Fachhochschule Bonn-Rhein-Sieg

Electronic Voting

Bestimmung von Anforderungen an Internetwahlen

Stand: 15. Juli 2004

Daniel Stojceski

Studienarbeit zur Erlangung eines
Leistungsnachweises im 4. Semester

Inhaltsverzeichnis

1 Definitionen und Abgrenzungen

Unter dem Begriff Electronic Voting (E-Voting) verbirgt sich das Prinzip der digitalen Stimmabgabe über ein elektronisches Medium bei Wahlen und Abstimmungen. Aufgrund der stetig zunehmenden Nutzung des Internets und sinkender Wahlbeteiligung bietet es sich an, rechtlich verbindliche Wahlen wie Bundestags-, Landtags- und Kommunalwahlen über das Internet durchzuführen. Neben Begriffen wie Electronic Commerce (E-Commerce), Electronic Business (E-Business) oder Online-Banking, gewinnt der Begriff des E-Voting eine immer größere Beachtung. Auf politischer Ebene wird E-Voting in Deutschland als Schwerpunkt der staatlichen Electronic Democracy–Projekte (E-Democracy) geführt, wobei E-Democracy in engem Bezug zu Electronic Government (E-Government) steht. Der ausschlaggebende Unterschied zwischen E-Government und E-Democracy ist der, dass hinter E-Government das Konzept steht, die staatliche Verwaltungsebene zu digitalisieren, während hinter E-Democracy die Beteiligung und Mitbestimmung des Bürgers bei politischen Prozessen im Vordergrund steht. Das Ziel ist es, dem Bürger mehr Service und Transparenz in Hinsicht auf internetfähige Dienstleistungen und politische Prozesse zu bieten (z.B. Online-Formulare, elektronische Anträge, Online-Bürgersprechstunden oder eben E-Voting).

Bereits im 19. Jahrhundert gab es Bemühungen Abstimmungen mit Hilfe mechanischer und elektrischer Systeme zu beschleunigen. Werner von Siemens stellte 1860 einen elektrischen Abstimmungstelegraphen [Abb. 1] vor, der ein korrektes Ergebnis ermitteln und das Abstimmungsverhalten jedes einzelnen Abgeordneten protokollieren konnte. 1868 folgte eine Entwicklung von Thomas Alva Edison, die ebenfalls die Wahlprozedur beschleunigen konnte und unter der Bezeichnung Electric Vote Recorder [Abb. 2] bekannt war.

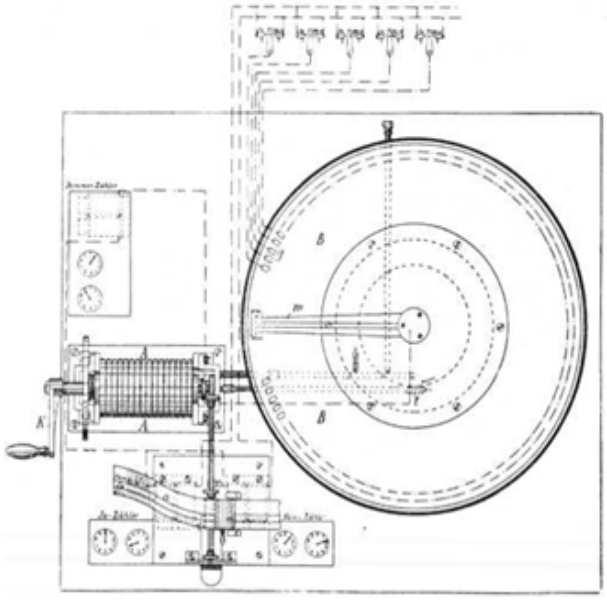

Abb. 1: Abstimmungstelegraph von Werner von Siemens, 1860 [Wilm, 2004]

Es folgten im 20. Jahrhundert so genannte rechnerbasierte Direct Recording Electronic (DRE) – Systeme, die eine Weiterentwicklung der elektrischen Systeme darstellen und heute breite Anwendung finden. Sie sind unvernetzt und dienen der Auszählhilfe. Oft sind sie mit einem Touchscreen ausgerüstet. Der Wahlberechtigte kann darauf seine Stimme abgeben, die elektronisch auf dem DRE-System gespeichert wird.

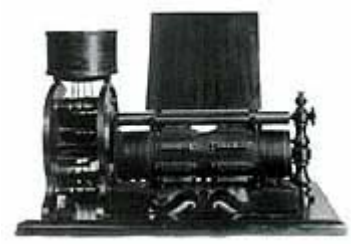

Abb. 2: Electric Vote Recorder von Thomas Edison, 1869 [Smithsonian, o.J]

Hauptargument der Befürworter von Internetwahlen ist, dass die Wahlbeteiligung mit Hilfe von Internetwahlen gesteigert werden könnte. Besonderes Augenmerk wird dabei auf junge Menschen, die mit dem Internet aufwachsen sowie auf Menschen, die zu faul sind zum Wahllokal zu gehen oder aus anderen Gründen ihr Wahllokal nicht aufsuchen können, geworfen.

