technischen Machbarkeit eines Systems an sich. Im folgenden Abschnitt wird e-Voting in Bezug auf ausgewählte Wahlgrundsätze untersucht, wobei versucht wird, kritische Erfolgsfaktoren für e-Voting herauszuarbeiten.

2. Wahlrechtsgrundsätze und e-Voting

Jedes e-Voting-System muss – unabhängig vom gewählten technischen Verfahren – zwei Funktionsblöcke abbilden: (i) die *Identifizierung/elektronische Anmeldung* des Wahlberechtigten zum e-Voting sowie (ii) den anonymen Akt der *Stimmabgabe* selbst. Diese Schritte können in einem (einstufiges Verfahren) oder zeitlich getrennt sein (zweistufig); in letzterem Fall registriert sich der Wahlberechtigte und erhält eine elektronische „Briefwahlkarte", die zur Stimmabgabe verwendet wird.[2]

---

[2] Für eine Einführung vgl. *Prosser, A., Müller-Török, R.:* E-Democracy – eine neue Qualität im demokratischen Entscheidungsprozess; Wirtschaftsinformatik 44 (2002) 6, S. 545-556, *Philippsen, Michael:* Internetwahlen – Demokratische Wahlen über das Internet? In: Informatik Spektrum 25 (2002) 2, S. 138–150.

2.1. Gleiche Wahl

Es muss verhindert werden, dass Stimmberechtigte mehrfach oder für andere Bürger ihre Stimme abgeben. Dies setzt die Identifizierung und Authentisierung des Wählenden voraus. Grundlage dafür ist eine elektronische Wählerevidenz. Erfolgt die Anmeldung vor der Wahl muss der/die Betreffende aus dem Wählerverzeichnis für konventionelle Wahlen entfernt werden, wobei diese Verzeichnisse dann durchaus papierbasiert weitergeführt werden können; erfolgt dies in einem Schritt mit der Stimmabgabe, so müssen alle Formen der Stimmabgabe auf ein zentrales elektronisch geführtes Verzeichnis zugreifen können.

Zur Identifizierung können Transaktionscodes (TAN) oder digitale Signaturkarten verwendet werden. Die Schweizer Initiative verwendet hiezu TAN, die zusammen mit Briefwahlunterlagen dem Wahlberechtigten per Post zugesandt werden.[3] In Österreich wurde e-Voting bisher in zwei Wahlordnungen gesetzlich geregelt[4]; beide sehen die Verwendung der Bürgerkarte vor, wobei diese eine digitale Signaturkarte ist, die zusätzlich den Eintrag der Bürger im Zentralen Melderegister und das digitale Zertifikat (also reale und digitale Identität des Bürgers) untrennbar miteinander verknüpft. Die Bürgerkarte ist daher nicht nur ein Mittel der Authentisierung, sondern auch der Identifizierung. Voraussetzung hiefür ist die Existenz eines entsprechenden Melderegisters, in dem aus den aktuellen Adressdaten auch automatisiert der Wahlkreis ableitbar ist.

Besonders relevant ist der Schutz gegen den Ausfall des elektronischen Wahlsystems am Wahltag. Handelt es sich um ein TAN-basiertes System und sind die Wahllokale miteinander vernetzt, so ist leicht feststellbar, ob der entsprechende TAN bereits eingesetzt wurde oder nicht. Bei kryptographischen Verfahren ist dies hingegen nicht ohne weiteres möglich. Wird beispielsweise eine blinde Signatur[5] für die Authentisierung der elektronischen Wahlkarte verwendet, so sieht die Stelle, die die blind signierte Wahlkarte ausgibt, diese niemals. Eine Prüfung, ob die Wahlkarte authentisch ist, kann aber mithilfe eines im Wahllokal aufgestellten PC erfolgen, wobei eine Kontrolle gegen Doppelverwendung aber wieder die Vernetzung der Wahllokale voraussetzt. Es wären aber auch elektronische Wahlkabinen denkbar, in denen e-Voter ihre Stimme ohne Identifizierung abgeben können, falls ihr eigenes System, ihr Provider oder die zentralen Server ausfallen.

