Internet-Wahlen

Dr. Guido Schryen, M.O.R.
Lehrstuhl für Wirtschaftsinformatik und Operations Research
der Rheinisch-Westfälischen Technischen Hochschule Aachen

Zusammenfassung: Im Rahmen des E-Governments werden zunehmend Internetwahlen diskutiert. Der Beitrag diskutiert zunächst die Vor- und Nachteile derartiger Wahlen und zeigt Anwendungsgebiete sowie durchgeführte Pilotprojekte im politischen wie auch wirtschaftlichen Bereich auf. Im Rahmen eines Anforderungssystems werden anschließend aus demokratischen Wahlgrundsätzen sicherheitstechnologische Anforderungen herausgearbeitet. Zu deren Adressierung werden kryptographischen Wahlkonzepte herangezogen, von denen die wichtigsten vorgestellt werden. Aufgrund der Komplexität der Anforderungslandschaft wird ein sicherheitstechnologisches Strukturmodell vorgestellt, das insbesondere dazu dient, die Sicherheit(skomponenten) eines Wahlsystems systematisch mit den Anforderungen abzugleichen. Der Artikel schließt mit einem Ausblick auf notwendige Untersuchungen.

Schlüsselworte:Internet-Wahlen, E-Democracy, Sicherheit, Kryptographie

1 Einleitung

Die Durchführung geschäftlicher Transaktionen auf der technologischen Basis des Internets ist weit verbreitet und es wird von einer gewissen Etablierung des Electronic Business gesprochen. Vergleichsweise jung sind Aktivitäten im Bereich des Electronic Government, wo öffentliche Institutionen wie Behörden, Ämter, oder Ministerien den Bürgern interaktive Kommunikationsschnittstellen über das Internet anbieten und dabei vor allem Web-Informationen, -Formulare und Email-Verkehr anbieten. Diskutiert man in diesem Kontext über die internetbasierte Unterstützung von Bürgeranliegen und -rechten, so finden sich in jüngster Zeit vermehrt Vorstellungen und Vorschläge, das Internet auch bei politischen Wahl(entscheid)en einzusetzen und dem Wähler den physischen Gang zur Wahlurne abzunehmen. Auch im deutschen Schriftgut findet man hier oftmals den Begriff „E-Democracy“.

Es ist nicht verwunderlich, dass schon im Vorfeld technologischer Überlegungen zahlreiche Vorbehalte gegen derartige Bestrebungen bestehen, ist doch mit der politischen (Bürger-)Wahl ein Teil des demokratischen Rückgrats betroffen. Im

Sog eines noch andauernden Internet-Hypes gilt es ausgewogen zu untersuchen und diskutieren, welche Möglichkeiten das Internet aufweist, Wahlen zu unterstützen, welche Risiken damit verbunden sind und ob Internet-Wahlen gesellschaftlich und politisch gewünscht sind. Es handelt sich hierbei also um einen höchst interdisziplinären Komplex, in den zumindest Verfassungs- und Wahlrechtsjuristen, Politologen und Soziologen wie auch technische Sicherheitsexperten, Kryptologen, Mathematiker und (Wirtschafts-)Informatiker zu involvieren sind.

Betrachtet man die Literatur und die praktischen Erfahrungen zu Online-Wahlen, so lässt sich feststellen, dass zum einen Bedarf in der (technologischen, polit-soziologischen und juristischen) Grundlagenforschung besteht, zum anderen großer Experimentierbedarf existiert.

Der vorliegende Beitrag widmet sich dem informationstechnologischen Sicherheitsbedarf, der im politischen Bereich schon aufgrund (verfassungs)gesetzlicher Wahlgrundsätze besteht. Dabei sollen jedoch nicht nur Online-Wahlen betrachtet werden, wie sie im politischen Rahmen von Kommunal- Landtags- oder Bundestagswahlen stattfinden können, sondern auch Wahlen im Umfeld von Hochschulen, Personalräten, Aktionärsversammlungen usw. Die Zielsetzung besteht zum einen darin, einen deskriptiven Überblick über die Landschaft von Online-Wahlen zu geben. Zum anderen wird ein informationstechnologisches, generisches Rahmenwerk vorgestellt, das die Infrastruktur bei Online-Wahlen modelliert und als Ausgangspunkt zur systematischen Überprüfung der Umsetzung von Sicherheitsanforderungen verwendet werden kann.

Es werden zunächst die wesentlichen Argumente von Befürwortern und Gegnern der Internetwahl vorgestellt, so dass sich der Leser mit seiner Einstellung bereits hier wieder finden mag. Anschließend werden Anwendungsgebiete für Online-Wahlen näher vorgestellt und diskutiert, wobei auf Pilotprojekte eingegangen wird. Es folgt eine Skizzierung (technologischer) Sicherheitsanforderungen, die sich größtenteils aus gesetzlichen Bestimmungen ableiten lassen. Nach einer kurzen Vorstellung kryptographisch-technologischer Ansätze wird das o.a. Rahmenwerk vorgestellt, bevor der Artikel mit einem Ausblick auf offene Problemfelder schließt.

2 Pro und Contra

Als wesentliche allgemeine Argumente für die Einführung von Online-Wahlen finden sich die folgenden [Phil02, S. 139f; Otte02]:

- Steigende Wahlbeteiligung
  Inwiefern dauerhaft eine signifikant höhere Wahlbeteiligung erreicht werden

kann, ist bislang empirisch nicht ausreichend untersucht, auch wenn einzelne Beteiligungszahlen an Pilotprojekten veröffentlicht wurden: Die Forschungsgruppe Internetwahlen [Otte00] an der Universität Osnabrück hat im Februar 2000 die Wahlen zum Studentenparlament online ermöglicht und dabei ca. 400 Studenten zur Teilnahme bewegt. Im Januar 2003 führte der Genfer Vorort Anières erstmals in der Schweiz eine offizielle Internet-Wahl zu einem Gemeindeprojekt durch, hier wählten ca. 28% der Wahlberechtigten online [Genf03]. Bei Vorpräsidentschaftswahlen der US-Demokraten im Jahr 2000 nutzten fast 40.000 Wahlberechtigte die Möglichkeit zur Online-Wahl [Elec00][1]. Diese Zahlen allein sind insofern schwierig interpretierbar, da (1) unklar ist, wie viele der Online-Wähler auch sonst gewählt hätten, und (2) diese Zahlen um temporäre Effekte aufgrund von Werbung und Medieninteresse zu bereinigen sind.
Der Einfluss einer Online-Wahl auf eine Wahlbeteiligung wird vermutlich nicht nur von der Art der Wahl abhängen, sondern beispielsweise auch von den jeweiligen kulturellen, politischen und geographischen Gegebenheiten: Australiens geringe Besiedlungsdichte, Griechenlands Forderung, in seiner Geburtsgemeinde wählen zu müssen und die politische Etablierung von (unmittelbaren) Volksabstimmungen in der Schweiz sind mitentscheidende Charakteristika. Hiermit hängen auch finanzielle Einsparpotentiale zusammen.

- Kostensenkung
  Bei volkswirtschaftlicher Betrachtung können Kosteneinsparungen auftreten, wenn weniger Personal für die Verwaltung von Briefwahlunterlagen und die Auszählung von Stimmen erforderlich ist oder wenn geringere Reiseaktivitäten anfallen. Dem gegenüber stehen Kosten für die Bereitstellung und den Betrieb einer Wahlinfrastruktur und die initiale Ausstattung der Wähler mit erforderlicher Hardware (s. Abschnitt 4). Im politischen Bereich werden auf absehbare Zeit auch keine Wahllokale obsolet. Ob und bei welchen Wahlen sich Kosteneinsparungen in welcher Zeit einstellen, ist derzeit nur spekulativ diskutierbar.