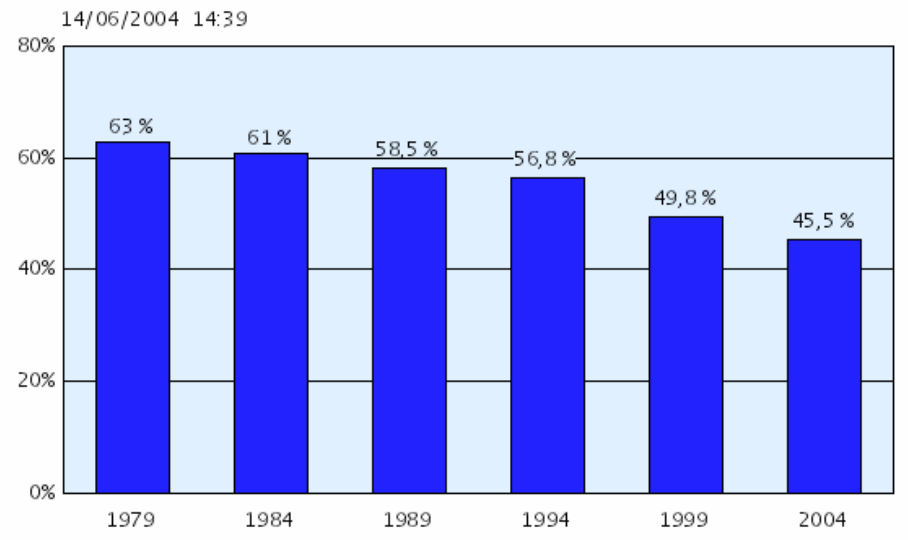

Abb. 3: Entwicklung der Wahlbeteiligung bei Europawahlen [Europäische Gemeinschaften, 2000]

Im Folgenden werden weitere Vorteile, die die Relevanz von Internetwahlen rechtfertigen, aber auch Nachteile [Philippsen, 2002] aufgeführt.

Vorteile:

- Hoffnung auf Kostensenkung
- Komfortable Möglichkeit der Stimmabgabe für kranke und abwesende Menschen
- Effizienzsteigerung (schnell, fehlerfrei und Vermeidung von ungültigen Stimmen)
- Technologische Offensive

Nachteile:

- Wahlprüfung nur mit Spezialwissen möglich
- Vertrauensverlust
- Mögliche Wahlverschiebung
- Schwindendes Gefühl der Bürgergemeinschaft

E-Voting ist ein umschreibender Begriff für elektronische Wahlsysteme, die z.B. auch mit Hilfe elektronischer unvernetzter Wahlmaschinen in Wahllokalen mittels DRE-Systeme realisiert werden können, um z.B. den Stimmzettel bei der Stimmabgabe zu ersetzen oder die Stimmenauszählung durch Wahlmaschinen zu übernehmen.

Diese Arbeit beschäftigt sich mit politischen Internetwahlen und dessen Typen sowie - besonders im Hinblick auf die IT-Sicherheit - mit Anforderungen und nötige Eigenschaften an Internetwahlsystemen bezogen auf den rechtlichen Rahmen in Deutschland. Nicht betrachtet werden DRE-Systeme oder Internetnetwahlverfahren, wie sie z.B. Aktiengesellschaften für Abstimmungen auf Hauptversammlungen verwenden. Internetwahlen sind eine Untergruppe von E-Voting und müssen – sind sie politisch motiviert – die im Artikel 38 des Grundgesetzes festgelegten Wahlrechtsgrundsätze der allgemeinen, unmittelbaren, freien, gleichen und geheimen Wahl sowie die daraus ableitbaren Anforderungen erfüllen. Ein zentrales Problem von Internetwahlen stellt die widersprüchliche Herausforderung dar, den Wähler einerseits eindeutig zu identifizieren und ihm andererseits dennoch eine anonyme Stimmabgabe zu ermöglichen. Dabei wird ein offenes Kommunikationsnetz wie das Internet als Übertragungsmedium für die Kommunikation zwischen den eingebundenen Instanzen im elektronischen Wahlsystem verwendet. Eine Instanz kann z.B. der heimische Rechner, ein für die Stimmenauszählung zuständiger Rechner, ein Urnenserver oder ein kryptographisches Verfahren sein, welches für die Anonymität des Wählers sorgt. Eine Internetwahl ist mit einer im Bundeswahlgesetz, § 36, vorgesehenen Möglichkeit der Briefwahl vergleichbar. Eine Briefwahl erlaubt auch denjenigen Wahlberechtigten die Teilnahme an der Wahl, die sich am Wahltag nicht in ihrem Wahlkreis oder ständig außerhalb des Bundesgebietes aufhalten sowie aus anderen wichtigen Gründen verhindert sind, persönlich ihre Stimme abzugeben. Es lässt sich ableiten, dass eine Internetwahl zunächst als Ergänzung des bisherigen Wahlverfahrens verstanden werden darf, da z.B. nicht jeder Wahlberechtigter einen internetfähigen Rechner besitzt und somit einige der Wahlrechtsgrundsätze, wie z.B. der Grundsatz der allgemeinen Wahl, verletzt würden.

Internetwahlen lassen sich weiter in folgende drei Kategorien unterteilen [Will, 2002], wobei für diese Arbeit die Internetwahl im individuellen Bereich relevant ist; falls nicht anders vermerkt ist immer diese gemeint:

Internetwahl im Wahllokal. Die öffentliche Wahlkabine im Wahllokal wird durch ein öffentliches Eingabegerät im Wahllokal ersetzt. Die vom Wähler eingegeben Daten werden zur Weiterverarbeitung an andere Stellen (Wahlserver), z.B. Stimmenauszählung, über das Internet übermittelt. Die Infrastruktur steht unter staatlicher Kontrolle.

Kiosk-Internetwahl. Das öffentliche Eingabegerät wird an öffentlich zugänglichen Orten, wie z.B. Supermärkte oder Bahnhöfen aufgestellt. Die vom Wähler eingegeben Daten werden zur Weiterverarbeitung an andere Stellen über das Internet übermittelt. Die Infrastruktur steht unter staatlicher Kontrolle.

