Die Online-Wahl auf dem Weg zum Durchbruch

Probleme und Lösungen für die Durchführung von Online-Wahlen in Deutschland

Melanie Volkamer · Robert Krimmer

In regelmäßigen Abständen müssen in Demokratien auf den verschiedensten Ebenen Wahlen und Abstimmungen abgehalten werden.

Neben den mit großem öffentlichem Interesse stattfindenden Bundestags-, Landtags- und Kommunalwahlen, auch Wahlen erster Ordnung genannt, gibt es eine Vielzahl weiterer Wahlen zweiter Ordnung wie Personal- und Betriebsrats-, Sozial-, Studentenvertretungs-, Vereins- sowie Pfarrgemeinderatswahlen. Jeder deutsche Bürger hat so zumeist mehrmals im Jahr die Möglichkeit, an Wahlen teilzunehmen. Um eine Wahl sicher und ordnungsgemäß durchzuführen, bedarf es neben einer routinierten Wahlorganisation vor allem auch viel Zeit und Geld. Seit Anfang der 70er Jahre ist eine zunehmende Wahlverdrossenheit zu verzeichnen, was sich in einem Rückgang der Wahlbeteiligung über alle Ebenen hinweg widerspiegelt. Diese Tatsachen führten zu Überlegungen, derzeitige Wahlverfahren durch den Einsatz von Computern zu reformieren, um die Kosten sowie den Zeitbedarf zu senken und die Zugänglichkeit und Wählermobilität am Wahltag zu erhöhen.

Einleitung

Seit Beginn der Entwicklung von Computern haben Visionäre wie Fromm, Fuller, Arterton oder Rheingold die Veränderung der Demokratie mit Hilfe der Informationstechnologie in Richtung des Athenischen Ideals einer direkten Demokratie erdacht. Neben diesen politologischen Überlegungen wurden früh auch theoretische technische Umsetzungen erarbeitet. So stellte Chaum 1981 [1] ein erstes theoretisches Wahlprotokoll vor, welches als fundamentale Grundlage für viele weitere Wahlprotokolle (z.B. [4, 8, 9]) gilt. Auftrieb für eine praktische Umsetzung bekamen diese Visionen durch den vom Internet angetriebenen großen Transformationsprozess in der Abwicklung der privaten Wirtschaft und der öffentlichen Verwaltung. Dies hatte zur Folge, dass verschiedene Projekte zur Erprobung von Online-Wahlen ins Leben gerufen wurden.[1] Das bekannteste deutsche Projekt ist das Projekt *Wählen in elektronischen Netzen* (kurz: W.I.E.N.), welches vom Bundesministerium für Wirtschaft und Arbeit (BMWA) gefördert wird und aus der *Forschungsgruppe Internetwahlen* der Universität Osnabrück entstanden ist. So wurden in Deutschland bis heute mehr als vierzig Online-Wahlen – davon etwa die Hälfte mit Rechtsgültigkeit – durchgeführt. Neben den praktischen Projekten ist seither auch eine Vielzahl wissenschaftlicher Arbeiten aus technischer, politischer, juristischer und gesellschaftlicher Sicht entstanden.

Die Diskussionen rund um das Thema Online-Wahlen wurden immer auch von Kritikern begleitet, die vor allem die Verletzung der Grundsätze der geheimen und gleichen Wahl und eine Gefährdung der „Institution Wahl" sehen. Neben dieser Kritik an

[1] Für einen Überblick über die Entwicklungen in anderen europäischen Ländern siehe die Proceedings des Workshop „Electronic Voting in Europe" [10].

DOI 10.1007/s00287-006-0064-1

Melanie Volkamer
Deutsches Forschungszentrum
für Künstliche Intelligenz GmbH,
Stuhlsatzenhausweg 3,
66123 Saarbrücken
E-Mail: volkamer@dfki.de

Robert Krimmer
Wirtschaftsuniversität Wien,
Institut für Produktionsmanagement,
Nordbergstraße 15,
1090 Wien
E-Mail: robert.krimmer@wu-wien.ac.at

Zusammenfassung
Der Beitrag zeigt, welches die grundlegenden Probleme bei elektronischen Wahlen sind und welche interdisziplinären Fragen geklärt werden müssen, um in Zukunft Wahlen rechtsgültig über das Internet abzuwickeln. Nach der Klärung spezifischer Begriffe wird ein Einblick in die rechtlichen Grundlagen von Wahlen gegeben. Als Hauptbeitrag dieses Artikels werden Sicherheitsanforderungen an Online-Wahl-Systeme erklärt und zugehörige Sicherheitsmechanismen erläutert. Dabei wird das Hauptaugenmerk auf die in Deutschland eingesetzten Verfahren gelegt. Der Beitrag schließt mit einem Überblick über alle bisher in Deutschland durchgeführten Online-Wahlen und einer daraus abgeleiteten Empfehlung, was zu tun ist, um den Durchbruch von Online-Wahlen in naher Zukunft zu erreichen.

sozialen Ein- und Auswirkungen gibt es auch Kritiker der Technologie an sich, die die Lösbarkeit der informationstechnologischen Sicherheitsprobleme bezweifeln. Diese Stimmen sowie die fehlenden durchschlagenden Erfolge führten dazu, dass das Thema Online-Wahlen seit Ende 2002 bei vielen Wissenschaftlern und Politikern in Vergessenheit geriet.

Erst die Präsidiumswahl der *Gesellschaft für Informatik e.V.* (GI), die gezeigt hat, dass rechtsgültige Online-Wahlen mit großen Wählerzahlen (rund 20.000 Wahlberechtigte) sehr wohl erfolgreich durchgeführt werden können, führte dazu, dass Online-Wahlen wieder zu einem Diskussionspunkt wurden, insbesondere auch in der Fachgruppe ECOM – „E-Commerce, E-Government und Sicherheit" –, die sich derzeit intensiv mit dem Thema beschäftigt. Verstärkt wird das Interesse durch die soeben beendete zweite Online-Wahl der GI und dadurch, dass auch die *Initiative D21* im Oktober 2005 bereits ihre zweite Vorstandswahl elektronisch abgewickelt hat.

Betrachtet man die ganze historische Entwicklung von Online-Wahlen, entstehen die Fragen, warum es noch nicht zum flächendeckenden Einsatz von Online-Wahl-Systemen gekommen ist, warum der deutsche Online-Wahl Pionier Dieter Otten sein Vorhaben „*zur Europawahl 2004 […] ein rechtskräftiges Wahlverfahren über das Internet anbieten zu können*" nicht umsetzen konnte und warum die diesjährigen Bundestagswahlen nicht, wie von der Initiative D21 gefordert, online durchgeführt wurden. Weiter stellt sich die Frage, ob durch die jüngsten Projekte der Durchbruch erreicht wird.

In diesem Beitrag wird gezeigt, was die grundlegenden Probleme bei elektronischen Wahlen sind und welche interdisziplinären Fragen geklärt werden müssen, um in Zukunft Wahlen rechtsgültig über das Internet abzuwickeln. Zu Beginn werden verschiedene spezifische Begriffe erklärt und gegeneinander abgegrenzt. Außerdem wird ein Einblick in die rechtlichen Grundlagen von Wahlen gegeben. Als Hauptbeitrag dieses Artikels folgen ein Überblick über die verschiedenen Sicherheitsanforderungen an Online-Wahl-Systeme und eine Erörterung zugehöriger Sicherheitsmechanismen, insbesondere über diejenigen, die bei den in Deutschland durchgeführten Online-Wahlen zum Einsatz gekommen sind. Der Beitrag schließt mit einer Empfehlung an alle Beteiligten, was sie tun sollten, um den Durchbruch von Online-Wahlen in naher Zukunft zu erreichen.

Wahlformen

Die Art, wie Wahlen durchgeführt werden, hängt sehr stark vom jeweiligen Umfeld ab. Doch unabhängig davon lassen sich zwei wesentliche Grundformen erkennen: die *Distanz-* und die *Präsenzwahl*, die sich durch den Ort der Stimmabgabe bzw. die Anwesenheit von Wahlhelfern unterscheiden. Ein hierzu orthogonales Unterscheidungskriterium ist das Medium der Stimmabgabe. Hier spricht man von *papierbasierter-* bzw. *elektronischer Wahl*.

Wählt man diese Unterscheidungsmerkmale, also den ‚Ort' und das ‚Medium' der Stimmabgabe, lassen sich folgende vier Grundformen und zwei Mischformen unterscheiden:

Papierbasierte Wahl

Die *papierbasierte Wahl* beinhaltet alle Wahlformen, die als Medium zur Erfassung der Stimme Papier einsetzen. Der Ort der Stimmabgabe ist dabei wesentliches Unterscheidungsmerkmal.