- Verringerung der Anzahl ungültiger Stimmen
  Ungültige Stimmen können bewusst oder unbewusst erzeugt werden. Bewusst ungültig abgegebene Stimmen sind denkbar als Zeichen des Wählerprotests und daher auch bei Online-Wahlen zu ermöglichen.[1] Unbewusst ungültig abgegebene Stimmen können mittels einer Plausibilitätsprüfung theoretisch bereits bei der Eingabe als solche identifiziert werden, und es kann darauf

[1] Der verfassungsrechtliche Grundsatz der Gleichheit einer Wahl verpflichtet bei deutschen politischen Wahlen in Deutschland dazu, alle Stimmzettel unabhängig von der Wahlart (Urnenwahl oder Briefwahl) einheitlich zu gestalten und einheitlich „ausfüllbar“ zu gestalten [Rüß02].

hingewiesen werden. Ob die hierdurch erfolgende Einschränkung des Gleichheitsgrundsatzes tolerierbar ist, muss juristisch geklärt werden.

- Weniger Wahlbetrug in gefährdeten Ländern
  Die Sicherheit von Wahlen begründet sich bei der traditionellen Urnenwahl auf das Vertrauen in Personen und die Unabhängigkeit von Gremien. Beispielsweise sind in Deutschland im Rahmen politischer Wahlen in einem Wahllokal stets Personen unterschiedlicher Parteien anwesend, und die Auszählung der Stimmen erfolgt von anderen Personen. In „gefährdeten" Ländern mit jungen Demokratien ist das Vertrauen in diese Mechanismen geringer, und eine Verlagerung organisatorischer Sicherheitsvorkehrungen auf technische (u.a. Verschlüsselung im Internet) kann hier helfen. Es muss an dieser Stelle jedoch betont werden, dass die koexistente Verwendung organisatorischer und technischer Sicherheitsvorkehrungen graduellen Charakter hat, d.h. die sicherste Technik kann stets ausgehebelt werden, wenn alle beteiligten Organisationseinheiten korrumpierend kooperieren.
- Unterstützung der Basisdemokratie
  Ist erst eine internetbasierte Wahlinfrastruktur etabliert, können basisdemokratische Wahlprozesse praktikabler werden.

Nicht weniger scharf werden Bedenken gegen Online-Wahlen ins Feld geführt [Phil02, S. 140f; CIVT00]

- Sicherheit
  An erster Stelle der Contra-Argumente stehen Sicherheitsbedenken. Für jedermann ist beispielsweise offensichtlich, dass bei der Urnenwahl eine Zuordnung von Wähler und seiner Wahlentscheidung nicht möglich ist, denn er trägt sein Wahlkreuz hinter einer physischen Absperrung ein, und er wirft seinen verschlossenen Umschlag selbst in die Urne, in der auch die Umschläge vieler anderer Wähler enthalten sind. Der Wähler selbst kann das Geheimhaltungsprinzip hier realisieren. Anders sieht dies bei der Briefwahl aus, die dennoch gesellschaftlich, politisch und juristisch akzeptiert ist. Dass Stimmen nicht verändert werden, kann der Wähler nicht garantieren, hier vertraut er auf die Integrität der beteiligten Personen und Organisationen sowie bei der Briefwahl auf die Wahrung des Postgeheimnisses nach §202 StGB. Diese und viele weitere Aspekte der Wahlsicherheit wie auch die Garantie des Zugangs der Stimme werden wohl auch aus Gewohnheitsgründen nicht mehr thematisiert oder implizit als realisiert wahrgenommen. Zu Recht wird im Kontext der Internetwahl die Frage nach der Sicherheit erneut gestellt. Eine US-amerikanische Studie der Internet Voting Task Force [CIVT00] äußert sich z.B. skeptisch hinsichtlich der Sicherheit auf den Internetclients, da die Existenz von Würmern, Viren und trojanischen Pferden nicht hinreichend sicher ausgeschlossen werden kann. Die facettenreiche Fragestellung der technologischen Sicherheit wird in den folgenden Abschnitten detaillierter behandelt.

Interessant in diesem Zusammenhang ist, dass die Briefwahl – die Internetwahl hat ebenfalls den Charakters einer Fernwahl und könnte daher juristisch gleich oder ähnlich behandelt werden – als Fernwahl zwar nicht den verfassungsrechtlichen Grundsatz der geheimen Wahl in dem Maß unterstützt wie die Urnenwahl, da bei der Briefwahl Ehepartner oder Freunde „über die Schulter schauen“ können, jedoch vom Verfassungsgericht zweimal (1967 und 1981) als verfassungsgemäß eingestuft wurde [Phil02, S. 149]. Dieser Sichtweise liegen jedoch die Umstände zugrunde, dass (1) ein triftiger Verhinderungsgrund vorliegt und (2) der Anteil der Briefwähler zum Zeitpunkt der Entscheidung mit 5-7% recht klein war. Ggf. ist eine erneute Überprüfung der Zulässigkeit der Fernwahl erforderlich.

- Geringe Transparenz
  Es scheint klar, dass die Umsetzung der Sicherheitsanforderungen kein triviales informationstechnologisches Problem ist, auch wenn die Kryptographie ein reichhaltiges Instrumentenbündel zur Verfügung stellt (s. Abschnitt 4). Dies führt zu einer erhöhten Intransparenz für den Wähler beim Wahlvorgang und der Auszählung, so dass Akzeptanzprobleme verständlich wären.

- Kosten
  Inwiefern und wann sich die Kosten zur Etablierung und dem Betrieb einer Internet-Wahlinfrastruktur amortisieren, ist derzeit unklar. Gegner der Internetwahl verneinen ein mittelfristiges Kosteneinsparpotential.

3 Anwendungsfelder und Pilotprojekte

Potentiell zukunftsträchtige Anwendungsfelder für Online-Wahlen sind alle Wahlen, bei denen ein beträchtlicher organisatorischer Aufwand bspw. aufgrund der Anzahl berechtigter Wähler anfällt. Dazu gehören kaum Wahlen bei Ortsvereinen oder -verbänden, sondern vielmehr politische Wahlen (Kommunalwahlen, Landtagswahlen, Bundestagswahlen, Volksentscheide EU-Wahlen), Sozialwahlen, Personal-, Betriebsrats und Aufsichtsratswahlen, Aktionärsabstimmungen bei Hauptversammlungen von Aktiengesellschaften sowie, Gremienwahlen an Hochschulen und Schulen.

Zu bemerken ist, dass es bei der Diskussion über Online- bzw. Internetwahlen im politischen Bereich einen allgemeinen Konsens darüber gibt, dass diese nicht substituierend, sondern komplementär zu traditionellen Wahlverfahren eingesetzt werden sollen. Bei nicht-politischen Wahlen ist ein derartiger Konsens nicht gegeben.

Internet-Wahlen können in unterschiedlicher Ausprägung durchgeführt werden. Die California Internet Voting Task Force unterscheidet im Kontext eines

Stufenplans nach dem Ort, an dem die Stimme über das Internet abgegeben wird [CIVT00, S. 13ff]:

1. Internetwahl im zuständigen Wahllokal
2. Internetwahl in einem beliebigen Wahllokal
3. Internetwahl an zertifizierten Wahlterminals (z.B. an öffentlichen Plätzen)
4. Internetwahl über einen beliebigen Zugang

Im Fokus dieses Artikels stehen Anforderungen an und Erfahrungen mit der vierten Stufe.