Individuelle Internetwahl/Internetwahl im individuellen Bereich. Die Stimmabgabe erfolgt über ein privates Eingabegerät (Wahlclient), wie z.B. der heimische internetfähige Rechner, aber auch über beliebige andere Rechner, die nicht gerade für die Internetwahl aufgestellt wurden. Das hat zu Folge, dass der Wähler seine Stimme unabhängig vom Ort seines Wohnsitzes abgeben kann und eine Verlagerung der Stimmabgabe aus öffentliche in private Räume stattfindet. Diese Art von Internetwahl erfordert deshalb eine genauere Untersuchung der politischen und sicherheitsrelevanten Anforderungen, weil ein Teil des Wahlprozesses in den privaten Bereich des Wahlberechtigten fällt. Dadurch ergibt sich die Frage, wer zum Zeitpunkt der Wahl für die Sicherheit des Wahlclients verantwortlich ist. Abb. 4 zeigt schematisch eine mögliche Infrastruktur für eine Internetwahl im individuellen Bereich.

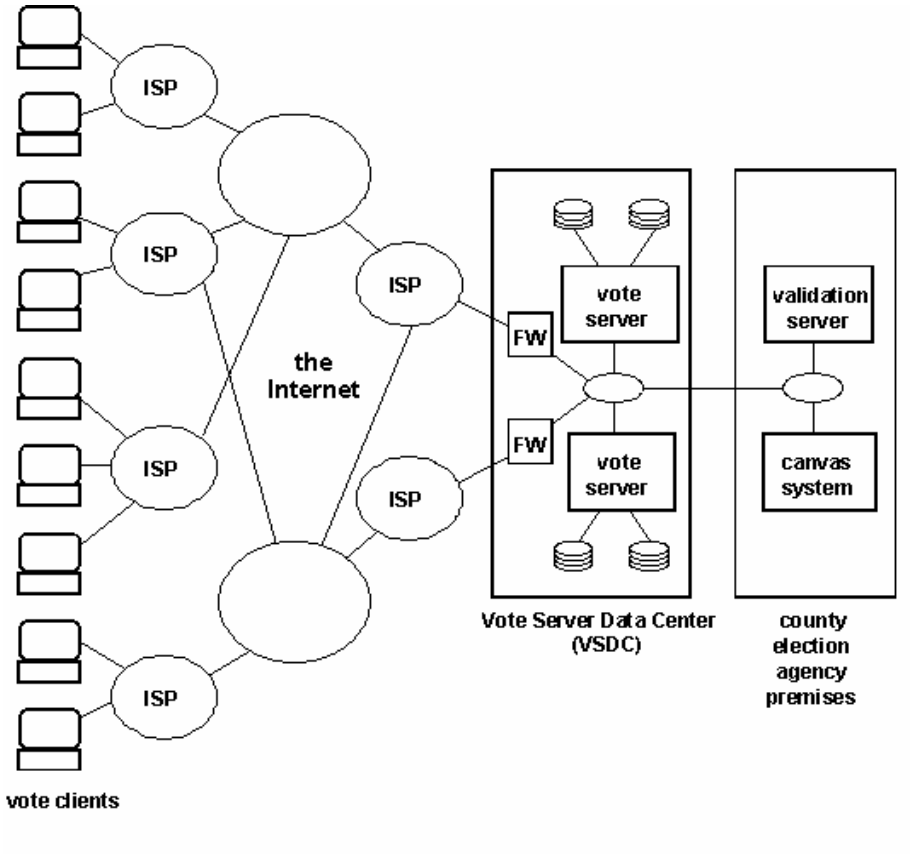

Abb. 4: Schematische Infrastruktur eines Internetwahlsystems [California Internet Voting Task Force, 2000]

In Kapitel 2 werden allgemeine Voraussetzungen zur Durchführung sowie ein Modell zur Integration von Internetwahlen vorgestellt und der aktuelle Stand in der BRD dargelegt. Anschließend werden in Kapitel 3 Anforderungen festgelegt, die für die Realisierung von Internetwahlen erforderlich sind. Es wird insbesondere auf politische und sicherheitsrelevante Aspekte eingegangen.

Im Folgenden werden die Definitionen festgelegt, die für das Verständnis dieser Arbeit benötigt werden.

- Wahlclient. Eingabegerät, das vom Wähler zur Stimmabgabe eingesetzt wird und Dienste eines Wahlservers nutzt und darstellt.
- Wahlserver. Bietet Wahlclients Dienste des Wahlsystems an, wie z.B. die Möglichkeit einen Wähler zu identifizieren oder die Zusendung eines elektronischen Wahlzettels.
- Elektronisches Wählerverzeichnis. Liste, in der alle wahlberechtigten Personen aufgeführt sind.

2 Voraussetzungen und aktueller Stand in Deutschland

2.1 Anschlussfähigkeit und Akzeptanz von Internetwahlen

Werden politische Internetwahlen angestrebt, muss zunächst ihre Anschlussfähigkeit geprüft sowie das Interesse für die Nutzung elektronischer Medien für eine Stimmabgabe auf Seiten des Wahlberechtigten festgestellt werden [Kubicek et al., 2001]. Mit Anschlussfähigkeit ist die Einbettung von Internetwahlen an das bestehende Wahlsystem und dessen Rahmenbedingungen gemeint. Im Folgenden wird insbesondere auf rechtliche, technische sowie gesellschaftliche Aspekte eingegangen.