Urnenwahl

Hierbei handelt es sich um die „klassische" Form der Wahl, bei der der Wähler/die Wählerin am Wahltag in das ihm/ihr zugeteilte Wahllokal geht, um die

Abstract
In this article the basic problems of remote electronic voting are described. In addition, the interdisciplinary questions are discussed. After a clarification of e-voting specific terms an introduction to the legal regulations for elections is given. The main contribution of this article is the presentation of security requirements for remote electronic voting and the respective security mechanisms to fulfil the requirements. The paper concludes with an overview of all remote electronic votings conducted in Germany. From these experiences, recommendations on how to make remote electronic voting work are derived.

Stimme auf einem normierten und eigens für die Wahl produzierten Papierstimmzettel abzugeben. Für die ordnungsgemäße Abwicklung der Wahl sorgen Wahlhelfer. Es handelt sich dabei also um eine *Papier-Präsenzwahl*.

Briefwahl

Bei der Briefwahl kann der Wähler/die Wählerin seinen/ihren Papierstimmzettel statt im Wahllokal an einem von ihm/ihr gewählten Ort ausfüllen und auf dem Postweg der Wahlzentrale zusenden. Üblicherweise muss dafür erst ein Antrag gestellt werden und danach werden die Unterlagen auf dem Postweg an die Wählerin übermittelt. Die Sicherstellung einer ordnungsgemäßen Abwicklung der Wahl obliegt dem Wähler/der Wählerin selbst, was in Deutschland durch die Abgabe einer eidesstattlichen Erklärung dokumentiert wird. Diese Form wird auch als *Papier-Distanzwahl* bezeichnet.

Elektronische Wahl

In Analogie zur Empfehlung des Europarats zu E-Voting [2] lassen sich alle Wahlformen, bei denen zumindest die Stimmabgabe an einem elektronischen Gerät erfolgt, unter dem Oberbegriff *elektronische Wahl* zusammenfassen.

Wahlgeräte

Erfolgt die Stimmabgabe an einem elektronischen Gerät im Wahllokal, spricht man von Wahlgeräten. Da diese in ihrem Funktionsumfang und unter dem Gesichtspunkt der Sicherheitsanforderungen stark differieren, muss man sie noch weiter untergliedern. Die bereits in Deutschland eingesetzten Wahlgeräte sind die *Stand-alone-Wahlgeräte*. Sie speichern die abgegebenen Stimmen lokal und zählen sie am Ende der Wahl aus. Im Gegensatz dazu steht die Online-Wahl im Wahllokal, bei der *vernetzte Wahlgeräte* zum Einsatz kommen. Dies bedeutet, dass entweder die Wahlberechtigungsprüfung, die Stimmabgabe oder beide Prozessschritte (Berechtigungsprüfung und Stimmgabe) online erfolgen.

Alle hier beschriebenen Formen werden auch als *elektronische Präsenzwahl* bezeichnet.

Remote Online-Wahl

Diese Form ist unter vielen Begriffen bekannt, darunter Remote E-Voting, Internetwahl und Mobil-Voting. Wichtig ist hierbei, dass die Wahlberechtigungsprüfung und die Stimmabgabe über einen Online-Kanal von einem beliebigen elektronischen Endgerät erfolgt. Vorrangig kommen dabei als Endgeräte PCs und als Kommunikationsmedium das Internet zum Einsatz. Diese Formen stellen die *elektronische Distanz-Wahl* dar.

Mischformen

Neben diesen vier Wahlformen gibt es auch noch zwei Mischformen, die anhand der zuvor genannten Kriterien nicht eindeutig einer der Klassen zugeordnet werden können: der Auszählungsautomat und die Online-Wahl am Kiosk.

Auszählungsautomat

Die *Auszählautomaten* stellen eine Mischform aus papierbasierter und elektronischer Wahl dar. Hierbei werden die Papierstimmzettel automatisch eingelesen, ausgewertet und das Ergebnis berechnet. Bekannte Beispiele hierfür sind die kalifornischen Wahlgeräte von AccuVote sowie der in Hamburg zur diesjährigen Bundestagswahl testweise eingesetzte digitale Stift, der nach jeder Stimmabgabe ausgelesen wird.

Online-Wahl am Kiosk

Die *Online-Wahl am Kiosk* ist eine Mischform zwischen der elektronischen Präsenz- und Distanzwahl. Hierbei stehen die vernetzten Wahlgeräte nicht in einem Wahllokal unter Aufsicht der Wahlhelfer, sondern in öffentlich zugänglichen Gebäuden und Räumen wie Bibliotheken, Schulen

und Einkaufszentren. Sie müssen daher ähnlich den Geldausgabeautomaten besonders gegen Vandalismus, Manipulation und Ausspähung der Stimmabgabe geschützt sein.

Zusammenfassung

Die beschriebenen Wahlformen lassen sich unter den zuvor genannten Gesichtspunkten ‚Ort der Stimmabgabe' und ‚Medium der Stimmabgabe' als Matrix, wie in Tabelle 1 geschehen, darstellen.

Diese Aufstellung ist deshalb sehr wichtig, weil sie eine saubere Trennung zwischen allgemeinen und informationstechnisch-spezifischen Anforderungen an Wahlen erlaubt. Als Beispiel seien hier nur die vielfach diskutierten Probleme des Stimmenkaufs und Wahlzwangs genannt, die bei allen Formen der Distanzwahl, also auch der Briefwahl und der Remote Online-Wahl, die gleichen sind.[2]

Außerdem zeigt diese Aufstellung auch, dass mit dem vielfach verwendeten Begriff „Online-Wahl" verschiedene Wahlformen gemeint sein können:

1. Online-Wahl im Wahllokal (vernetzte Wahlgeräte)
2. Online-Wahl am Kiosk
3. Remote Online-Wahl

Allen dreien ist gemein, dass eine direkte Verbindung zwischen dem Endgerät (Wahlgerät, Kiosk, PC/Handy) und einem zentralen Server zur Übermittlung der Wahlberechtigung oder der Stimmabgabe besteht, allerdings jeweils mit komplett unterschiedlichen Problemstellungen.

In diesem Artikel konzentrieren wir uns auf die Remote-Online-Wahl, welche die technisch spannendste, gleichwohl gesellschaftlich und juristisch umstrittenste Form darstellt.

[2] Siehe den Beitrag der Autoren in [6].

Tabelle 1

	Präsenzwahl	Distanzwahl	Auszählautomat
Papierwahl	Urnenwahl	Briefwahl	
Elektronische Wahl	Stand-alone Wahlgerät Vernetztes Wahlgerät (Online-Wahl im Wahllokal)	Remote Online-Wahl (PC, Handy)	
	Online-Wahl am Kiosk		

Rechtsgrundlagen

Auch wenn auf den ersten Blick eine elektronische Abbildung der herkömmlichen Wahlformen, wie im vergangenen Kapitel aufgezeigt, einfach erscheinen mag, so ist dies aus rechtlicher Sicht schwierig. Derzeit sind für Wahlen in Deutschland nur Stand-alone-Wahlgeräte gesetzlich zugelassen. Nach dem Bundeswahlgesetz sind solche Geräte seit 1975 in mechanischer Form und seit 1999 in elektronischer Form zu Wahlen des Deutschen Bundestages sowie zu Europaratswahlen[3] zulässig. Die Anforderungen an diese Stand-alone-Wahlgeräte legt die Bundeswahlgeräteverordnung fest. Die entsprechenden Geräte werden vor ihrem Einsatz von der Physikalisch Technischen Bundesanstalt (PTB) geprüft und erhalten ggf. vom Bundesministerium des Inneren (BMI) die Bauartzulassung.

Die Online-Wahl ist dagegen nur in Einzelfällen zulässig. So ist beispielsweise in Abschnitt 3.5.4 der Satzung der Gesellschaft für Informatik e.V. festgelegt, dass „der Briefwahl […] vergleichbar sichere elektronische Wahlverfahren gleich gestellt" sind. Ihre *Ordnung der Wahlen und Abstimmungen (OWA)* regelt die Details für ein elektronisches Wahlverfahren.

In allen anderen Bereichen ist die Online-Wahl noch in den Wahlgesetzen und entsprechenden Verordnungen zu verankern. Dabei kann auch auf entsprechende Vorarbeiten im Rahmen des Europarates zurückgegriffen werden. Am sinnvollsten erscheint es, analog zur Bundeswahlgeräteverordnung eine *Online-Wahlverordnung* zu erlassen, in der die Anforderungen an das System und die Durchführung sowie die Zuständigkeiten für Prüfung und Zulassung festgelegt sind. Problematisch erscheint hier insbesondere, dass einerseits die PTB und das BMI große Fachkenntnis und Erfahrung bezüglich der Prüfung von Wahlgeräten haben und andererseits die Expertise für die Prüfung und Zertifizierung von sicherheitskritischen IT-Produkten nach ITSEC bzw. den zukunftsweisenden Common Criteria (CC) beim Bundesamt für Sicherheit in der Informationstechnik (BSI) und den vom BSI akkreditierten Prüfstellen liegt. Es bleibt damit zu

[3] In allen Bundesländern bis auf Brandenburg, Hessen, Nordrhein-Westfalen, Rheinland-Pfalz und Sachsen-Anhalt dürfen diese Stand-alone-Wahlgeräte auch für Landes- und Kommunalwahlen eingesetzt werden.

klären, in welcher Konstellation diese Einrichtungen zusammenarbeiten werden.