---

[3] Siehe den Beitrag von *Braun* in diesem Sammelband.

[4] Siehe den Beitrag von *Heindl* sowie von *Krimmer* in diesem Sammelband.

[5] Für eine Einführung vgl. *Chaum, David:* Blind Signatures for Untraceable Payments. In: *Chaum, David; Rivest, Ron L.; Sherman, Alan T.* (Hrsg.): Advances in Cryptology, Proceedings of Crypto 82. S. 199–203.

2.2. Geheime Wahl

Diesen Anforderungen diametral entgegengesetzt ist die Forderung nach Sicherung der Anonymität in der Stimmabgabe. Ansatzpunkte können dabei die Server der Wahladministration, die Datenübertragung und der Arbeitsplatzrechner des Wählenden sein; mögliche Angreifer sind Dritte und die Serveradministration.

Der Schutz gegen Angriffe Dritter in der Datenübertragung und der Speicherung auf den Wahlservern kann durch Standardmaßnahmen sichergestellt werden.[6] Der PC des Wählenden hingegen ist oft ein weitgehend offenes und ungeschütztes System und kann daher für Angriffe entweder auf die Anonymität oder für Manipulationsversuche verwendet werden. Zwei effektive Möglichkeiten der Abwehr wurden bisher vorgeschlagen: (i) die Auslieferung einer bootfähigen „Wahl-CD", die den Start eines vollkommen sauberen Betriebssystems sicherstellen soll oder (ii) die Verwendung von digitalen Signaturkarten für den Ablauf kryptographischer Protokolle. Erstere Variante stellt enorme logistische Anforderungen: die CDs müssen erzeugt und verteilt werden, außerdem müssen sie mit den unterschiedlichsten Hardwarevoraussetzungen kompatibel sein. Schließlich sollte der Benutzer ein ihm bekanntes Betriebssystem zum Wahlakt zur Verfügung gestellt bekommen. Diese Schwierigkeiten führen vielfach zur Behauptung, dass der PC des Wählenden grundsätzlich als unsicher zu betrachten ist und e-Voting daher nicht möglich sei.[7]

Wenn dies aber tatsächlich der Fall wäre, dürfte der PC auch nicht für digitale Signaturen verwendet werden. Im Falle der digitalen Signatur wird die Signaturkarte mit einer sicheren Leseapplikation ausgeliefert, die dem Unterschreibenden nichtmanipulierbar anzeigt, was zur Unterschrift freigegeben werden soll. Dies wird dann durch einen sicheren Tunnel an die Karte zur Signatur weitergegeben. Ein analoge Lösung ist für e-Voting möglich: die entscheidenden Teile des kryptographischen Protokolls laufen in der Karte, wobei der Antrag für die elektronische Stimmabgabe, Stimmzettel etc. in einer sicheren Leseapplikation angezeigt werden. Natürlich setzt dies auch voraus, dass das Betriebssystem der Karte über sämtliche für das entsprechende kryptographische Protokoll notwendigen Befehle verfügt.

---

[6] Für eine Einführung vgl. etwa *Feghhi, J.; Feghhi, J.; Williams, P.:* Digital Certificates – Applied Internet Security. Addison-Wesley, Reading 1999.

Tilborg van, Henk C. A.: Fundamentals of Cryptology. Kluwers Academic Publishers, Boston 2000.

[7] Internet Policy Institute: Report on the National Workshop on Internet Voting, Issues and Research Agenda. The Internet Policy Institute, Washington (DC), 2001. http://www.internetpolicy.org/research/e_voting_report.pdf, Abruf am 2001-11-20.

Die Signaturkarte ist jedoch auch ideales Trägermedium einer elektronischen Wahlkarte, falls Identifikations-/Anmeldephase und Stimmabgabe zeitlich getrennt werden. Um aber als Trägermedium dienen zu können, müssen einige Voraussetzungen erfüllt sein:

(i) die elektronische Wahlkarte muss mit einem Standard-Kartenlesegerät auf der Karte in einem PIN-gesicherten Bereich speicherbar sein. Dies kann gelöst werden, indem bereits bei der Ausgabe derartige Bereiche im Filesystem der Karte angelegt und mit PIN-Sicherung versehen werden. Die PIN-Sicherung schützt gegen unbefugtes Auslesen der Wahlkarte bei Verwendung der Karte mit Applikationen Dritter.