2.1.1 Anschlussfähigkeit von Internetwahlen

Folgende Faktoren sind für die Realisierung und Anschlussfähigkeit von Internetwahlen an das bestehende Wahlsystem relevant:

Aktualisierung des rechtlichen Rahmens. In Deutschland legen das Grundgesetz, das Bundeswahlgesetz, die Bundeswahlordnung und die Bundeswahlgeräte-Verordnung die Anforderungen an Wahlen und Wahlverfahren fest. Aus diesen rechtlichen Vorgaben leiten sich verbindliche Anforderungen ab, für die Art und Weise, wie eine politische Wahl durchgeführt werden muss. Diese Rechtsvorschriften müssen derart geprüft und ergänzt werden, dass sie den Sicherheitsanforderungen einer Internetwahl gerecht werden [Ullmann et al., 1998]. Die im April 1999 geänderte Bundeswahlgeräteverordnung erlaubt den Einsatz programmgesteuerter Geräte im Wahllokal, allerdings erst, wenn gemäß § 2 eine Bauartzulassung erteilt wurde. Unproblematisch ist dies bei hardwarebasierten Gerätetypen wie sie z.B. die Stadt Köln seit Jahren offline einsetzt. Für softwarebasierte Wahlrechner (Wahlclient und –server) im Internet ist nicht definiert, was unter einer Bauartzulassung zu verstehen ist und was diese Rechner besonders im Hinblick auf die IT-Sicherheit beinhalten und leisten müssen [Kubicek et al., 2001]. Im Bundeswahlgesetz, § 35, Abs. 1, ist festgelegt, dass zur Erleichterung der Abgabe und Zählung der Stimmen anstelle von Stimmzetteln und Wahlurnen Wahlgeräte benutzt werden können. Ausgangspunkt sind vom Bundesministerium des Innern zugelassene Wahlgeräte. Der Autor dieses Kapitels fordert, dass auch eine Möglichkeit für die Zulassung privater Wahlgeräte – wie privater Rechner – eingeräumt wird. Weitere Lösungsansätze zu dieser Problematik können hier die Einbindung digitaler Signaturen und Public Key Infrastrukturen in die Wahlgesetze sein. Ebenfalls muss geregelt werden, welche Anforderungen Stimmabgabe-, Wählerverzeichnis-, Urnen- und Auszählungssoftware erfüllen muss [Kubicek et al., 2001]. Auf den juristischen Rahmen von Internetwahlen wird in dieser Arbeit nicht mehr näher eingegangen. Hier sei auf Fachliteratur verwiesen, wie z.B. [Will, 2002] oder [Bremke, 2004]. In [Will, 2002] gelang man vor allem zu dem Schluss, dass der derzeitige rechtliche Rahmen, wegen des Verstoßes gegen den Grundsatz der allgemeinen Wahl, keine ausschließlich individuelle Internetwahlen erlaubt.

Technische Voraussetzungen. Die zentrale technische Herausforderung bei Internetwahlen besteht darin, dass der Wahlberechtigte zum einen sicher identifiziert werden und zum anderen anschließend die abgegebene Stimme unbedingt geheim bleiben muss. Während bei der klassischen Wahl dieser Schritt durch Wahlhelfer bewacht wird, muss dies bei einer Internetwahl mittels elektronischer Verfahren geschehen. Für die Umset-

zung werden folgende technische Voraussetzungen gefordert [Burmester et al., 2002; Otten et al., 2002]:

- Anonyme Kanäle. Anonyme Kanäle sind, z.B. mittels MIXE [Chaum, 1981], in der Lage, den Weg einer Nachricht in einem offenem Netz wie dem Internet nicht mehr rückverfolgbar zu machen und tragen zur Anonymität des Wählers bei.
- Blinde Signatur. Ein auf [Chaum, 1982] zurückgehendes Verfahren, mit dem die Anonymität einer Person, die zuvor identifiziert wurde, erreicht werden kann. Dazu besitzt der Wähler einen geheimen symmetrischen Schlüssel, mit dem er die Nachricht mit seiner Wahlentscheidung verschlüsseln und unterschrieben an eine legitimierte Instanz, z.B. ein Registrierungsserver, senden kann. Diese Instanz überprüft die Identität des Wählers anhand der digitalen Signatur und signiert bei Erfolg die Nachricht ohne den Inhalt lesen oder entschlüsseln zu können. Darauf hin sendet die Instanz die Nachricht zurück an den Wähler. Im nächsten Schritt entschlüsselt der Wähler die Nachricht mit seinem geheimen Schlüssel und entfernt seine Identität, so dass er sein signiertes Votum anonym an ein Urnenserver senden kann, ohne dass der Urnenserver oder ein möglicher Mithörer die Identität des Wählers rekonstruieren können.
- Elektronische Signatur. Elektronische Signaturen überprüfen die Integrität und die Authentizität einer Nachricht.
- Public Key Infrastructure (PKI). Infrastruktur, in der Dienste zur Verschlüsselung und digitalen Signatur auf Basis von Public Key Verfahren bereitgestellt werden wie Zertifikate, kryptographische Schlüssel oder eine Trusted Third Party (TTP). Eine TTP ist der vertrauenswürdige Dritte im Rahmen der Nutzung digitaler Signaturen, dem alle Nutzer in einer PKI vertrauen. Im Falle von Internetwahlen eine staatliche Instanz.
- Redundanz. Zur Erhöhung des Sicherheitsniveaus und der Verfügbarkeit muss das Wahlsystem redundant sein. Die Stimmabgabe oder die Auszählung der Stimmen dürfen durch eine technische oder gewollte Störung nicht verhindert werden können.
- Transparenz. Die Funktionsweise des elektronischen Wahlsystems muss mindestens gleichermaßen transparent und überprüfbar sein wie das jetzige System und öffentlich zugänglich gemacht werden. Vor allem muss die eingesetzte Software überprüfbar sein. Das bedeutet, dass der gesamte Quellcode offen gelegt werden muss, da sonst die Einhaltung der Wahlrechtsgrundsätze nicht gewährleistet werden kann.
- Verdecktheit. Die im Wahlsystem eingebundenen Instanzen wie Urnenserver, Stimmauszählungsserver etc, dürfen nicht in der Lage sein, Stimmen zu fälschen, vermehren, verkleinern oder auf eine andere Weise das Wahlergebnis zu manipulieren.