Bei der Erstellung einer Online-Wahlverordnung ist zu beachten, dass ein Online-Wahl-System die Grundanforderungen an eine verfassungskonforme Wahl einhalten muss. Diese Grundanforderungen werden durch die fünf *Wahlrechtsgrundsätze*, die eine *allgemeine, unmittelbare, freie, gleiche und geheime* Wahl fordern, abgedeckt. Sie sind in Deutschland bereits im Grundgesetz verankert und regeln hier die Wahl der Abgeordneten des deutschen Bundestages. Dabei verlangt der Grundsatz der allgemeinen Wahl die Gleichheit für alle Wahlberechtigten beim Zugang zur Wahl. Der zweite Wahlrechtsgrundsatz der unmittelbaren Wahl verlangt, dass sich die abgegebene Stimme unmittelbar auf das Ergebnis auswirkt und keine Wahlmittelsmänner eingeschoben werden dürfen. Der Wahlrechtsgrundsatz der gleichen Wahl verlangt eine Zählwert- und Erfolgswertgleichheit aller Stimmen. Dass jeder Wähler sein Wahlrecht ohne Zwang und unzulässige Beeinflussung abgibt, stellt die freie Wahl sicher. Der letzte Wahlrechtsgrundsatz der geheimen Wahl schreibt eine obligatorische und unverzichtbare geheime Wahl für alle Wähler vor, wobei das Wahlgeheimnis zeitlich unbegrenzt sichergestellt werden muss.

Darüber hinaus ist zu beachten, dass in Deutschland die herkömmliche Urnenwahl in Form einer Präsenzwahl die Regelwahlart darstellt. Dagegen ist die Distanzwahl in Form der Briefwahl nur als Ausnahmeregelung erlaubt. Der Grund dafür ist die im Wahllokal durch eine Wahlkabine und die Wahlhelfer gegebene sichere Umgebung zur Stimmabgabe, die eine geheime und freie Stimmabgabe ermöglicht. Dagegen liegt es bei der Briefwahl in der Verantwortung der Wählerin/des Wählers, dass sie/er ihre/seine Stimme unbeobachtet und unbeeinflusst abgibt, was sie mit einer Eidesstattlichen Erklärung beteuert. Dass diese Problematik und damit die klare Trennung zwischen Präsenz- und Distanzwahl nicht zu unterschätzen ist, zeigen auch Klagen vor dem Bundesverfassungsgericht. Daher ist diese Differenzierung auch bei elektronischen Wahlen zu beachten.

Selbst wenn die Onlinewahl in den Bundesgesetzen inklusive einer eigenen Online-Wahlverordnung verankert wäre, muss diese aber noch in den entsprechenden anderen Wahlgesetzen auf anderen Ebenen, sei es in Vereinssatzungen, in der Wahlordnung von Betriebsräten etc. umgesetzt werden. Diese Umsetzung ist je nach Bereich, in dem die Online-Wahl eingesetzt werden soll, unterschiedlich einfach oder schwer. Dies hängt zunächst davon ab, ob der politische Wille vorhanden ist oder nicht. Ein weiterer Einflussfaktor ist die bisherige Wahlform, ob eine reine Briefwahl vorgesehen ist oder ob die Briefwahl die Ausnahme darstellt. So eignen sich – aus rein juristischer Sicht – Bereiche, in denen die Wahlen nicht gesetzlich geregelt sind, am ehesten für die Online-Wahl, da sich die Organisation hier selbst ihre Wahlordnung gibt. Außerdem eignen sich Bereiche, in denen derzeit ausschließlich per Briefwahl gewählt wird, eher als andere zur Einführung der Remote-Online-Wahl, da hier keine Diskussion bzgl. der Distanzwahlproblematik nötig ist. Hierzu zählen beispielsweise die Sozialwahlen.

Sicherheitsanforderungen

Auch wenn noch keine konkrete Online-Wahlverordnung existiert, so gibt es doch eine Reihe von Überlegungen und Katalogen[4], die Anforderungen für ein Online-Wahl-System definieren. Die bekanntesten und umfangreichsten Zusammenstellungen von Anforderungen an Online-Wahl-Systeme sind der Anforderungskatalog für *Online-Wahlen für nicht-parlamentarische Wahlen* der PTB [5], der auf die Online-Wahl im Wahllokal abzielt, sowie die *Empfehlung des Europarates* [2], die sich auf die Remote-Online-Wahl konzentriert.

Untersucht man diese Kataloge genauer, lassen sich die darin enthaltenen Anforderungen in drei Kategorien unterscheiden: 1. die sicherheitstechnischen und 2. die funktionalen Anforderungen an ein Online-Wahl-System sowie 3. die organisatorischen Anforderungen an die Wahlvorbereitung und -durchführung.

Sicherheitstechnische Systemanforderungen

Die sicherheitstechnischen Systemanforderungen werden von den allgemeinen Wahlrechtsgrundsätzen abgeleitet. Die Sicherheitstechnik betrifft die Software der Online-Wahlsystemkomponenten wie auch das zugrunde liegende Kommunikationsprotokoll. Eine Operationalisierung der Grundsätze in Form von Anforderungen findet sich in allen

[4] Eine Zusammenstellung der verschiedenen Überlegungen in Form von Anforderungskatalogen ist unter [14] online verfügbar.

Katalogen. Sie enthalten immer die folgenden Punkte:

1. Zu keinem Zeitpunkt darf eine Zusammenführung von Wählerin und abgegebener Stimme hergestellt werden können. Darüber hinaus darf das System der Wählerin/dem Wähler nicht die Möglichkeit geben, ihre/seine Stimme gegenüber anderen zu beweisen (*Anonymität: Grundsatz der geheimen und freien Wahl*).
2. Eine zuverlässige und eindeutige Identifizierung muss sichergestellt werden. Nur Wahlberechtigte dürfen wählen und jeder darf seine Stimme nur einmal abgeben. (*Authentifizierung: Grundsatz der allgemeinen und gleichen Wahl*).
3. Es darf an keiner Stelle – weder bei der Übertragung noch bei der Speicherung – möglich sein, Stimmen unbemerkt zu verändern, zu löschen oder hinzuzufügen (*Integrität: Grundsatz der allgemeinen und gleichen Wahl*).
4. Die Berechnung von Zwischen- oder Teilergebnissen muss ausgeschlossen werden (*Integrität: Grundsatz der allgemeinen und gleichen Wahl*).
5. Das Ergebnis muss korrekt ausgezählt werden, insbesondere müssen alle abgegebenen Stimmen auch gezählt werden (*Korrektheit: Grundsatz der allgemeinen und gleichen Wahl*).
6. Das Online-Wahl-System muss für alle Server ein Back-Up-System haben und für sämtliche Ausfälle der Server und der Kommunikation, wie auch eines Endgeräts einen Wiederanlaufmechanismus definieren (*Robustheit: Grundsatz der allgemeinen und gleichen Wahl*).

Die genannten Anforderungskataloge unterscheiden sich jedoch in Bezug auf die Verifizierbarkeit des Wahlvorgangs und des Ergebnisses. Teilweise wird sogar gefordert, dass alle Wähler verifizieren können müssen, dass ihre Stimme gezählt wurde. In anderen Katalogen verfolgt man den Ansatz, dass die Korrektheit der Ergebnisberechnung von allen Wählern verifiziert werden können muss.

Funktionale Systemanforderungen

Unter funktionalen Anforderungen versteht man wahlspezifische Durchführungsanforderungen, die je nach spezifischer Wahl oder Organisation, in der die Wahl durchgeführt wird, neu definiert werden können. Dies umfasst üblicherweise Form und Aussehen der Stimmzettel, die Wahlperiode (einerseits lang genug, um DoS-Angriffe sinnlos zu machen und andererseits nicht zu lang, damit Politiker nicht zu oft ihre Meinung ändern), Aus- und Nachzählung der Stimmen, unterstützte Client-Betriebssysteme sowie meistens auch die Definition der Inhalte des Wählerverzeichnisses.