(ii) Im Akt der Stimmabgabe wird die Wahlkarte von der Signaturkarte gelesen; dabei muss die Anonymität gewahrt bleiben, was bedeutet, dass keine die Person identifizierenden Daten auf der Karte ungeschützt gespeichert sein dürfen.

Letzteres ist dabei die entscheidende Einschränkung. Digitales Zertifikat oder Personenbindung liegen regelmäßig frei auslesbar auf den Karten; eine PIN-Sicherung ist nicht vorgesehen. Dies zeigt, dass die heutigen Signaturkarten für ein vollkommen anderes Paradigma entwickelt wurden; eine legitime anonyme Verwendung der Karte war offensichtlich nicht vorgesehen. Dennoch gibt das notwendige periodische Redesign der einschlägigen Karten die Möglichkeit, eine solche PIN-Sicherung in Zukunft vorzusehen.

Nicht nur Dritte, auch die Serveradministration der elektronischen „Urnen" kann die Anonymität unterlaufen. Da die Stimmabgabe selbst anonym ist, kann dies nur durch Kollusion mit der Administration der Registrationsstelle erfolgen. Diese Kollusion muss entweder organisatorisch oder technisch verhindert werden.

2.3. Persönliche Wahl

Dieser Grundsatz kann im Wahllokal gesichert werden, bereits bei der Briefwahl jedoch nicht mehr. Die anderen Beiträge in diesem Band sind sich weitgehend einig, dass e-Voting in diesem Punkt analog zur Briefwahl gesehen werden kann. Sieht also eine Wahlordnung diese vor, so ist dies wohl ein wichtiger „Enabler" für e-Voting.

2.4. Nachvollziehbarkeit und Nichtmanipulierbarkeit

Im Unterschied zum papierbasierten sind im elektronischen System grundsätzlich Manipulationen denkbar, in denen einige wenige Personen das gesamte Wahlergebnis verändern können. Für Manipulationen bieten sich dieselben Ansatzpunkte wie für den Bruch der Anonymität (Abschnitt

2.2), wobei hier die Serveradministration der elektronischen Urnen in einer besonderen Situation ist.

Ansätze zur Sicherung in diesem Bereich umfassen: (i) die Verknüpfung der Stimme mit einem Berechtigungstoken, das nicht von der Wahladministration erzeugt wurde und das diese auch nicht kennt, (ii) die Vercodierung der Stimme durch Kryptoschlüssel der Wahlbeobachter, wobei die Stimme beim Wähler mit den öffentlichen Teilen verschlüsselt wird und erst nach Ende der Wahl und Sicherung der Ergebnistabellen von den Wahlbeobachtern mit ihrem geheimen Schlüssel geöffnet werden kann. Besonders gut ließe sich dieses Verfahren mit Chipkarten kombinieren, die als Schlüsselträgermedien verwendet werden können.

3. Ausblick

E-Voting wird nur dann implementiert werden, wenn die technischen Probleme glaubhaft gelöst wurden. Dabei darf keineswegs eine erhoffte Steigerung der Wahlbeteiligung (die übrigens in allen anderen Beiträgen zumindest hinterfragt wird) dazu führen, dass Systeme zum Einsatz kommen, die die Einhaltung der Wahlrechtsgrundsätze nur im „Gutfall" sicherstellen können. Hier ist die Informatik als Wissenschaftsdisziplin gefordert, Lösungen anzubieten, die die Einhaltung der Wahlgrundsätze auch unter schwierigen Bedingungen garantieren können und gegen Angriffs- und Manipulationsversuche entsprechend robust sind. In jedem Fall ist angesichts der Kritikalität der Anwendung und der Komplexität der technischen Materie ein stufenweises Vorgehen angebracht, wie es in dem in diesem Band veröffentlichten Beitrag von *Karger* und *Rüß* klar dargestellt wird.