Besonders das Vorhandensein oder Fehlen der Transparenz könnte Auswirkungen auf die Akzeptanz von Internetwahlen zur Folge haben. In den folgenden zwei Unterkapiteln wird aufgezeigt, dass im Allgemeinen eine Akzeptanz in der breiten Bevölkerung für Internetwahlen nicht erwartet werden kann und wie Akzeptanz und Vertrauen erlangt werden könnten.

2.1.2 Akzeptanz von Internetwahlen

Eine wesentliche Schwierigkeit von Internetwahlen ist die Schaffung einer ausreichenden Transparenz bei der Ergebnisermittlung. Ein im Jahre 2002 veröffentlichtes Bürgergutachten der Innovations- und Technikanalyse (ITA) über Möglichkeiten und Formen einer elektronischen Demokratie reflektiert unter anderem die Akzeptanz von Internetwahlen unter den Bürgern. In dem Gutachten flossen Empfehlungen der Bürgerforen der Städte Stuttgart, Bad Schussenried, Weikersheim, Mannheim und Ettenheim ein. Vor allem der Sicherheitsaspekt sorgte bei den Bürgern für eine kritische Bewertung von Internetwahlen. Internetwahlen werden höchstens als Ergänzung des jetzigen Wahlsystems oder der Briefwahl akzeptiert. Der Grund ist die Angst vor Verlust der politischen Kultur, z.B. der symbolische Gang zum Wahllokal. Nach Meinung der Bürger stellen die Manipulation des Wahlergebnisses, Verletzung des Grundsatzes der geheimen Wahl und das Fehlen einer verlässlichen digitalen Signatur die größten Risiken dar. Befürwortet wurden allerdings Internetwahlen im Wahllokal und Kiosk-Internetwahlen, sofern die Anforderungen an demokratische Wahlen eingehalten werden können.

Die Anschlussfähigkeit von Internetwahlen ist auch vom Zugang zum Internet und der Bereitschaft für die Nutzung des Internets abhängig. Oft entscheiden soziale Faktoren, ob das Internet als Kommunikationsmedium genutzt werden kann. Dieser Umstand ist auch unter dem Stichwort Digital Divide (Digitale Kluft/Spaltung) bekannt und ist entscheidend für die Anschlussfähigkeit von Internetwahlen [Kubicek, 2001].

Im Folgenden wird ein Verfahren der California Internet Voting Task Force beschrieben, mit dem das Vertrauen der Bürger in Internetwahlen stufenweise erhöht werden könnte.

2.1.3 In vier Stufen zur Internetwahl

Wie das Vertrauen und die Akzeptanz von Internetwahlen schrittweise gewonnen und erlangt und die technische und organisatorische Umsetzung vereinfacht werden kann, zeigt [California Internet Voting Task Force, 2000]. Dort wurde ein vier-Stufenplan [Abb. 5] vorgestellt, der folgende Schritte beinhaltet:

1. Internetwahl im zuständigen Wahllokal.
2. Internetwahl in beliebigem Wahllokal.
3. Internetwahl über Kiosksysteme.
4. Internetwahl über beliebigen Zugang.

In den ersten zwei Stufen erfolgt die Wähleridentifizierung noch durch Wahlhelfer, während bei den letzten zwei Stufen die Wähleridentifizierung durch eine digitale Signatur o.ä. übernommen wird. Während bis zur dritten Stufe die Infrastruktur – Wahlclients, Wahllokale usw. – unter staatlicher Kontrolle bleiben, fällt im vierten Schritt diese Kontrolle weg und der Wahlberechtigte darf von einem beliebigen Standort seine Stimme abgeben. Diese Vorgehensweise vereinfacht die Implementierung und Realisierung von Internetwahlen, indem zunächst die technische Komplexität einfach gehalten wird. Aufbauend auf den praktischen Erfahrungen aus den jeweiligen Stufen wird die Komplexität des Wahlsystems stufenweise erhöht.

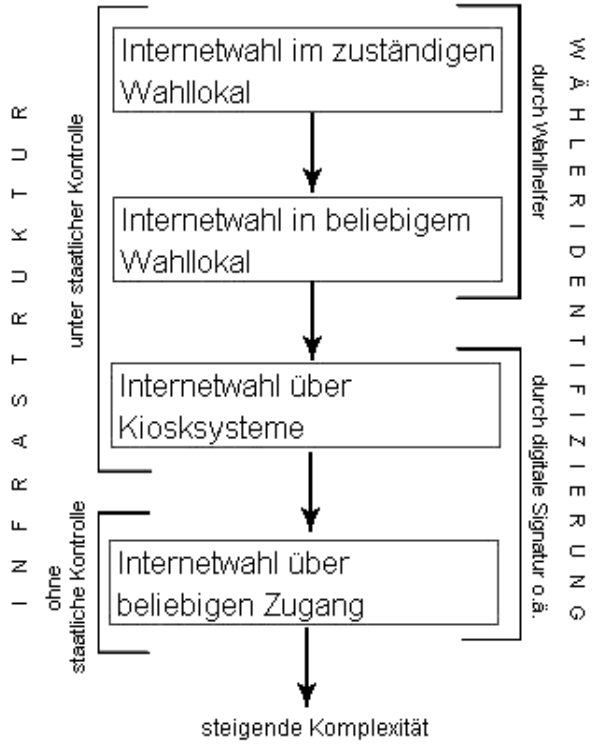

Abb. 5: Schritte zur Realisierung von Internetwahlen [In Anlehnung an: California Internet Voting Task Force, 2000]