Am wichtigsten erscheint aufgrund der internationalen Diskussion die Festlegung der Anforderungen rund um den Stimmzettel. Die gleiche Wahl fordert, dass die Stimmzettel in Papier- und in elektronischer Form jeweils die gleichen Chancen für alle Kandidaten einräumen. Es muss insbesondere festgelegt werden, wie mit Stimmzetteln umgegangen wird, die nicht auf den Bildschirm passen. Weiterhin muss geklärt sein, wie mit ungültigen Stimmen umgegangen wird. Es ist festzulegen, ob und in welcher Form (z.B. in Form eines Buttons oder eines ungültigen Kandidaten) die bewusste ungültige Stimmabgabe ermöglicht werden soll. Weiterhin muss beim Stimmzettel der Punkt „Schutz vor Übereilung“ Berücksichtigung finden. Hierbei soll durch eine Rückfrage „Sie wählen hiermit XY. Sind Sie sicher?“ eine vorschnelle Stimmabgabe vermieden werden.

Die Liste an funktionalen Anforderungen ist sehr umfangreich und findet sich vor allem in den Empfehlungen des Europarats wieder. Allen Anforderungen ist gemein, dass hier ein großer Entscheidungsspielraum besteht und es sich vor allem um politische Entscheidungen handelt, wie mit den einzelnen Fragen umgegangen wird.

Organisatorische Anforderungen

Die organisatorischen Anforderungen betreffen weniger das Online-Wahl-System an sich, sondern vielmehr Vorgehensvorschriften wie die Inbetriebnahme und Bedienung der Server, die Erstellung des zentralen elektronischen Wählerverzeichnisses, die Information der Wählerinnen und Wähler oder die Verteilung der Wählerauthentifizierungsmerkmale.

Entwicklung eines Schutzprofils

In den existierenden Katalogen sind bereits umfassende sicherheitstechnische, funktionale und auch organisatorische Anforderungen definiert worden, die bei der Entwicklung entsprechender Systeme berücksichtigt werden können und sollen. In Bezug auf eine Prüfung, ob ein System einen speziellen Anforderungskatalog erfüllt oder nicht, ist ein wesentlicher Aspekt, der bisher ausgelassen worden war die *Definition der Rahmenbedingungen*.

Es wird nämlich nicht festgeschrieben, unter welchen Rahmenbedingungen ein Online-Wahl-System die definierten Anforderungen erfüllen muss. Es müssen also die Anforderungen an die Umgebung und das Bedrohungspotenzial festgelegt werden. Erst dann kann entschieden werden, ob ein System die Anforderungen erfüllt. Genau dies hat auch die Expertenrunde, die die GI-Wahlen begleitet, erkannt und daher eine Arbeitsgruppe unter Leitung von Rüdiger Grimm ins Leben gerufen, die das Ziel verfolgt, ein Common Criteria Protection Profile (Schutzprofil) für Online-Wahlen zu entwickeln. Es soll nicht nur die fehlenden Punkte abdecken, sondern sorgt gleichzeitig für eine international akzeptierte Strukturierung der Anforderungen mit dem besonderen Vorteil, dass das Vorgehen zur Prüfung einheitlich und bekannt ist. Hierbei ist derzeit noch die Frage nach der Evaluierungsstufe zu klären.

Sicherheitsmechanismen

Aus den zahlreichen technischen Anforderungen sind die beiden Basisanforderungen *Wählerauthentifizierung* und *Anonymität der Stimme* hervorzuheben. Der Wähler muss eindeutig identifiziert und authentifiziert werden und gleichzeitig seine Stimme vollständig anonym abgeben können. Ein weiteres Merkmal des Sicherheitsdesigns eines Wahlsystems ist die Gestaltung und Umsetzung der *Sicherheit am Endgerät*. Die derzeit vornehmlich eingesetzten Mechanismen werden daher im Anschluss vorgestellt.

Wählerauthentifizierung

Ein wichtiger Bestandteil jedes Online-Wahl-Systems stellt die Identifizierung (durch die Eingabe einer eindeutigen Wählerkennung) gegenüber dem System und die anschließende Authentifizierung (Echtheitsnachweis der Identität) dar. Dieser Nachweis ist erforderlich, um sicherstellen zu können, dass nur Wahlberechtigte eine Stimme abgeben können, jeder Wahlberechtigte nur eine Stimme abgeben kann und insbesondere nicht jemand für eine andere Person wählen kann. Unter anderem wird damit auch der Bedrohung des Stimmenkaufs[5] entgegengewirkt.

[5] Beim Stimmenkauf können zwei Formen unterschieden werden: Entweder der Wähler kann seine Kandidatenwahl dem Käufer beweisen oder der Wähler gibt dem Käufer die Möglichkeit selbst die Stimme abzugeben, beispielsweise indem er ihm sein Authentifizierungsmerkmal überlässt.

Die Identifikation erfolgt über den Namen sowie über weitere persönliche Angaben, die die Wählerkennung einmalig machen. Der Wahlberechtigte überträgt zur Wahlberechtigungsprüfung neben seiner Wählerkennung sein Authentifikationsmerkmal oder Daten, die mit Hilfe dieses Merkmals erzeugt wurden. Es wird zwischen drei Authentifikationsmerkmalen unterschieden:

1. in Form eines Geheimnisses (z.B. ein Passwort),
2. in Form eines Besitzes (z.B. ein elektronisch lesbarer Bibliotheksausweis) oder
3. in Form bestimmter persönlicher Eigenschaften (z.B. der eigene Fingerabdruck).

In der Praxis wird zumeist eine Mischung aus den oben genannten Formen eingesetzt. Die für die Remote-Online-Wahl relevanten Verfahren werden im Folgenden bzgl. ihrer Sicherheit, Benutzerfreundlichkeit und Kosten diskutiert.

Authentifizierung durch die Kenntnis eines Geheimnisses

Eine Möglichkeit der Identifikation und Authentifizierung erfolgt analog zum Anlegen eines Email-Accounts. In der Vorbereitungsphase kann man sich entsprechend einen Wahl-Account anlegen (Festlegen der Nutzerkennung und des Passwortes durch den Wähler), über den man sich bei der eigentlichen Wahl einloggt, um seine Stimme abzugeben.

Auch wenn dieser Ansatz aus Anwendersicht einfach handhabbar und benutzerfreundlich ist, so hat er doch drei Schwachstellen: Erstens kann nicht ausgeschlossen werden, dass auch Personen, die gar nicht wahlberechtigt sind, einen Account anlegen. Zweitens besteht die Gefahr, dass die Wähler einfach zu brechende Passwörter wählen. Drittens kann Stimmenkauf nicht ausgeschlossen werden, da die Wahlberechtigten ihre Zugangsdaten ohne großen Aufwand an einen potentiellen Käufer versenden können.

Eine weitere Umsetzung der Authentifizierung durch Kenntnis eines Geheimnisses stellt die Verwendung einer Wahl-TAN dar. Diese wird Wahlberechtigten vor der Wahl zugeschickt. Diese Variante ist der Authentifizierung mittels eines Geheimnisses bzgl. Benutzerfreundlichkeit sehr ähnlich. Die Kosten dagegen steigen, da den Wahlberechtigten die Wahl-TAN (aus Sicherheitsgründen) mit der Post zugeschickt wird. Dafür steigt aber die

Sicherheit, da die Wahl-TAN vom Veranstalter entsprechend schwer zu brechen gewählt wird. Es bleibt aber die Gefahr des Weitergebens der Wahl-TAN zwecks Stimmenkaufs.

Authentifizierung durch Besitz

Die zweite Kategorie bildet die Authentifizierung mittels eines Besitzes. Hierbei lassen sich zwei Varianten unterscheiden:

1. Verwendung einer Wahl-Chipkarte, die ebenfalls vor der Wahl den Berechtigten zugestellt wird,
2. Verwendung einer Chipkarte, die die/der Wahlberechtigte bereits besitzt und zur Berechtigungsprüfung in anderen Bereichen nutzt, wie etwa seine Jobkarte oder seinen Bibliotheksausweis.

Entscheiden sich die Verantwortlichen den Wählern statt der Wahl-TAN eine Wahl-Chipkarte zuzuschicken, dann erhöhen sie damit einerseits die Sicherheit, da der Stimmenkauf und das illegale Erzeugen des Authentifizierungsmerkmals erschwert werden. Dafür wird in Kauf genommen, dass die Kosten erheblich steigen. Neben den Kosten für die Erzeugung und Verteilung der Chipkarten entstehen auf der Seite des Wählers ebenfalls erhebliche Kosten für einen entsprechenden Kartenleser. Das Anschließen und Installieren dieses Kartenlesers an den eigenen Rechner wirkt sich daneben negativ auf die Benutzerfreundlichkeit aus.