Da sich politische Wahlen aufgrund ihres verfassungsrechtlichen Bezugs von anderen Wahlen ausnehmen, werden zunächst diese betrachtet. Die im Folgenden vorgestellten Pilotprojekte erheben keinen Anspruch auf Vollständigkeit, der Autor hofft jedoch, die wesentlichen erkannt zu haben.

3.1 Politische Wahlen

Online-Wahlen im politischen Bereich gehören sicherlich zu den sicherheitskritischsten, da neben wahlspezifischen Gesetzen wie z.B. dem Bundestagswahlgesetz auch verfassungsrechtliche Grundsätze einzubeziehen sind. In Deutschland hat bislang noch keine derartige politische Wahl stattgefunden. Nach Aussage des derzeitigen Bundesinnenministers Otto Schily sollen bei der Bundestagswahl 2006 die Wahllokale (davon gibt es in Deutschland ca. 80.000) in einem ersten Schritt mit Wahlcomputern ausgestattet werden, im Jahre 2010 sollen die ersten Internetwahlen stattfinden [Phil02, S. 149].

Bei den US-amerikanischen Präsidentschaftswahlen im Jahr 2000 konnten ca. 250 Soldaten auf „certified virus-free“-Rechnern ein Internetwahlverfahren verwenden [Phil02, S. 148], über das jedoch wenig bekannt ist. Wie schon oben erwähnt nutzten bei Vorpräsidentschaftswahlen der US-Demokraten im Jahr 2000 fast 40.000 Wahlberechtigte die Online-Wahl [Elec00], die vom Unternehmen election.com[2] informationstechnologisch begleitet wurde und in der Literatur ausführlich diskutiert wird [PhSp01; MoGl01]. Hier traten diverse Sicherheitsprobleme auf, u.a. Denial of Service-Angriffe sowie die Unsicherheit beim Wähler, ob seine Stimme auch angekommen ist.

Wie im Abschnitt 2 bereits aufgeführt führte der Genfer Vorort Anières im Januar 2003 erstmals in der Schweiz eine offizielle Internet-Wahl zu einem Gemeindeprojekt durch [Genf03]. Inwiefern die Onlinewähler-Quote von ca. 28%

[2] Das Unternehmen election.com hat bereits zahlreiche Internetwahlen weltweit durchgeführt. Bei all diesen ist nachzuprüfen, ob dieselbe Software verwendet wurde und diegleichen Sicherheitsrisiken bestanden.

auf den Charakter des Neuen zurückzuführen ist, ist dem Autor nicht bekannt. Auch über aufgetretene Sicherheitsprobleme ist nichts bekannt.

3.2 Nicht-politische Wahlen

Zu den nicht-politischen Wahlen werden an dieser Stelle im Sinne der obigen Differenzierung auch Hochschulwahlen gezählt. Es hat bereits in vielen Ländern und in unterschiedlichen Kontexten zahlreiche Pilotprojekte gegeben. In Deutschland hat die Forschungsgruppe Internetwahlen [Otte00], die vom Bundesministerium für Wirtschaft und Technologie gefördert wurde, Pionierarbeit geleistet, eine eigene Wahlsoftware i-vote entwickelt und damit zahlreiche Wahlen durchgeführt. Im Februar 2000 fanden beispielsweise die Onlinewahl zum Studierendenparlament der Universität Osnabrück statt [Otte01], im Mai 2002 die Wahl zur Personalvertretung des LDS Brandenburg (Landesbetriebs für Datenverarbeitung und Statistik), bei der die Mitarbeiter(innen) des LDS ihre Stimme ausschließlich am Computer in (Wahllokalen) unter Einsatz von Signaturkarten abgeben konnten, die im Anschluss an die Wahl als eGovernment-Karte des Landes Brandenburg weiterverwendet werden sollen (s. Abbildung 1).

Abbildung 1: E-Government-Karte und Lesegerät des Land Brandenburgs, Quelle: http://www.brandenburg.de/evoting/

Philippsen hat die Wahl zum Studierendenparlament genauer untersucht und einige Sicherheitsprobleme identifiziert. Darüber hinaus bemängelt er, dass das genaue Verfahren immer noch geheim ist und der Quellcode nicht offen gelegt ist [Phil02, S. 47].

Mit Unterstützung des Bundesministeriums für Wirtschaft und Arbeit wurde 2002 das Projekt W.I.E.N. (Wählen in elektronischen Netzen) gestartet, das die

Entwicklung und Erprobung von Online-Wahlverfahren vorwiegend im wirtschaftlichen Bereich als Zielsetzung hat, während sich das Bundesministerium des Inneren (BMI) um die Verwirklichung von Wahlen im politischen Bereich bemühen will [BMWi02].

International sind eine Reihe von Internet-Wahlen von dem Unternehmen election.com durchgeführt worden. Neben der o.a. Vorpräsidentschaftswahl wurden sie beispielsweise beauftragt, Wahlen für das englische Sheffield City Council, für das "Board of Directors" der Australian Information Industry Association (AIIA) und das neuseeländische Studentenparlament der Auckland's University of Technology durchzuführen. Hierzu sind dem Autor keine (sicherheitsrelevanten) Informationen bekannt.

Im Mai 2002 fanden die ersten Online-Wahlen zum „europäischen Studentrat" statt [EUSt02]. Die Sicherheitsvorkehrungen waren insofern gering, da man sich mit persönlichen Code und Passwort auf einer Webseite einloggen konnte, auf der man dann die Stimme abgeben konnte, so dass das Geheimhaltungsprinzip nicht erfüllt wurde.

3.3 Sicherheit

Die vielfältigen Aktivitäten im Bereich der Online-Wahlen motivieren eine eingehende Beschäftigung mit den Sicherheitsanforderungen, die an derartige Wahlen zu stellen sind. Zum einen werden Sicherheitsprobleme sicherlich nicht immer gleich bekannt, zum anderen werden diese aufgrund noch „verhaltener Angriffe" möglicherweise auch nicht aufgedeckt. Mit zunehmender Verbreitung von Online-Wahlen werden sich diese sicherlich ernsteren und systematischeren Angriffen ausgesetzt sehen. Aus diesem Grund plädiert der Autor auch für zahlreiche Pilotprojekte, bei denen die eingesetzten Verfahren und Infrastrukturen vollständig offen gelegt werden und Angriffsversuche willkommen sind, um Schwachstellen zu identifizieren. Im Bereich der Kryptologie hat sich diese Vorgehensweise hervorragend bewährt.