2.2 Stand in der Bundesrepublik Deutschland

In Deutschland wird seit 1998 die Machbarkeit von Internetwahlen im Rahmen von E-Government untersucht und erprobt. Dabei wird stufenweise vorgegangen [Schily, 2002]. Dazu wurde im Oktober 2000 im Bundesinnenministerium die Arbeitsgruppe Internetwahlen eingerichtet. Es wurde das i-Vote-Protokoll entwickelt, welches digitale Signatur, Chipkartensysteme und blinde Signatur verwendet [Forschungsgruppe Internetwahlen, 2002] [Vgl. Kapitel 6.1]. Als Folgeprojekt von i-Vote startete im September 2002 das Projekt W.I.E.N. (Wählen in elektronischen Netzwerken), mit dem Ziel unterschiedliche Typen von Online-Wahlen im nicht-parlamentarischen Raum, wie z. B. Betriebsrats-, Personalrats-, Aktionärs- oder auch Sozialwahlen zu entwickeln und erproben. Im Vordergrund stehen die Anpassung der Technik, die organisatorische Gestaltung, rechtliche Fragen und die Akzeptanz bei den Wählenden. Daneben wurde ein gemeinnütziger Verein, die 'Initiative D21' gegründet. Mitglieder sind Unternehmen; er arbeitet mit Vertretern aus Politik und Verwaltung zusammen. Die Ergebnisse aller Projekte dienen dem Ziel politische Internetwahlen zu ermöglichen. Das Vorhaben Internetwahlen bei der Bundestagswahl 2006 anzubieten [Körper, 2001] wurde, wegen Sicherheitsbedenken und fehlendem Vertrauen der Bevölkerung in die Stimmabgabe und die Akzeptanz des Verfahrens, verschoben auf frühestens 2010 [Schily, 2002].

3 Anforderungen an Internetwahlen

3.1 Politische Anforderungen

Die Wahlrechtsgrundsätze für rechtlich verbindliche, politische Wahlen werden in Deutschland im Grundgesetz, Artikel 38 festgelegt. Im Folgenden wird näher auf diese eingegangen, da sie für das Verständnis der Arbeit unverzichtbar sind und sich daraus die Sicherheitsanforderungen an Internetwahlen ableiten lassen.

Folgende gleichrangige Wahlrechtsgrundsätze müssen eingehalten werden:

- Allgemein. Der Grundsatz der allgemeinen Wahl garantiert die Gleichheit beim Zugang der Wahl. Dazu muss das Wahlverfahren ausfallsicher sein. Wie die Briefwahl, könnte eine Internetwahl die Allgemeinheit der Wahl steigern, da Abwesende, Kranke usw. ihre Stimme von einem beliebigen Ort aus abgeben können [Will, 2002].
- Unmittelbar. Der Grundsatz der unmittelbaren Wahl garantiert, dass zwischen Stimmabgabe und Stimmwertung keine weitere Instanz (wie z.B. ein Wahlmännergremium), liegen darf, die das Wahlergebnis beeinflussen könnte. Dazu muss der Wähler überprüfen können, ob seine Stimme korrekt und unverändert gezählt wurde. Bei dieser Überprüfung darf auf dem Rechner des Wählers keine Quittung zurückbleiben, die die Wahlentscheidung des Wählers beweisen könnte.
- Frei. Der Grundsatz der freien Wahl stellt sicher, dass der Wähler seine Stimme frei von physischem oder psychischem Druck abgeben kann. In § 32, Abs. 1, Bundeswahlgesetz ist festgeschrieben, dass „jede Beeinflussung der Wähler durch Wort, Ton, Schrift oder Bild“ vor und in dem Wahlraum während der Wahlzeit verboten ist. Abgebildet auf Internetwahlen könnte der Grundsatz der freien Wahl durch Wahlpropaganda mittels Banner, Pop-ups, bezahlte Bannerwerbung und Browser Banner auf dem Bildschirm des Wählers verletzt werden [Will, 2002].
- Gleich. Der Grundsatz der gleichen Wahl garantiert, dass jede Stimme den gleichen Zählwert und somit den gleichen Einfluss auf das Wahlergebnis hat. Das eingesetzte Internetwahlverfahren muss deshalb die Mehrfachwahl eines Wahlberechtigten ausschließen können. Eine Mehrfachwahl lässt sich ausschließen, indem der Wähler mittels eines Wählerverzeichnisses identifiziert und z.B. immer nur seine letzte abgegebene Stimme gewertet wird [Will, 2002].
- Geheim. Der Grundsatz der geheimen Wahl besagt, dass ausschließlich der Wähler seine Wahlentscheidung kennen darf. Seine Entscheidung darf zu keinem Zeitpunkt zurückverfolgbar sein. Das bedeutet auch, dass seine Entscheidung dauerhaft geheim bleiben muss. Daraus resultiert, dass der Wähler, nachdem er im Wählerverzeichnis als Wahlberechtigter identifiziert wurde, während der gesamten Datenübertragung anonym bleiben muss, auch wenn die Daten ausgespäht werden. Dies ist die zentrale Problematik von Internetwahlen. Es kann nicht gewährleistet werden, dass heute als sicher geltende Verschlüsselungsverfahren – wie die asymmetrische Verschlüsselung – in Zukunft ebenso nicht entschlüsselbar sind. Zu dieser Problematik kommt hinzu, dass der Wähler im Augenblick der Stimmabgabe beobachtet werden könnte. Es gibt heute technische Mittel, die es erlauben elektromagnetische Strahlung – wie z.B. ein Abbild des Inhalts eines Monitors, Strahlung der Graphikkarte oder Verbindungskabel zwischen Graphikkarte und Monitor - aus der Entfernung aufzuzeichnen und zu dekodieren. Somit könnte z.B. der elektronische Stimmzettel mit der Wahlentscheidung des Wählers ausgespäht werden.