Einige der Nachteile dieser Authentifizierungstechnik lassen sich durch den Einsatz einer bereits vorhandenen und in anderen Bereichen eingesetzten Karte ausräumen. Es bleiben aber die Kosten für das Kartenlesegerät, falls der Wähler ein solches noch nicht besitzt. In Bezug auf Stimmenkauf ist ebenfalls eine Verbesserung erreicht, weil ausgeschlossen werden kann, dass Wahlberechtigte ihre Karte zur Stimmabgabe an einen Käufer weitergeben, da sie ihm damit auch Berechtigungen wie Raumzugänge oder ähnliches weitergeben würden. Die Benutzerfreundlichkeit ist insofern gestiegen, als die Wahlberechtigten bereits mit dem Umgang mit der Karte aus anderen Bereichen vertraut sind.

Authentifizierung durch persönliche Eigenschaften

Die dritte Form der Authentifizierung erfolgt durch eine persönliche (biometrische) Eigenschaft eines Wählers. Die gebräuchlichsten biometrischen Eigenschaften eines Menschen sind sein Fingerabdruck, seine Augen (Iris) oder sein Gesicht. Die Überprüfung der über entsprechende Scanner eingelesenen Daten erfolgt durch Abgleich mit einer Datenbank oder in Kombination mit der Signaturkarte des Wählers auf der Grundlage der dort gespeicherten biometrischen Wähler-Daten. Dieser Ansatz stellt ein Höchstmaß an Sicherheit bzgl. einer eindeutigen Wählerauthentifizierung dar, da biometrische Merkmale nicht weitergegeben werden können. Die Nachteile dieses Ansatzes liegen in den Kosten für die derzeit nicht vorhandene Infrastruktur und der fehlenden Reife der Technologien insbesondere im Zusammenhang mit großen Populationen. Darüber hinaus ist bei der bisherigen Forschung die *False Rejection Rate (FRR)* vernachlässigt worden, da für die Sicherheit in erster Linie die *False Acceptance Rate (FAR)* eine Rolle spielt. Bei Wahlen wird durch eine False Rejection allerdings die Allgemeinheit der Wahl verletzt.

Authentifizierung durch Mischtechniken

In der Praxis kommen zumeist Mischformen der oben genannten Authentifizierungsformen zum Einsatz. Die bekanntesten sind die Kombination aus Besitz und Geheimnis in Form der Signaturkarte zur Erzeugung qualifizierter elektronischer Signaturen und die Kombination aus Besitz und Eigenschaft, bei der die Überprüfung der biometrischen Daten lokal auf einer Karte erfolgt, um das Problem mit dem Datenschutz zu umgehen. Der Einsatz dieser Mischtechniken ermöglicht maximale Sicherheit, da die Imitation dieser Karten sowie die Weitergabe ausgeschlossen werden kann. Benutzerfreundlichkeit und Kosten hängen davon ab, ob die Wahlberechtigten bereits über diese Karte verfügen und sie einsetzen.

Bei einer Entscheidung für eine der Varianten gilt es immer, Sicherheit, Benutzerfreundlichkeit und Kosten einander gegenüberzustellen.

Anonymität der Stimmabgabe

Die Herstellung vollständiger Anonymität bei gleichzeitiger eindeutiger Identifizierung und Authentifizierung der Wahlberechtigten gilt in den Kreisen von Kryptologen als die Königsdisziplin, womit vermutlich die große Anzahl an technischen Lösungsvorschlägen für Wahlprotokolle zu erklären ist.

Für die Einteilung der verwendeten Anonymitätsverfahren gibt es bereits umfangreiche Untersuchungen, die die zahlreich vorhandenen Protokolle in Protokollfamilien untergliedern. In seiner Dissertation hat Manhard Schlifni eine der differenziertesten Klassifikationen [11, S. 130] mit acht verschiedenen Varianten vorgenommen. In der Praxis wird aber nur eine Auswahl davon auch tatsächlich eingesetzt. In Anlehnung an Schlifni werden daher im Folgenden die drei Kategorien vorgestellt, die bei der Durchführung von Online-Wahlen am häufigsten zum Einsatz gekommen sind: 1. Systeme mit *vorgelagerter Wähleridentifizierung*, 2. *Systeme mit verdeckter Auswertung* (Homomorphe Systeme, Hardware Security Module) und 3. *Systeme mit Blinder Signatur*.

Systeme mit vorgelagerter Wähleridentifikation

Bei diesen Online-Wahl-Systemen wird allen Wahlberechtigten ein zufälliges Geheimnis per Post oder eMail zugestellt. Anschließend sind zwei Formen zu unterscheiden.

1. Bei der einfacheren Variante wird die Wahlberechtigung während der Wahl ausschließlich anhand dieses Geheimnisses geprüft, d.h., falls das Geheimnis gültig ist und damit noch keine Stimme abgegeben wurde, so wird die zusammen mit dem Geheimnis verschickte verschlüsselte Stimme gespeichert und später ausgezählt. Da außer der Wählerin/dem Wähler selbst niemand die Zuordnung zwischen ihm/ihr und Geheimnis kennt, wird die Anonymität sichergestellt. Problematisch ist bei dieser Form die aus praktischen Gründen manchmal erforderliche Entfernung von Wahlberechtigten aus dem Wählerverzeichnis während der Wahl. Dies ist faktisch nicht möglich, da die Geheimnisse anonym gespeichert sind.
2. Die einfache Variante der vorgelagerten Wähleridentifikation wurde daher in der Weise erweitert, dass im ersten Schritt das Geheimnis an einen Wahlberechtigungsserver geschickt wird, der die Wahlberechtigung anhand des Geheimnisses und ggf. weiterer Daten überprüft und dem Wähler/der Wählerin dann ein zweites anonymes Geheimnis zuschickt, das er/sie zur berechtigten Stimmabgabe am Urnen-Server vorweisen muss. Neben dem Einsatz bei der GI-Wahl wird diese Variante auch bei den Projekten in Genf und Zürich verwendet.

Für die Sicherstellung der Anonymität ist die Geheimhaltung der Zuordnung von Geheimnis und Wähler/Wählerin erforderlich. Damit ist die Lösung keine rein technische, sondern verlangt auch organisatorische Maßnahmen.

Systeme mit verdeckter Auswertung

Bei Systemen mit verdeckter Auswertung handelt es sich um Verfahren, bei denen die einzelne Stimme nicht entschlüsselt wird, ihr Besitzer aber bekannt ist und nur die Summe über alle Stimmen gebildet und dann das Wahlergebnis entschlüsselt wird. Durch diesen Verfahrensablauf gelten die Systeme als besonders nachvollziehbar und werden deshalb bei Wahlen eingesetzt, bei denen die Stimmabgabe über mehrere Kanäle möglich ist.

Diese Eigenschaft wird in der Praxis durch zwei verschiedene Wege realisiert – entweder durch den Einsatz von Hardware Security Modules (HSM) oder durch homomorphe Kryptographie:

1. HSM werden zur Wahrung der Anonymität in der Weise eingesetzt, dass die verschlüsselten Stimmen im HSM decodiert und ausgezählt werden, aber nicht einzeln, sondern nur in ihrer Summe ausgelesen werden können. Solch ein System kam bei den Lokalwahlen in Estland im Herbst 2005 zum Einsatz.
2. Eine kryptographische Funktion E gilt dann als homomorph, wenn folgende Regel gilt: $E(T_1) \times E(T_2) = E(T_1 + T_2)$. Dann braucht man zur Wahlauswertung nur die verschlüsselten Stimmen miteinander zu multiplizieren, denn das Produkt entspricht dem verschlüsselten Wahlergebnis $T_1 + \ldots + T_n$. Durch diese Eigenschaft können die Stimmen gezählt werden, ohne eine einzelne Stimme zu kennen. Das bekannteste Protokoll wurde von Schoenmakers [12] vorgestellt und war Basis des EU CyberVote Projekts.

Die Sicherstellung der geheimen Wahl beruht bei diesen Verfahren darauf, dass die Auszählung tatsächlich verdeckt erfolgt.

Systeme mit blinder Signatur

Diese Online-Wahl-Verfahren basieren im Wesentlichen auf dem von Chaum bereits 1981

vorgestellten Verfahren zur blinden elektronischen Unterschrift [1]. Chaums Verfahren kann mit dem Einsatz eines Blaupapierkuverts verglichen werden. A will von B eine Unterschrift, ohne dass B den Inhalt des zu unterschreibenden Dokuments kennt. Dazu steckt A das Dokument in das Blaupapierkuvert, versiegelt es, übergibt es B zur Unterschrift. Dieser unterschreibt auf dem Kuvert, die Unterschrift drückt sich durch die Blaupapierfunktion auf das Dokument durch und gibt das Kuvert an A zurück. A öffnet das Kuvert, entnimmt das Dokument, das nun die authentische Unterschrift von B besitzt, ohne dass dieser das Dokument gesehen hat. Setzt man diese Technologie bei Wahlen ein, so werden zwei Varianten unterschieden: Entweder lässt sich der Wähler/die Wählerin den geblendeten Stimmzettel von einer Stelle elektronisch unterzeichnen, um die Stimme dann anonym an eine andere Stelle schicken zu können (wie in [5]), oder das blind signierte Dokument ist ein anonymes Pseudonym (wie in [9]), welches dem Wähler/der Wählerin dann erlaubt, seine/ihre Identität von seinem Stimmzettel zu lösen.