4 Sicherheitsanforderungen

Die juristischen, politologischen und gesellschaftlichen Anforderungen an Wahlen sind in entsprechenden Gesetzen verankert und wurden bislang vornehmlich durch organisatorische Maßnahmen adressiert. So trägt die Sichtschutzwand zur geheimen Wahl bei und gewährleisten die Öffnungszeiten des Wahllokals die zeitlich begrenzte Stimmabgabe. Die Briefwahl erforderte bereits eine Sonderbehandlung und musste juristisch verankert werden. Zur Gewährleistung der geheimen Wahl wurde das Postgeheimnis herangezogen, und die rechtliche

Verankerung der Internetwahl wird sicherlich nicht einfacher und noch zu prüfen sein. Es tritt mit der Informationstechnologie hier eine neue Dimension auf, die den regulatorischen Rahmenbedingungen einer Wahl Rechnung tragen muss. Mit anderen Worten lässt sich festhalten, das sich diese Rahmenbedingungen und Gesetze in der informationstechnologischen Umsetzung der Internetwahl verwirklicht finden müssen. Die technologischen Maßnahmen dürfen also nicht zum Selbstzweck ergriffen werden, sondern dienen der Verwirklichung der regulatorischen Rahmenbedingungen. Man kann auch von einer Abbildung dieser Bedingungen auf informationstechnologische Komponenten sprechen. Darüber hinaus ergeben sich sekundär weitere Anforderungen insbesondere wirtschaftlicher und ergonomischer Art, d.h. Internetwahlen sollten möglichst preiswert und benutzerfreundlich sein (s. Abbildung 2). Kubicek et al. sprechen im Zusammenhang der gesellschaftlichen Verankerung von Internetwahlen und umfassender Anforderungen an diese von interdisziplinärer Anschlussfähigkeit [Kub+02, S. 24]. Schon 1996 hat Cranor allgemeine Anforderungen an elektronische Wahlen formuliert [Cran96].

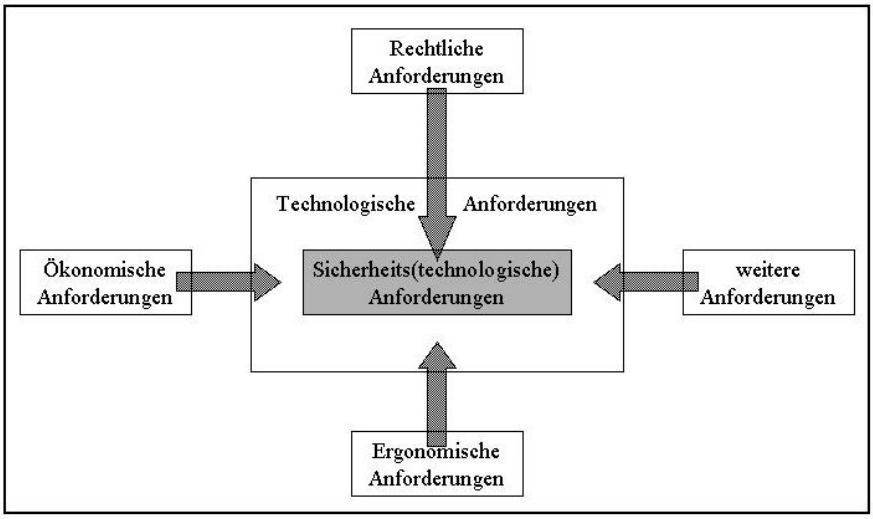

Abbildung 2: Anforderungssystem

Abbildung 2 zeigt die Abhängigkeiten nicht vollständig, die Pfeile deuten aber die wesentlichen Abhängigkeiten an. Die sicherheitstechnologischen Anforderungen gehören zu den kritischen technologischen Anforderungen, da vor allem auf sie die rechtlichen Anforderungen wirken. Sie sind Kern der weiteren Betrachtung.

Die Notwendigkeit einer systematischen Betrachtung von Sicherheitsanforderungen zeigt sich bereits in den bei durchgeführten Wahlen aufgetretenen Sicherheitsproblemen (s. Abschnitte 3.1 und 3.2).

Die exakten Sicherheitsbedingungen sind abhängig von der konkreten Wahlsituation. So bedarf es bei einer landesweiten politischen Wahl anderer Instrumente als bei einer lokal oder regional bezogenen Wahl zum Studentenparlament. Dennoch lassen sich zumindest die im deutschen Grundgesetz festgeschrieben demokratischen Wahlgrundsätze als Ausgangspunkt für die Formulierung sicherheitstechnologischer Anforderungen heranziehen. Ergänzend sind jeweils weitere gesetzliche Rahmenbestimmungen zu beachten wie z.B. Wahlgesetze (horizontale Ausdehnung der Anforderungen). Es ist denkbar, dass für bestimmte Wahltypen unterschiedliche Anforderungsmengen aufgestellt werden. An dieser Stelle soll betont werden, dass es bei der konkreten sicherheitsbezogenen Ausgestaltung von Wahlen nur darum gehen kann, ein wahlindividuell festzulegendes Sicherheitsniveau zu erreichen (vertikale Ausdehnung der Anforderungen), da eine absolute Sicherheit nicht zu erreichen sein dürfte[3].

Im deutschen Grundgesetz heißt es in Artikel 28, Absatz 1, Satz 2: „In den Ländern, Kreisen und Gemeinden muss das Volk eine Vertretung haben, die aus allgemeinen, unmittelbaren, freien, gleichen und geheimen Wahlen hervorgegangen ist." Im Artikel 38, Absatz 1, Satz 1heißt es: „Die Abgeordneten des Deutschen Bundestages werden in allgemeiner, unmittelbarer, freier, gleicher und geheimer Wahl gewählt."

Unter Einbeziehung der juristischen Diskussion dieser Aspekte von Rüß [Rüß00] lässt sich folgende juristisch-technologische Brücke schlagen:

- Allgemeine Wahl
  Der Grundsatz der Allgemeinheit der Wahl sichert allen Wahlberechtigten die Wahlmöglichkeit zu. Da die Internetwahl neben der Briefwahl und Urnenwahl eine zusätzliche Möglichkeit der Wahl darstellt, ergibt sich oberflächlich betrachtet kein Problem. Es ist jedoch zu klären, ob der Ausfall von Systemkomponenten das allgemeine Wahlrecht einschränkt, wenn z.B. fünf Minuten vor Wahlende der Wahlserver nicht zu erreichen ist. Denkt man Client-Server-basiert, so ergeben sich folgende Anforderungen: Auf der Clientseite ist zu gewährleisten, dass die eingesetzte Software während der Wahlzeit korrekt arbeitet. Hier liegt eine Mitverantwortung sicherlich beim Wähler, der dafür zu sorgen hat, dass auf seinem Rechner keine störende Software läuft, die z.B. die Netzwerkkarte ausfallen lässt. Für die Seite der eingesetzten Wahlserver gilt gleiches. Eines der größten Probleme stellt die Störung einer Netzwerkverbindung durch den Ausfall von Teilen der Internetinfrastruktur dar. Mit Denial of Service-Angriffen auf Router oder Wahlrechner ist zu rechnen. Der Autor wagt die These, dass eine derartige

[3] Selbst bei der Urnenwahl kann nicht mit Sicherheit ausgeschlossen werden, dass bei der Kooperation der Wahlhelfer im Wahlbüro die Urne manipuliert wird. Bei der Briefwahl kann der Wähler nicht sicher sein, dass seine Stimme gezählt wurde.

Zuverlässigkeit aller eingesetzten Systeme nicht garantiert werden kann. Aus o.a. Grund stellt sich aber auch die Frage, ob eine derartige Zuverlässigkeit garantiert werden muss.

- Unmittelbare Wahl
  Die Unmittelbarkeit der Wahl besagt, dass zwischen der Stimmabgabe und der Stimmwertung nur die mathematische Ermittlung des Wahlergebnisse liegen darf, also dürfen z.B. keine Wahlmänner eingesetzt werden. Dieser Aspekt ist für Internetwahlen unproblematisch, er hat sich natürlich in der Implementierung der Wahlprozesse widerzuspiegeln.