3.2 Sicherheitsanforderungen und Schutzziele

Im Folgenden werden allgemeine Sicherheitsanforderungen und Schutzziele bestimmt,

die jedes Internetwahlsystem erfüllen muss, um obigen politischen Anforderungen gerecht zu werden:

- Identifizierung. Der Wähler muss sich vor der Stimmabgabe eindeutig als Wahlberechtigter identifizieren.
- Authentifizierung. Eine Instanz des Wahlsystems muss, z.B. mit Hilfe von digitalen Signaturen, überprüfen können, ob der Wähler auch tatsächlich die Person ist, für die sie sich ausgibt.
- Anonymität. Dem Wähler muss zugesichert werden, dass er seine Stimmabgabe ausführen kann, ohne seine Identität zu offenbaren. Auch der Kommunikationspartner darf nicht die Identität des Wählers erfahren. Eine Ausnahme stellt die Instanz dar, die den Wähler als Wahlberechtigten identifizieren muss.
- Integrität. Die Korrektheit und Manipulationssicherheit des Wahlergebnisses muss gewährleistet sein. Dazu muss das eingesetzte Wahlverfahren garantieren, dass Nachrichten unverändert zwischen den Instanzen des Wahlsystems übertragen werden. Zumindest müssen Manipulationen von einer Instanz oder einem Dritten erkennbar sein und gemeldet werden.
- Unbeobachtbarkeit. Der Wähler muss seine Stimme abgeben können, ohne dass Dritte die Wahlentscheidung beobachten können. Aus Kapitel 3.1 ist ersichtlich, dass diese Anforderung nur schwer realisierbar ist.
- Vermeidung der Mehrfachwahl. Kein Wahlberechtigter darf seine Stimme mehrfach abgeben und dadurch das Wahlergebnis beeinflussen. Die Stimmabgabe muss in einer zentralen Liste sofort registriert und der Status des Wählers auf gewählt gesetzt werden. Dadurch kann man auch vermeiden, dass der Wähler nach der Onlinewahl seine Stimme auch in einem Wahllokal abgibt oder umgekehrt.
- Clientsicherheit. Der Wahlclient muss vor Angriffen bösartiger Software wie Trojaner, Viren und Würmer, sicher sein, die die Integrität oder Anonymität der Wahl gefährden könnte. Während beim jetzigen Wahlverfahren wenige Wahlbetrugsfälle bekannt sind, könnte bei einer Internetwahl ein Angriff automatisiert und auf einer großen Anzahl von Wahlclients des gleichen Typs durchgeführt werden [Wilm, 2003]. Dieses Bedrohungspotenzial lässt sich vermindern, indem der Wahlclient mit Hilfe eines wohldefinierten, bootfähigen Systems auf CD gestartet und sicher konfiguriert wird. Dadurch könnte die Verantwortung der Clientsicherheit weg vom Wähler auf den Staat übertragen und die Frage geklärt werden, wer zum Zeitpunkt der Wahl für die Clientsicherheit verantwortlich ist [Wilm, 2003].
- Serversicherheit. Die Wahlserver müssen gegen Angriffe wie Denial of Service (DoS) und Distributed Denial of Service (DDoS) geschützt sein, um die Verfügbarkeit der Systeme zu gewährleisten. Dos- und DDoS-Angriffe könnten den Zugang zum Wahlsystem verhindern, wodurch bereits abgegebene Stimmen einen Wahlserver nicht oder zu spät erreichen. Die Folge wäre die Verletzung der Grundsätze der allgemeinen und gleichen Wahl.
- Überprüfbarkeit. Der Wähler muss den Erfolg der Stimmabgabe und die korrekte Wertung seiner Stimme überprüfen können. Dabei darf beim Wähler keine Quittung zurückbleiben [Vgl. Quittungsfreiheit].
- Verfügbarkeit. Während der gesamten Wahlzeit muss das Wahlsystem nutzbar sein und dem Wähler jederzeit zur Verfügung stehen.
- Quittungsfreiheit. Das eingesetzte Wahlverfahren muss die Eigenschaft der Quittungsfreiheit besitzen, d.h. einerseits muss der Wahlberechtigte selbst überprüfen

können, ob seine Stimme unverändert gezählt wurde und andererseits darf dabei keine Quittung beim Wahlberechtigten zurückbleiben, die seine Wahlentscheidung beweisen könnte und dadurch den Grundsatz der geheimen Wahl verletzen würde. Es ist der Forschung bislang nicht gelungen ein funktionierendes Verfahren mit Quittungsfreiheit vorzustellen [Philippsen, 2002].

- Sichere Aufbewahrung der Wahldaten. Um den Grundsatz der geheimen Wahl nicht zu verletzten, müssen die gespeicherten Stimmen so gut wie möglich nach außen hin abgesichert sein. Dazu muss der physikalische sowie der Netzzugriff der Medien verhindert werden, die die Wählerstimmen enthalten.

4 Literatur

Bremke, N.: Internetwahlen - Eine Analyse einer Wahlverfahrensergänzung für das 21. Jahrhundert unter besonderer Berücksichtigung rechtlicher Anforderungen, in: LKV Heft 3, Potsdam 2004.