Anforderungen an die Anonymisierung

Neben den hier vorgestellten drei Varianten zur Wahrung der Anonymität in der Stimmabgabe gibt es zahlreiche weitere Vorschläge. Ihnen gemein ist, dass sie zumeist nur Teilprobleme lösen oder auf einen spezifischen Einsatz abzielen. In der Praxis gilt es aber auch, neben der tatsächlichen Erfüllung der geheimen Stimmabgabe, das Vertrauen der Wähler in das Verfahren zu gewinnen. Dies gelingt nicht allein durch mathematische Beweise, sondern vielmehr durch eine anschauliche Darstellung der Ergebnisse und durch eine möglichst hohe Analogie mit herkömmlichen Verfahren, da diese bereits in der Praxis bewährt sind und daher Vertrauen genießen.

Sicherheit am Endgerät

Der Wähler muss zur Stimmabgabe mit dem Endgerät (in der Regel ein PC) auf die Wahl-Server zugreifen können, um seine Stimme dort abzugeben. Es existieren verschiedene Ansätze für die Gestaltung der *Client-Software* des Online-Wahl-Systems, die sich bzgl. Sicherheit, Kosten und Benutzerfreundlichkeit unterscheiden und im Anschluss diskutiert werden.

Client-Software

Für die Realisierung der Client-Software gibt es vier Varianten: 1. kann sie als reine Webbrowser-Lösung, 2. durch einen Rich-Client, 3. durch ein Wahlbetriebsystem und 4. durch ein eigenes Endgerät realisiert werden.

Unter einer reinen *Webbrowser-Lösung* versteht man den Einsatz einer Online-Applikation, die ohne zusätzliche Programme wie Applets, Java Script oder ähnlichem auskommt. Es ist daher die kostengünstigste und benutzerfreundlichste Möglichkeit, Wählern die Online-Stimmabgabe zu ermöglichen, da sie über den beim Wähler bereits installierten Browser erfolgt. Die Kommunikation wird dabei über SSL abgesichert. Bei der Webbrowser-Lösung entfallen alle Protokollansätze, die Berechnungen auf Seiten des Wählers vorsehen. Übrig bleiben daher nur noch Systeme, die sich auf vorgelagerte Wähleridentifikation verlassen (siehe Abschnitt „Systeme mit vorgelgerer Wähleridentifikation“). Die Einfachheit geht einher mit der Übernahme der Verantwortung für die technische und organisatorische Sicherheit durch die Wahlverantwortlichen. Es muss den einzelnen Wahl-Servern vertraut werden, dass sie nicht zusammen arbeiten, um die Wahl zu manipulieren oder das Wahlgeheimnis zu brechen.

Um sämtliche Protokollansätze umsetzen zu können und damit die technische Sicherheit zu erhöhen, werden so genannte *Rich-Clients* beim Wähler eingesetzt. Die Stimmabgabe selbst, sowie verschiedene mathematische und kryptographische Berechnungen erfolgen über eine Wahlsoftware. Einen *Rich-Client* lädt der Wähler aus dem Internet herunter oder erhält ihn auf CD beispielsweise mit der Post oder an öffentlichen Stellen und installiert ihn auf seinem Rechner. Die Erhöhung der technischen Sicherheit wirkt sich einerseits negativ auf die Benutzerfreundlichkeit und andererseits auf die Kosten aus, denn Implementierung und Verteilung werden teuer.

Bei der dritten Variante soll der Wähler eine CD mit einem Knoppix-artigen *Wahlbetriebssystem* ausgehändigt werden, mit der er seinen PC bootet, um seine Stimme abzugeben. Auf diese Weise kann eine erheblich höhere Sicherheitsstufe erreicht werden. Aus Kostengründen sowie wegen der Benutzerfreundlichkeit ist dieser Ansatz aber problematisch: Zum einen entstehen wesentlich höhere Entwicklungskosten (das Betriebssystem muss auf allen PCs einsetzbar sein und eine Verbindung

zum Internet herstellen können) und zum anderen muss das Betriebssystem verteilt werden.

Die letzte Variante lässt sich nur bei kleinen Wählerzahlen umsetzen, da hier jedem Wähler ein *spezielles Wahlgerät* ausgehändigt wird, das die eigentlichen wahlspezifischen Berechnungen wie Verschlüsseln sowie Signieren übernimmt und den PC nur zur Übertragung der Daten an das und aus dem Internet verwendet. Diese Variante bietet zwar ein Maximum an Sicherheit und wäre bzgl. der Benutzerfreundlichkeit akzeptabel, ist aber aus Sicht der entstehenden Kosten nur selten in die Praxis umsetzbar.

Zusatzmechanismen gegen bösartige Software

Da aus Kostengründen und für die Benutzerfreundlichkeit in der Praxis keine 100% sichere Client-Lösung eingesetzt werden kann, gilt das Endgerät als schwächstes Glied in der Sicherheitskette, da auf ihm bösartige Software installiert sein kann. Daher muss ihm besondere Beachtung geschenkt werden. Bösartige unentdeckte Software auf dem Endgerät kann automatisch und unbemerkt großen Schaden anrichten und die Wahlrechtsgrundsätze verletzen: Die Stimme des Wählers kann beispielsweise durch ein Trojanisches Pferd zwecks Stimmenkauf (*freie Wahl*) oder um das *Wahlgeheimnis* zu brechen vor dem Verschicken an den Wahlserver zusätzlich an eine dritte Person übermittelt werden. Die *allgemeine* Wahl kann verletzt werden, indem die Malware dem Wähler vorgibt, seine Stimme am Wahlserver abgegeben zu haben, obwohl diese nie dorthin verschickt wurde. Die auf dem Endgerät installierte Malware kann auch dergestalt programmiert sein, dass die *freie* und *gleiche* Wahl verletzt ist. Die Software könnte hierzu die Stimme vor dem Abschicken verändern. Auf diese Weise kann im großen Stil das Wahlergebnis unbemerkt und automatisch manipuliert werden.

Als Gegenmaßnahmen bieten sich drei Varianten an:

1. Eine Möglichkeit ist, dem Wähler *Hilfestellungen* bei den Sicherheitseinstellungen seines Rechners zu geben. Dies kann beispielsweise in Form einer leicht verständlichen Handreichung geschehen, wie dies bei der GI-Wahl der Fall war.
2. Ein ähnlicher Ansatz kann in Form eines „*automatischen Sicherheitschecks*“ durch die Wahlsoftware erfolgen. Dabei wird vor dem Start der eigentlichen Stimmabgabe das Endgerät auf Malware untersucht.
3. Mit der *Verschleierung der tatsächlichen Stimme* beschäftigen sich die Ansätze von Bernard van Acker [13] und von Gerald Fischer und Wolfang Zuser [3]. Bei ihren Ansätzen wird nicht die eigentliche Stimme verschickt. In van Ackers Vorschlag ist für die Software nicht ersichtlich, ob die Stimme, die gerade verschickt wird, auch die ist, die gezählt wird, oder nur eine Fake-Stimme. Dazu schickt der Wähler dem Server ein zusätzliches zuvor vereinbartes Geheimnis mit, mittels dem der Server entscheiden kann, ob die Stimme gespeichert oder als Fake-Stimme verworfen werden kann. Bei Fischer und Zuser erhält der Wähler zusätzlich zu seinen bisherigen Wahlunterlagen eine eindeutige Zufallszahl (einen Modulo-Wert) und eine mit Hilfe dieser Zahl permutierte Kandidatenliste. Der Wähler entscheidet sich nun für einen Kandidaten und gibt die zugehörige Kandidatenzahl in der Wahlsoftware ein. Der Wahlserver kann dann am Ende anhand der Zuordnung der eindeutigen Zufallszahl und der zugehörigen Kandidatenpermutation den eigentlichen Kandidaten extrahieren und das Ergebnis berechnen. In beiden Fällen kann die Malware auf dem Endgerät keine gezielte Manipulation mehr vornehmen. Es findet allerdings eine Verlagerung der Bedrohungen statt, denn das Offenlegen der jeweiligen Zuordnungsliste ist seinerseits sicherheitskritisch.