- Freie Wahl
  Nach dem Grundsatz der freien Wahl hat der Wahlvorgang frei von öffentlicher Gewalt und privatem Druck zu erfolgen. Es ergeben sich diesbezüglich bei der Internetwahl dieselben Aspekte und Bedenken wie bei der Briefwahl, denn die Verhinderung einer Einflussnahme ist technologisch nicht möglich. Hier können keine technologischen Vorkehrungen getroffen werden, sondern es muss eine juristische Bewertung erfolgen.

- Gleiche Wahl
  Der Grundsatz der Gleichheit subsumiert zwei Aspekte: (1) Es sind allen Wahlvorschlägen gleiche Chancen einzuräumen, so dass der Stimmzettel im Internet dasselbe Aussehen und dieselbe Struktur haben muss wie alle anderen Stimmzettel. Fordert man im Zusammenhang mit der geheimen Wahl den Einsatz dedizierter Hardware (Kartenlesegerät), so sind an diese Hardware konsequenterweise die gleichen Anforderungen zu stellen. Insbesondere muss der ganze Wahlzettel zu sehen sein und darf nicht durch Scrollen „gewichtet“ werden. Dies sind keine sicherheitstechnologischen Anforderungen, sondern „nur“ technologische, was jedoch zeigt, dass die rechtlichen Implikation in Abbildung 2 sich nicht nur auf den sicherheitsorientierten Kernbereich beziehen. (2) Hinsichtlich der einzelnen Wähler muss grundsätzlich gelten, dass jede Stimme gleiches Gewicht hat. Dies bedeutet erstens, dass es nicht zur mehrfachen Stimmabgabe derselben Person kommen darf (Authentifizierung). Im Zusammenhang mit der Autorisierung zur Wahl können hier signaturgesetzkonforme Signaturen eingesetzt werden. Es bedeutet zweitens, dass die abgegebene Stimme auch unverändert der Auswertung zugeführt wird (Integrität). Dabei ist sicherzustellen, dass keine „bösartige“ Software auf dem Clientrechner (Viren, Würmer, trojanische Pferde etc.) die Stimme unbemerkt verändert. Das Geheimhaltungsprinzip ist vermutlich nur zu gewährleisten, wenn entsprechend sichere Zusatzhardware mit eigener Anzeige und eigener Tastatur verwendet wird, so wie dies auch im Rahmen des Online-Bankings mit HBCI vorgesehen ist [Stai02]. Ferner darf auf dem Übertragungsweg die Stimme nicht verändert werden. Hier kann man auf bewährte krytographische Verfahren (s. Abschnitt 5) zurückgreifen. Auch sicherzustellen ist, dass die Stimme nicht auf einem Wahlserver verändert werden kann. Die Umsetzung dieser Anforderung bedarf zusätzlicher infrastruktureller und organisatorischer

Maßnahmen (s. Abschnitt 5). Erhebt man sogar den Anspruch, dass der Wähler den Beweis erhalten soll, dass seine Stimme unverändert gezählt wurde, kann man an einen Quittierungsmechanismus denken, der jedoch nur sicherstellen darf, dass die abgegebene Stimme unverändert gezählt wurde und nicht, was gewählt wurde. Denn dadurch wird das Prinzip der freien Wahl insofern unterwandert, als dass mit der Nachweisbarkeit der persönlichen Wahlentscheidung dem Kauf von Stimmen oder der Erpressung Türen geöffnet werden. Drittens darf die elektronisch abgegebene Stimme von keinem Beteiligten oder „Lauscher" kopiert werden können.

- Geheime Wahl
  Die Wahrung des Wahlgeheimnisses gehört mit der Anforderung der Gleichheit der Wahl und der damit verbundenen Anforderung der Stimmintegrität sicherlich zu den schwierigsten Aufgaben.[4] Es kann an denselben Stellen kompromittierend eingegriffen werden, die schon bei der Gleichheit der Wahl diskutiert wurden: Auf dem Rechner des Wählers kann bösartige Software vorhanden sein, die die Daten liest. Auch Fernadministrationssoftware kann hier eingreifen. Die Übertragung der Daten zu einem Wahlserver muss verschlüsselt erfolgen. Auf der Seite der Wahlserver ist zu gewährleisten, dass eine Zuordnung von Wähleridentität und Wählerentscheidung nicht möglich ist. Dies erfordert neben dem Einsatz einer Public-Key-Infrastruktur auch organisatorische Maßnahmen. Es bedarf mindestens zweier Wahlstellen, einem Wahlhost, der die eingehende Stimme bzgl. Autorisierung und Authentifizierung prüft, dabei aber nicht den Wahlentscheid lesen kann, und einem Urnenhost, der die Stimme zwar lesen kann, aber dem sie nur anonymisiert zur Verfügung gestellt werden darf.

Berücksichtigt man darüber hinaus weitere Aspekte diverser Wahlgesetze, so treten zusätzliche Anforderungen auf wie z.B. die Einhaltung der Wahlzeiten bei einer Bundestagswahl [BWG02, §36].

Die Menge der sicherheitstechnologischen Anforderungen ist zur Verifizierung und Validierung eines technologischen Wahlsystems systematisch heranzuziehen. Wie dies geschehen kann, wird im Abschnitt 6 erläutert. Zuvor soll noch kurz auf die wesentlichen kryptographischen Wahlkonzepte eingegangen werden, die die heutige Basis zur Umsetzung der o.a. Sicherheitsanforderungen darstellen.

[4] Schon bei der Briefwahl wurden hier ein Kompromiss eingegangen.

5 Kryptographische Wahlkonzepte

Die in der Literatur vorgeschlagenen Verfahren zur Realisierung einer elektronischen Wahl basieren auf kryptographischen Verfahren. Fundamental sind hier die Werke von Diffie und Hellman [DiHe76] zur asymmetrischen Verschlüsselung sowie von Rivest, Shamir und Adleman [Riv+78] zu digitalen Signaturen. Prinzipiell erhält jeder Kommunikationsteilnehmer ein Schlüsselpaar, das aus einem geheimen (privaten) und nur ihm bekannten Schlüssel und einem öffentlichen Schlüssel besteht. Möchte nun Bernhard eine verschlüsselte Nachricht an Bianca senden, so wendet er auf seine Nachricht und ihren öffentlichen Schlüssel eine Codierungsfunktion an. Nur Bianca ist unter Verwendung einer Decodierungsfunktion mit ihrem privaten Schlüssel in der Lage, die Nachricht zu entschlüsseln. Systeme, die dies realisieren, werden Public-Key-Kryptosysteme genannt und werden heute vielseitig eingesetzt. Verfahren zur digitalen Signatur basieren darauf, dass Bernhard zur Unterzeichnung eines Dokuments seinen privaten Schlüssel verwendet. Ergibt die Anwendung einer „Designierfunktion“ auf das unterzeichnete Dokument und den öffentlichen Schlüssels wieder die Originalnachricht, kann nur Bernhard der Unterzeichner gewesen sein, da nur er seinen privaten Schlüssel kennt. Die sicherheitskritische Stelle liegt bei der Erzeugung und Distribution der Schlüsselpaare.

Es ist klar, dass ein sicheres Verfahren aus mehr als nur einer Instanz bestehen muss, denn ansonsten könnte die einzige Wahlinstanz die jeweilige Stimme dem Wähler zuordnen, und damit (2) die Verwaltung der Wahlliste von einer anderen Instanz wahrgenommen werden muss, als der zur Annahme und Auswertung der Stimme. Im Folgenden sollen nur die beiden bedeutendsten Ansätze skizziert werden, die dieses Prinzip der Gewaltenteilung realisieren [Phil02, S.142ff; Menz01, S. 286ff].