Bruschi, D. et al.: Internet Voting: Do people accept it? Do they trust it?, http://csdl.computer.org/comp/proceedings/dexa/2002/1668/00/16680437.pdf. Milano 2002.

Bundesministerium für Bildung und Forschung (Hrsg.): Bürgerbeteiligung im Internet? Möglichkeiten und Grenzen elektronischer Demokratie. http://www.innovationsanalysen.de/download/buergerbeteiligung_internet.pdf. Bürgergutachten, Nr.207 / Februar, o.O. 2002.

Burmester, M.; Magkos, E.: Towards Secure and Practical E-Elections in the new Area, in: Advances, in: Kluwer Academic Publishers (Hrsg.): Information Security – Secure Electronic Voting, o.O 2003, S. 63-76.

California Internet Voting Task Force: A Report on the Feasibility of Internet Voting, http://www.ss.ca.gov/executive/ivote/final_report.pdf. Sacramento, California 2000.

Chaum, D.: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms, in: Communications of the ACM, 24 (1981) 2, S. 84-88.

Chaum, D.: Blind Signatures for Untraceable Payments, in: Chaum, D., Rivest R.L., & A.T. (Hrsg.): Advances in Cryptology Proceedings of Crypto 82, New York 1982, S. 199-203.

Chaum, D.: Security Without Identification: Transaction Systems to Make Big Brother Obsolete, in: Communications of the ACM, 28 (1985) 10, S. 1030-1044.

Europäische Gemeinschaften: http://www.elections2004.eu.int/ep-election/sites/de/results1306/turnout_ep/graphical.html, Luxemburg 2000.

Kersting, N.: Online-Wahlen im internationalen Vergleich, in: Das Parlament, Online Ausgabe, http://www.das-parlament.de/2004/18/Beilage/003.html, 18, 26.04.2004.

Körper, Fritz Rudolf: Voraussetzung für die Durchführung von Online-Wahlen, Rede des Parlamentarischen Staatssekretärs im Bundesministerium des Innern am 11. Oktober 2001.

Kubicek, H.; Wind, M.: Wie „modernisiere“ ich Wahlen? Der lange Weg vom Pilotprojekt zum Online Voting bei einer Bundestagswahl, in: Filzmaier, P. (Hrsg.): Internet und Demokratie. The State of Online Politics, Innsbruck et al. 2001.

Kubicek, H.; Westholm, H.; Wind, M.: Wahlen und Bürgerbeteiligung via Internet, in: Meier, A. (Hrsg.): HMD 226: E-Government, Heidelberg 2002, S. 21-36.

Menzel, T.: E-Voting an österreichischen Hochschulen, in: Schweighofer, E.; Lachmayer, F. (Hrsg.): Auf dem Weg zur ePerson, Wien 2001, S. 281-291.

Otten, D.; Küntzler, J.: Über die Herstellung von Anonymität bei elektronischen Wahlen, in: Datenschutz und Datensicherheit, 27 (2003) 5.

Philippsen, M.: Internetwahlen – Demokratische Wahlen über das Internet?, in: Informatik Spektrum, 25 (2002) 2, 138 – 150.

Rubin, A.: Security Considerations for Remote Electronic Voting over the Internet, http://avirubin.com/e-voting.security.html, o.O. o.J..

Schefbeck, G.: Elektronische Demokratie, in: Schweighofer, E.; Menzel, T. (Hrsg.): E-Commerce und E-Government, Wien 2000, S. 89-106.

Schreiner, H.: Wahlen per Mausklick – rechtliche Überlegungen zum I-Voting, in: Schweighofer E.; Lachmayer, F. (Hrsg.): Auf dem Weg zur ePerson, Wien 2001, S.259-267.

Schily, O.: Key Note Speech von Herrn Bundesminister Schily zur Fachkonferenz Balanced E-Government der Bertelsmann-Stiftung, Berlin 2002.

Schily, O.: Mit Internet Staat machen: E-Government und Zukunft der Demokratie, Rede von Herrn Bundesminister Schily zum Kongress der Initiative D21, Leipzig 2002.

Smithsonian: http://www.si.edu/lemelson/edison/000_story_02.asp. o.O. o.J.

Ullmann, M.; Koob, F.; Kelter, H.: Anonyme Online-Wahlen - Lösungsansätze für die Realisierung von Online-Wahlen, in: Datenschutz und Datensicherheit, 25 (2001) 11.

von Ameln, G.: Elektronische Demokratie. Neue Möglichkeiten für die Ausweitung der demokratischen Partizipation der Bürger, in: Gora, W.; Bauer, H. (Hrsg.): Virtuelle Organisationen im Zeitalter von E-Business und E-Government, Berlin et al. 2001, S. 381-391.

Will, M.: Internetwahlen – Verfassungsrechtliche Möglichkeiten und Grenzen, Boorberg 2002.

Wilm, P.: Notwendige technische Anforderungen an eVoting-Systeme für staatliche Volksvertreter-Wahlen, in: Dittrich, K. et al. (Hrsg.): INFORMATIK 2003, Innovative Informatikanwendungen, Band 2, Frankfurt 2003, S.222-224.

Wilm, P.: http://elektronische-wahlen.de, o.O. 2004.

Wolf, G.; Pfitzmann, A.: Charakteristika von Schutzzielen und Konsequenzen für Benutzungsschnittstellen, in: Informatik Spektrum, 23 (2000) 3, 173 – 191.

Wolff, C.: Erfahrungen mit der Einführung von E-Voting-Systemen, in: Schweighofer, E.; Lachmayer, F. (Hrsg.): Auf dem Weg zur ePerson, Wien 2001, S. 269-279.

5 Abbildungsverzeichnis