Verantwortung des Wählers

Die Sicherung des Endgeräts ist eine wesentliche Voraussetzung für eine sichere Wahl. Da sie aber im Einflussbereich des Wählers selbst liegt, muss dabei auch Verantwortung an den Wähler abgegeben werden. Um dies zu ermöglichen, muss ein Höchstmaß an Unterstützung in Form von hoher Benutzbarkeit, niedrigen Kosten und einfachen Handlungsanweisungen an den Wähler geboten werden.

Dabei darf auch nicht vergessen werden, dass die Wahlverantwortlichen alle in ihrem Einflussbereich liegenden Maßnahmen (automatischer Sicherheitscheck durch die Software etc.) einsetzen sollen, die eine größtmögliche Sicherheit auf der Seite des Wählers gewährleisten können.

Optimale Sicherheit

Bei dem Design eines Online-Wahl-Systems muss immer die Sicherheit an vorderster Stelle stehen. Die hier vorgestellten Mechanismen reichen einzeln für sich nicht aus, um den ordnungsgemäßen Ablauf einer Online-Wahl sicher zu gewährleisten. Erst der kombinierte Einsatz der Methoden macht eine Online-Wahl zu einer sicheren Wahl. Auch wenn damit nie eine 100%ige Sicherheit erreicht werden kann, so ist damit zumindest eine *optimale Sicherheit* erreichbar. Und wenn man sich die Papierwahl in der Praxis ansieht, stellt man fest, dass auch hier keine 100%ige Sicherheit gegeben ist.

Wahltests und rechtsgültige Wahlen in Deutschland

Es wurden in Deutschland in den vergangenen sieben Jahren 41 Online-Wahlen und davon 22 rechtsgültig durchgeführt. Ein Überblick über diese durchgeführten Wahlen findet sich in Tabelle 2 des Anhangs. Damit zählt Deutschland zweifellos neben der Schweiz, Großbritannien und Estland zu den europäischen Vorreitern.

In den letzten sieben Jahren wurden damit über 200 000 Stimmen online abgegeben. Der große Boom ist 2001 zu verzeichnen. Nur 5% der Wähler haben ihre Stimme dabei rechtsgültig abgegeben und 95% bei einem Wahltest. Auffallend ist, dass die Anzahl der Stimmberechtigten bei Wahltests viel größer ist als bei rechtsgültigen Online-Wahlen. Ausnahmen bilden die Wahl des Betriebsrates der T-Systems (1777 Stimmen) und die beiden GI-Wahlen (4845 bzw. 4030 Stimmen). Die Übersicht hebt auch die beiden bekanntesten deutschen Systeme hervor. Zum einen das *Polyas* System der Firma Micromata GmbH, das bereits erstmals 1997 in Finnland in einer Schule bei einem Wahltest zum Einsatz kam. Zum anderen das *ivote*-System, dessen erste Ideen bereits für das Wahlspiel 1998 implementiert wurden. Dieses wurde erst von der Forschungsgruppe Internetwahlen und dann im Rahmen des Projekt W.I.E.N. weiter entwickelt. Derzeit wird das *ivote*-System von der Stiftung Internetwahlen betreut. Das W.I.E.N. Projekt wird heute von T-Systems weitergeführt, um darin nun das *T-Vote* System zu entwickeln. Die Wahlen mit dem *Polyas* System zeichnen sich vor allem durch die großen Wählerzahlen aus, wogegen mit *ivote* bereits mehrere Wahlen mit unterschiedlichen Authentifizierungstechniken durchgeführt wurden.

Zur Authentifizierung wurde bei 22 der Wahlen Wahl-PINs oder Wahl-Passwörter eingesetzt und bei 11 Online-Wahlen kamen Chipkarten zum Einsatz. Nur ein einziges Mal wurde mit biometrischen Merkmalen gearbeitet. Homomorphe Verfahren kamen ebenfalls nur ein einziges Mal zum Einsatz. Dagegen halten sich blinde Signaturen (17) und vorgezogene Anonymisierung (19) die Waage.

Die zahlreichen durchgeführten Online-Wahlen zeigen, dass letztendlich nicht die eingesetzte Technik als solche verantwortlich für das Ausbleiben eines Durchbruchs von Online-Wahlen via Internet ist, denn sowohl alle Arten der Authentifizierungstechniken als auch alle Anonymisierungsmechanismen wurden in unterschiedlichen Systemen eingesetzt. Daher sind die Hindernisse auf einer anderen Ebene zu suchen.

Schlussfolgerung und Handlungsempfehlungen

Der Beitrag bietet einen breiten Einblick in die Thematik und Problematik von Online-Wahlen – insbesondere für den Standort Deutschland. Er spiegelt die Erfahrung der letzten 20 und insbesondere der letzten sieben Jahre wider, die gezeigt haben, dass es sich um ein hochkomplexes und interdisziplinäres Thema handelt (vgl. Abb. 1).

Neben den in diesem Artikel vorrangig angesprochenen technischen und juristischen Aspekten werfen Online-Wahlen auch verschiedene soziologische und politologische Fragestellungen auf. Politische Diskussionspunkte betreffen neue komplexere Wahlformen und den Weg zur direkten Demokratie mit einer Vereinfachung des Wahlvorgangs durch den Einsatz von Online-Wahlen. Die Aufgabe von Soziologen ist es zu untersuchen, wie *Junk Vote* vermieden werden kann und ob sich die

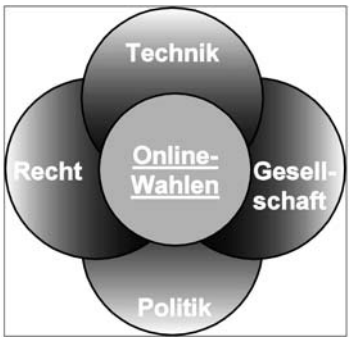

Abb. 1 Dimensionen von Online-Wahlen

Wahlbeteiligung und das Wahlverhalten durch die Einführung von Online-Wahlen verändert.

Viele der angesprochenen Fragestellungen können und sollen von den einzelnen Experten der vier Disziplinen parallel bearbeitet und erforscht werden. Generell muss aber jede Disziplin eine Grundvorstellung der Probleme der anderen Disziplinen haben. Einige Fragestellungen sind nur gemeinsam zu bewältigen, so vor allem die Erstellung einer Online-Wahlverordnung, die technische Anforderungen, die die juristischen Vorgaben ausdrücken, enthält.

Abschließend ist festzustellen, dass derzeit die ersten Früchte der zahlreichen Forschungsarbeiten der vergangenen Jahre geerntet werden können. Um jedoch flächendeckend rechtsgültige Online-Wahlen erfolgreich in Gremien, Vereinen, Verbänden und ähnlichen Organisationen durchführen zu können, sind weitere Arbeiten erforderlich. Hierzu liefert die Gesellschaft für Informatik e.V. einen entscheidenden Beitrag durch die Einrichtung der Expertengruppe mit Erfahrungen aus vielen Sicherheitsbereichen sowie dem Wahlgeräteumfeld, die die Durchführung der GI-Wahl als Online-Wahl begleitet und untersucht hat. Ein weiterer wichtiger Punkt ist die Erstellung und Zertifizierung eines Protection Profiles nach CC für Online-Wahlen in Gremien und Vereinen, um die sich auf dem Markt befindenden Online-Wahl-Systeme vor dem Einsatz nach allgemein anerkannten Regeln und Vorgehensweisen von unabhängigen Gutachtern prüfen zu können.

Hierdurch sind wir auf dem besten Wege, die erste Stufe des beispielsweise von Kubicek in [7] vorgeschlagenen schrittweisen Vorgehens zu erreichen, und können uns dann in einem weiteren Schritt staatlich geregelten Wahlen wie Betriebs- und Personalratswahlen widmen. Hierbei muss zunächst über die Art der Online-Wahl und das Authentifizierungsmerkmal entschieden werden, um die entsprechenden Verordnungen aus Gremienwahlen anpassen zu können. Bis hierher wird es aber noch einige Zeit dauern – aber die Entwicklung dahin scheint unaufhaltsam zu sein.