5.1 Verfahren vertrauenswürdiger Instanzen

Neben der Instanz zur Ermittlung und Verteilung der Schlüsselpaare werden ein so genannter Wahlwirt bzw. Validator, der die Wählerlisten verwaltet, und ein Urnenverwalter bzw. Psephor oder Auszähler, der die Stimmen sammelt und auszählt, vorgesehen. Das in Abbildung 3 grob dargestellte Konzept sieht folgenden Prozess vor:

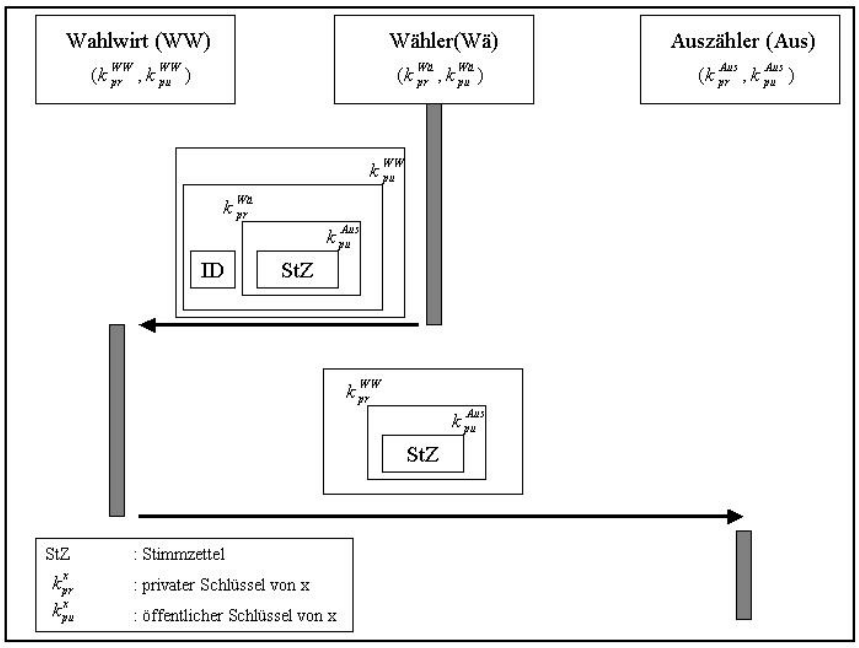

Abbildung 3: Verfahren vertrauenswürdiger Instanzen, in Anlehnung an [Phil02, S. 144]

Jeder Wähler, der Wahlwirt und der Auszähler erhalten jeweils einen geheimen und einen öffentlichen Schlüssel, der Wähler erhält darüber hinaus eine ID, mit der er im Wählerverzeichnis eingetragen ist. Der Wähler füllt seinen Wahlzettel aus und verschlüsselt ihn mit dem öffentlichen Schlüssel des Auszählers, dann signiert er ihn (mit seinem privaten Schlüssel). Zusammen mit seiner ID verschlüsselt er dies dann mit dem öffentlichen Schlüssel des Wahlwirts. Dieser decodiert mit seinem privaten Schlüssel die Nachricht – nur er kann dies – und erhält zunächst die ID. Dann überprüft er durch Anwendung des öffentlichen Schlüssels des (vermeintlichen) ID-Trägers, ob die Nachricht auch authentisch ist. Es verbleibt der mit dem öffentlichen Schlüssel des Auszählers codierte Stimmzettel. Diesen signiert nun der Wahlwirt mit seinem privaten Schlüssel und versendet das Ergebnis an den Auszähler. Dieser wendet den öffentlichen Schlüssel des Wahlwirts an und erhält damit die Garantie, eine (anonyme) Stimme von diesem erhalten zu haben. Es verbleibt ihm noch, mit seinem privaten Schlüssel den Wahlzettel zu decodieren, ohne dass er auf den Wähler schließen kann.

Offensichtliche Schwächen dieses Verfahrens sind die folgenden [Phil02, S.143f]:

- Der Wahlwirt kann Stimmzettel verwerfen und hinzufügen.
- Der Auszähler kann Stimmzettel ändern, verwerfen und hinzufügen.

- Wenn Wahlwirt und Auszähler kooperieren, ist die geheime Wahl nicht gesichert.

Für eine sichere Wahl muss allen Beteiligten vertraut werden. Ein komplexeres Verfahren, das dies nicht fordert, ist das unter Verwendung von Blindsignaturen und anonymen Kommunikationskanälen.

5.2 Verfahren mit Blindsignaturen und anonymen Kanälen

Dieses Verfahren, das auf [Fuj+92] zurückgeht, verwendet dieselben Akteure, unterscheidet sich vom Verfahren vertrauenswürdiger Instanzen jedoch in drei wesentlichen Punkten:

1. Der Wähler muss keiner einzelnen Instanz vertrauen, sondern er kann ein Fehlverhalten von Wahlwirt und Auszähler bemerken.
2. Nicht der Wahlwirt, sondern der Wähler ist für die letztendliche Zustellung seines Wahlzettels verantwortlich.
3. Die Kommunikation des Wählers mit dem Auszähler erfolgt über anonymisierende Kommunikationskanäle.

Abbildung 4 illustriert das Vorgehen analog zur Darstellung des Verfahrens vertrauenswürdiger Instanzen.

Der Wähler besitzt ein weiteres Schlüsselpaar, das zunächst nur er kennt und das nur für eine Wahl verwendet wird. Mit Hilfe dieses Schlüsselpaars kann der Wähler später überprüfen, ob seine Stimme korrekt gezählt wurde. Der Stimmzettel wird zunächst mit dem ersten wahlspezifischen Schlüssel verschlüsselt. Diese Verschlüsselung des Wahlzettels wird erst am Ende der Wahlprozedur aufgehoben, so dass ohne Preisgabe des zweiten Schlüssels niemand außer dem Wähler dessen Wahlentscheid kennt. Nun wird – konzeptionell betrachtet – der verschlüsselte Stimmzettel zusammen mit einem Stück Kohlepapier in einen so genannten Blendumschlag gesteckt mit dem Ziel, dass der Wahlwirt diesen Umschlag stempeln kann und sich dabei dieser Eingangsstempel auf den (verschlüsselten) Stimmzettel überträgt, ohne dass der Wahlwirt den Stimmzettel sehen kann [Chau85]. Damit kann er auch keinen Stimmzettel verändern. Algorithmisch betrachtet wird dazu eine vom Wähler generierte Zufallszahl verwendet. Zusammen mit diesem Blendumschlag wird die ID des Wählers nun vom Wähler signiert und mit dem öffentlichen Schlüssel des Wahlwirts verschlüsselt.