Literatur

1. Chaum, D.: Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms. Commun. ACM 24(2), 84–88 (1981)
2. Council of Europe: Legal, operational and technical standards for e-voting. Recommundation Rec(2004)11 and explanatory memorandum, Council of Europe, Straßburg 2004
3. Fischer, G., Zuser, W.: Increasing election secrecy: The vote scrambling algorithm. Technical Report der Technischen Universität Wien 2005
4. Fujioka, A., Okamoto, T., Ohta, K.: A Practical Secret Voting Scheme for Large Scale Elections. In: Advances in Cryptology – AUSCRYPT92., Springer-Verlag, Berlin, S. 244–251, 1993
5. Hartmann, V., Meißner, N., and Richter, D.: Online Voting Systems for Non-parliamentary Elections: Catalogue of Requirements: PTB Bericht 8.5-2004-1, Berlin 2004
6. Krimmer, R., Volkamer, M.: Bits or Paper? Comparing Remote Electronic Voting to Postal Voting. In: Andersen, K. V., Grönlund, Å., Traunmüller, R., Wimmer, M. (Eds.) Workshop and Poster Proceedings of the Fourth International EGOV Conference 2005, Universitätsverlag Rudolf Trauner, Copenhagen, S. 225–232, 2005
7. Kubicek, H., Wind, M.: Wie „modernisiere" ich Wahlen? Der lange Weg vom Pilotprojekt zum Online Voting bei einer Bundestagswahl. In: Filzmaier, P. (Ed.) Internet und Demokratie: The State of Online Politics, Studien-Verlag, Innsbruck Wien, S. 130–138, 2001
8. Otten, D., Küntzler, J.: Über die Herstellung von Anonymität bei elektronischen Wahlen. DuD – Datenschutz Datensicherheit 27(5) (2003)
9. Prosser, A., Müller-Török, R.: E-Democracy: Eine neue Qualität im demokratischen Entscheidungsprozess. Wirtschaftsinformatik 44(6), 545–556 (2002)
10. Prosser, A., Krimmer, R.: Proceedings of the ESF TED Workshop on Electronic Voting in Europe, GI Lecture Notes in Informatics P-47, Bonn 2004
11. Schlifni, M.: Electronic Voting Systems and Electronic Democracy: Participatory E-politics for a New Wave of Democracy. Dissertation, Technische Universität, Wien 2000
12. Schoenmakers, B.: A Simple Publicly Verifiable Secret Sharing Scheme and Its Application to Electronic Voting. Advances in Cryptology – Crypto 99, vol. 1666, Springer-Verlag, S. 148–164, 1999
13. van Acker, B.: Remote e-Voting and Coercion: a Risk-Assessment Model and Solutions, Proceedings of the ESF TED Workshop on Electronic Voting in Europe, Schloss Hofen/Bregenz, GI- Lecture Notes in Informatics P47, Bonn, S. 53–62, 2004
14. Volkamer, M., Meißner, N.: Anforderungskataloge für Online-Wahlen, 2005. http://www.dfki.de/fuse/AnforderungskatalogCC.ppt, abgerufen am 10.10.2005

Anhang – Übersicht der in Deutschland durchgeführten Wahlen

Tabelle 2

Deutsche Online-Wahlen im Überblick[a]

Name	Software	Jahr	Wahlform[b]	Authentifikation[c]	Anonymität[d]	Wahlbeteiligung	Zahl an teilnehmenden Wähler	Recht
Wahlsimulation „WK 329“	ivote	1998	R	–	B	–	17.000	☐
Vereine und Verbände	Wolff	1999	R	S	V	–	–	☐
TK Sozialwahl	ivote	1999	R	S	B	72%	1.000	☐
Studierendenwahl Osnabrück	ivote	2000	R&K	O	B	38%	356	☑
Personalratswahl LDS Brandenburg	ivote	2000	R	O	B	59%	329	☐
Abstimmung Mensaessen FH Hannover	FFH-Internetw@hl	2000	R	S	V	3%	150	☐
Studierendenwahl FH Hannover	FFH-Internetw@hl	2000	R	S	V	68%	220	☑
Virtueller Parteitag	Brokat	2000	R	S	V	100%	110	☑
Jugendgemeinderatswahl Esslingen	ivote	2001	–	O	B	–	34	☑
Komm'Un'W@hl des BDKJ Niedersachsen	ivote	2001	K	–	B	–	–	☐
neXTvote – ivote Landesjugendring Niedersachsen	ivote	2001	K	–	–	–	–	☐
Jugendgemeinderatswahl Fellbach	D-Trust, i-kom	2001	R&K	S	V	27%	444	☑
Jugendgemeinderatswahl Bobenheim-Roxheim	D-Trust, i-kom	2001	R&K	S	V	–	54	☐
Landratswahl im Kreis Marburg-Biedenkopf	KIV Hessen, Berminger Software, D-Trust	2001	R	S	–	–	–	☐
Hochschulwahl Universität Bremerhaven	ivote	2001	R&K	O	B	–	117	☑
Wahl zur Seniorenvertretung in Köln	Integrata (heute Unilog)	2001	K	S	–	–	–	☐
Jugendgemeinderatswahl Filderstadt	i-kom	2001	R&K	S	V	20,61%	354	☑
Personalratswahl LDS Brandenburg	ivote	2002	K	O	B	72%	385	☑

Fortsetzung

Name	Software	Jahr	Wahlform[b]	Authentifikation[c]	Anonymität[d]	Wahlbeteiligung	Zahl an teilnehmenden Wähler	Recht
Juniorwahlen zur Bundestagswahl	Polyas	2002	K	S	V	86%	58.000	☐
Betriebs- und Aufsichtsratswahl Webasto	ivote	2002	–	B	B	–	–	☑
Betriebsrat T-Systems CSM	ivote	2002	R&K	SO	B	–	1.777	☑
Betriebsrat der ivl GmbH	ivote	2002	–	–	–	–	–	☐
SPD-Parteitag Bochum	T-Vote	2003	K	–	B	–	–	☐
	T-Vote	2003	K	O	B	3%	3	☑
D21 Vorstandswahl	Polyas	2003	R	O	V	51%	54	☑
Hochschulwahlen Bremen	EUCyberVote	2003	K	O	H	20%	47	☑
Juniorwahlen zur Landtagswahl in Hessen	Polyas	2003	K	S	V	84%	5.800	☐
Juniorwahlen zur Landtagswahl in Bremen	Polyas	2003	–	–	V	88%	7.200	☐
Städte- und Gemeindebund Brandenburg	T-Vote	2004	K	S	B	–	270	☑
WSIS-Regierungsdelegation	GPL-WahlSW von Alvar Freude	2004	R	S	V	83%	30	☑
Gesellschaft für Informatik	Polyas	2004	K	S	V	24%	4.845	☑
Digitale Brücken	mimox-vote	2004	R	SO	–	100%	10	☑
Juniorwahlen zur Landtagswahl in Thüringen	Polyas	2004	K	S	V	86%	5.400	☐
Juniorwahl zur Landtagswahl in Brandenburg	Polyas	2004	K	S	V	83%	7.800	☐
Juniorwahlen zur Europawahl (Deutschland)	Polyas	2004	K	S	V	84%	42.000	☐
Sprecherausschusswahl – T-Systems international	T-Vote	2005	R	O	B	–	–	☑
Vorstandswahlen des Weimarer Kreises	ivote	2005	K	O	B	–	–	☑
Außerord. Betriebsratswahl – T-Systems international	T-Vote	2005	R	O	B	–	–	☑
Juniorwahlen zur Bundestagswahl 2005	Polyas	2005	K	S	V	90%	45.000	☐

Tabelle 2

Fortsetzung

Name	Software	Jahr	Wahlform[b]	Authentifikation[c]	Anonymität[d]	Wahlbeteiligung	Zahl an teilnehmenden Wähler	Recht
Betriebsratswahlen								
T-Systems (Nordbayern)	T-Vote	2005	R	S	B	–	–	☑
D21 Vorstandswahl	Polyas	2005	R	S	V	55,3%	57	☑
Gesellschaft für Informatik	Polyas	2005	R	S	V	20,1%	4.030	☑

[a] Die Tabelle inklusive Literaturangaben zu den einzelnen Projekten befindet sich auf der Seite http://www2.dfki.de/fuse/index.php?option=com_content&task=view&id=26&Itemid=42.onlinewahlenDeutschland.html, abgerufen am 28.11.2005.
[b] In dieser Spalte wird entsprechend dem Kapitel „Wahlformen" die eingesetzte Wahlform angegeben. Neben der reinen Remote-Online-Wahl wurden auch Wahlen mit Online-Wahl am Kiosk aufgenommen. Die Notation wird wie folgt verwendet: *R* bedeutet Remote-Online-Wahl, *K* bedeutet Online-Wahl am Kiosk, *R&K* ist die Kombination aus Remote-Online-Wahl und Online-Wahl am Kiosk.
[c] In dieser Spalte wird entsprechend dem Kapitel „Wählerauthentifizierung" die verwendete Art der Anonymisierung angegeben: *S* bedeutet: der Wähler erhält eine Wahl-TAN, *O* bedeutet: der Wähler hat oder erhält eine Chipkarte, *B* bedeutet: Wählerauthentifizierung mittels biometrischer Merkmale.
[d] In dieser Spalte wird entsprechend dem Kapitel „Anonymintät der Stimmabgabe" die verwendete Art an Anonymisierung angegeben: *V* entspricht der vorgelagerten Identifizierung, *H* entspricht der verdeckten Stimmauszählung, *B* entspricht der Pseudonymisierung mit blinden Signaturen.