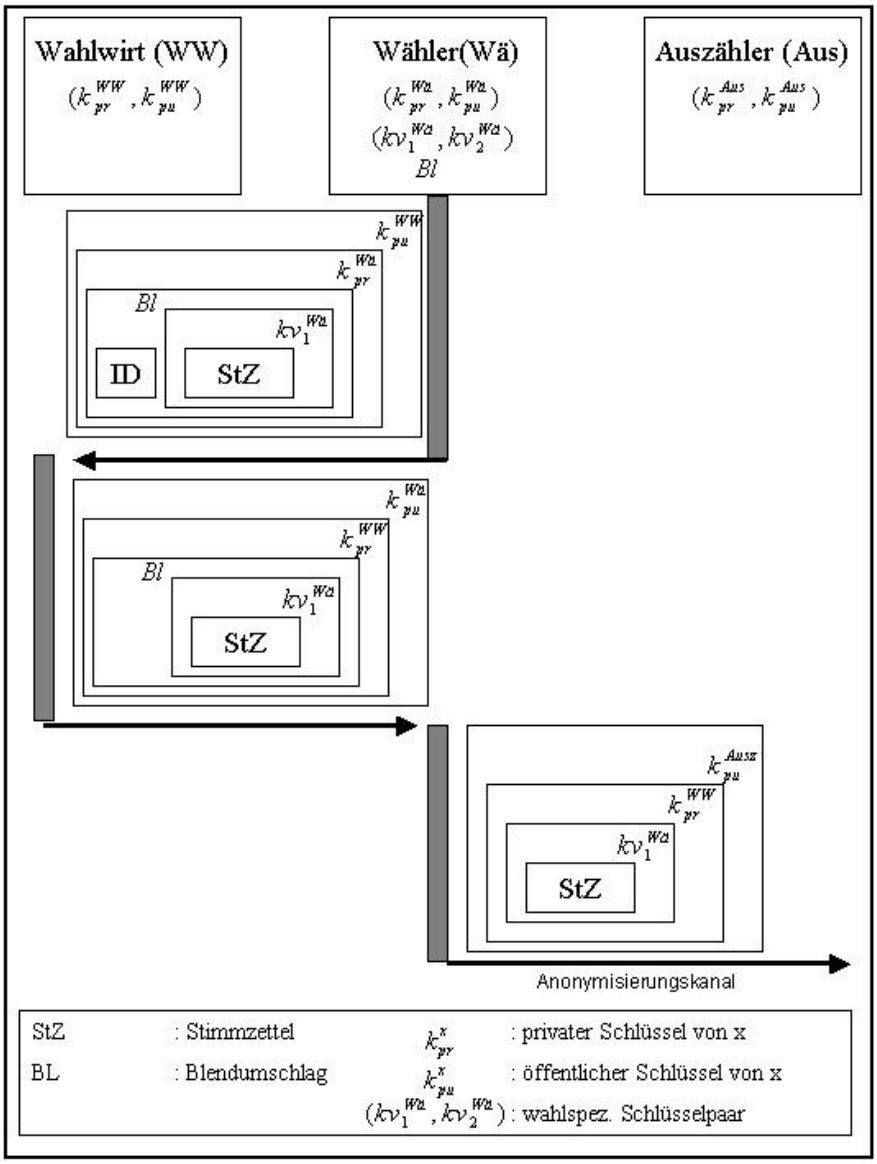

Abbildung 4: Verfahren mit Blindsignaturen und anonymen Kanälen

Nur der Wahlwirt kann die Nachricht entschlüsseln, dann kann er die Authentizität anhand der digitalen Unterschrift überprüfen. Der Wahlwirt notiert die ID und erfasst damit die Wahlhandlung des Wählers. Dann sendet er den Blendumschlag

wieder an den Wähler zurück, signiert und mit dem öffentlichen Schlüssel des Wählers verschlüsselt. Dem Wähler obliegt es nun, seinen verschlüsselten Stimmzettel zum Auszähler zu senden, erneut signiert und mit dem öffentlichen Schlüssel des Auszählers verschlüsselt. Die Kommunikation erfolgt dabei mittelbar über anonymisierende Kommunikationskanäle [Chau81], so dass der Auszähler den Kommunikationsweg nicht zurückverfolgen kann. Dem (mit dem ersten wahlspezifischen Schlüssel) verschlüsselten Stimmzettel weist der Auszähler dann eine Nummer zu und publiziert die Nummer und den zugehörigen (verschlüsselten) Stimmzettel im Internet in einer anonymen Ergebnisliste. Die Nummer sendet der Auszähler über anonymisierende Kommunikationskanäle dem Wähler zu. Zu diesem Zeitpunkt ist der Stimmzettel also noch nicht auswertbar.

Zu einem späteren Zeitpunkt sendet nun der Wähler den zweiten wahlspezifischen Schlüssel zusammen mit der Nummer wieder über anonymisierende Kommunikationskanäle dem Auszähler zu, der damit den verschlüsselten Stimmzettel lesen kann und die korrekte Auswertung dieses Stimmzettels im Internet (in der Ergebnisliste) transparent dokumentieren kann.

Als bedeutende Nachteile sind die folgenden bekannt:

- Aufgrund der Komplexität ist die Implementierung fehleranfällig.
- Es bleibt beim Wähler eine Quittung zurück, mit der er seine Wahlentscheidung beweisen kann.
- Unter bestimmten Bedingungen (nicht-kooperatives Verhalten des Wählers) ist eine Zwischenauswertung der Stimmen möglich: Die Auswertung der Stimme durch den Auszähler ist möglich, sobald dieser den zweiten Schlüssel des Wählers erhält, der idealerweise erst nach Ablauf der Wahl übermittelt wird.

Dem Autor ist kein Kommunikationsprotokoll bekannt, das alle im Abschnitt 4 dargelegten Anforderungen erfüllt.

6 Rahmenwerk

Die bisherige Diskussion hat gezeigt, dass eine Reihe von technologischen Sicherheitsanforderungen besteht, auf die hin Wahlsysteme zu prüfen sind. Neben der Festlegung von Verschlüsselungsfunktionen und -prozessen sind die Aufgaben der Beteiligten festzulegen, Sicherheitsmaßnahmen im Hardware- und Softwarebereich zu treffen sowie Datenkonventionen z.B. für Zertifikate zu vereinbaren. Wegen der Komplexität dieser Anforderungslandschaft und zur Vorbeugung einer Defragmentierung der Sicherheitsdiskussion erscheint es ratsam, derartige Systeme zu modellieren und damit einen systematischen Weg zu ermöglichen, Wahlsysteme mit Anforderungen abzugleichen. Die Beweislast

hinsichtlich einer sicheren Wahlinfrastruktur wird sicherlich zu Recht bei den Befürwortern der Internetwahl liegen.

Abbildung 5 zeigt ein Strukturmodell für Internetwahlsysteme, das die Hardwaresicht mit den klassischen Sichten der Wirtschaftsinformatik Organisation, Daten, Funktionen und Steuerung verbindet.

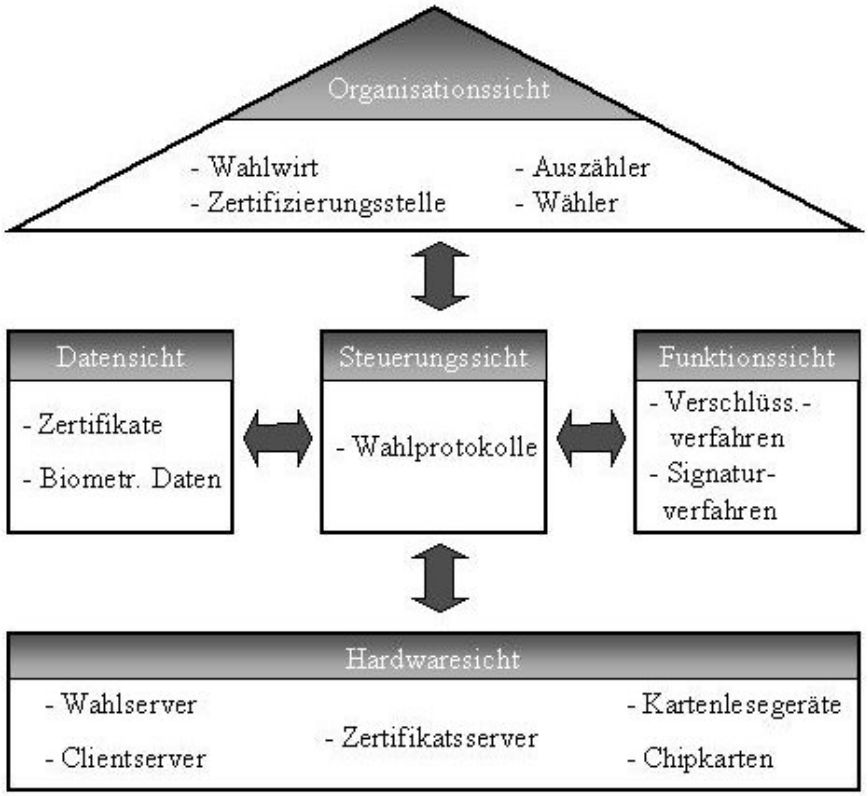

Abbildung 5:Strukturmodell für Internetwahlsysteme

Es gilt nun, geeignete Modellierungsverfahren für die unterschiedlichen Sichten zu identifizieren, die die Darstellung von Sicherheitsmaßnahmen und deren Abgleich mit den Sicherheitsanforderungen unterstützen. Das Rahmenwerk kann auch als Ausgangspunkt verwendet werden, um Qualitäts- und Sicherheitsstandards zu entwickeln.

7 Zusammenfassung und Ausblick

Eine Reihe von Pilotprojekten sind in den letzten Jahren gestartet worden, die mit großem Engagement Internetwahlen in unterschiedlichen Kontexten untersucht haben. Leider fehlt vielen Untersuchungen die Transparenz der eingesetzten Verfahren, was möglicherweise auch auf unternehmerisches Interesse an einer gewissen Geheimhaltung liegt. Auch besteht noch Forschungsbedarf im Grundlagenbereich, so ist beispielsweise noch ungeklärt, wie geeignete Quittierungsmaßnahmen für abgegebene Stimmen aussehen können. Ferner mangelt es an einem methodischen Instrumentarium zur Entwicklung von Sicherheitsstandards und zur Überprüfung der Umsetzung von Sicherheitsanforderungen. Die Forschung steckt trotz ermutigender theoretischer Ergebnisse sicherlich noch in den Kinderschuhen, und viele Probleme werden wohl erst im Rahmen weiterer Pilotprojekte identifiziert werden.

Der Diskurs über Internetwahlen sollte darüber hinaus wählerbezogen geführt werden und klären, in welchen Bereichen die Menschen Internetwahlen wünschen. Empirische Studien und Umfragen sind hier erforderlich. Im politischen Umfeld wird die Internetwahl sicherlich auch aufgrund der gesetzlichen Anforderungen einen schwierigeren Stand haben als in anderen Bereichen.

Literatur

[BMWi02] o.V.: Pressemitteilung des Bundesministeriums für Wirtschaft und Technologie. BMWi startet Projekt „W.I.E.N.- Wählen in elektronischen Netzen, 2002-09-30.

[BWG02] Bundestagswahlgesetz. http://www.bundestag.de/gesetze/bwg/, Abruf am 2003-02-14.

[CIVT00] o.V.: California Internet Voting Task Force. Final Report Online, 2000-01-18. http://www.ss.ca.gov/executive/ivote/, Abruf am 2003-02-15.

[Chau81] Chaum, D.L.: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. Communications of the ACM 2, 1981: S. 84-88.

[Chau85] Chaum, D.L.: Security without Identification. Transaction Systems To Make Big Brither Obsolete. Communications of the ACM 10, 1985: S. 1030-1044.

[Cran96] Cranor, L.F.: Electronic Voting. Computerized polls may save money, protect privacy. ACM Crossroads Student Magazine 4, 1996. http://www.acm.org/crossroads/xrds2-4/voting.html, Abruf am 2003-02-16.

[DiHe76] Diffie, W.; Hellman, M.E.: New Directions in Cryptography. IEEE Transaction on Information Theory, 1976: S. 644-654.

[Elec00] o.V.: Arizonans register overwhelming support for online voting. Online Vote More than Triples 1996 Returns. http://www.election.com/us/pressroom/pr2000/0312.htm, Abruf am 2003-02-15.

[Elec02] o.V.: Presseveröffentlichungen von election.com. http://www.election.com/us/pressroom/pressrel.htm, Abruf am 2003-02-15.

[EUSt02] o.V.: European Studentvote. http://www.eu-studentvote.org/, Abruf am 2003-02-15.

[Fuj+92] Fujioka, A., Okamoto, T., Ohta, K..: A Practical Secret Voting Scheme for Large Scale Elections. Advances in Cryptology. Proc. of AUSCRYPT '92: Workshop on the Theory and Applications of Cryptographic Techniques. Lecture Notes in Computer Science 718. Springer: Berlin et al., 1992: S. 244-251.

[Genf03] o.V.: Site officiel de l'Etat de Genève. http://www.geneve.ch/votations/20030119/resultats.html.

[GG02] Grundgesetz für die Bundesrepublik Deutschland, zuletzt geändert durch Gesetz vom 26. Juli 2002. http://www.bundestag.de/gesetze/gg/gg_07_02.pdf, Abruf am 2003-02-16.

[Kub+02] Kubicek, H.; Westholm, H. ; Wind, M.: Wahlen und Bürgerbeteiligung via Internet. HMD 4, 2002: S. 21-36.

[Menz01] Menzel, T.: E-Voting an österreichischen Hochschulen. In: Schweighofer, Mezel, Kreuzbauer (Hrsg.): Auf dem Weg zur ePerson. Aktuelle Fragestellungen der Rechtsinformatik. Verlag Österreich, 2001: S. 281-291.

[MoGl01] Mohen, J.; Glidden, J: The Case for Internet Voting. Communications of the ACM 1, 2001: S. 72-85.

[Otte98] Otten, D.: Forschungsgruppe Internetwahlen. http://www.internetwahlen.de.

[Otte01] Otten, D.: Wählen wie im Schlaraffenland? Erfahrungen der Forschungsgruppe Internetwahlen mit dem Internet als Wahlmedium. In: Holznagel, B.; Grünwald, A.; Hanssmann, A. (Hrsg.): Elektronische Demokratie. Bürgerbeteiligung per Internet zwischen Wissenschaft und Praxis. Beck: München, 2001, S. 73-85.

[Otte02] Otten, D.: i-vote Report. Chancen, Möglichkeiten und Gefahren der Internetwahl. Zusammenfassung der Ergebnisse und Empfehlungen der „Forschungsgruppe Internetwahlen" zur Nutzung des Internets für Wahlen. http://www.i-vote.de/report.htm, Abruf am 2003-02-14.

[Phil02] Philippsen, M.: Internetwahlen. Demokratische Wahlen über das Internet? Informatik Spektrum 2, 2002: S. 138-150.

[PhSp01] Philips, D.M.; von Spankovsky, H.A.: Gauging the Risks of Internet Election. Communications of the ACM 1, 2001: S. 73-85

[Riv+78] Rivest, R.; Shamir, A.; Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM 21, 1978: S. 120-126.

[Rüß00] Rüß, O.R.: Wahlen im Internet. Wahlrechtsgrundsätze und Einsatz von digitalen Signaturen. MultiMedia und Recht 2, 2000: S. 73-76. http://www.internetwahlen.de/ruess-ns.html, Abruf am 2003-02-14.

[Stai02] Staiger, A.: HBCI und digitale Signatur. Neue Lösungen für das Onlinebanking der Zukunft. HMD 2, 2002.