

Notwendige technische Anforderungen an eVoting-Systeme für staatliche Volksvertreter-Wahlen

Peter Wilm

Universität Oldenburg
Department für Informatik
Abt. Wirtschaftsinformatik
Ammerländer Heerstr. 114-118
26129 Oldenburg
wilm@elektronische-wahlen.de

Abstract: Es wird ein Überblick über die technischen Anforderungen an eVoting-Systemen für staatliche Volksvertreter-Wahlen gegeben. Insbesondere wird auf notwendige Protokoll-Eigenschaften, sowie auf Aspekte der Implementierung von Voting-Systeme eingegangen. Dieser Beitrag basiert auf Erkenntnissen, die der Autor während des Entwurfs und Implementierung eines sicheren, skalierbaren und robusten Voting-Systems zur Entscheidungsfindung in großen Communities (bei nicht-staatlichen Wahlen) erzielt hat. Dieser Beitrag möchte eine Diskussion über die Konkretisierung von technischen Anforderungen an eVoting-Systemen für staatliche Volksvertreter-Wahlen anstoßen.

1 Aktuelle Situation

Spätestens seit dem Jahr 2001 verfolgt die Bundesregierung das Ziel, stufenweise Internet-basierte Volksvertreter-Wahlen einzuführen. Dazu wurde bereits im Oktober 2000 eine Arbeitsgruppe Online-Wahlen im Bundesinnenministerium eingerichtet [Kör01].

Des Weiteren hat die Forschungsgruppe Internet-Wahlen mit dem von ihr entwickelten System i-vote bis zum Mai 2003 bereits sieben Test-Wahlen (wie zum Beispiel Personalrats-Wahlen und Hochschulwahlen) durchgeführt [For03]. Bei dieser Forschungsgruppe handelt es sich um einen zentralen Stützweiler für die Bemühungen der Bundesregierung. Zwar wurden einige Arbeitsberichte veröffentlicht [For02], jedoch wird aus ihnen nicht die tatsächliche Architektur des Systems i-vote ersichtlich. Auch existieren keine formalen Anforderungsdefinitionen an das System.

Das jetzige Wahlsystem der Bundesrepublik Deutschland funktioniert hervorragend: Es basiert vor allem auf einer Dezentralisierung und einer vollständigen Transparenz für den Bürger. Ein Wahlbetrug ist äußerst schwierig vorzunehmen, da es einer Verschwörung einer ganzen Reihe von Wahl-Helfern bedarf. Zudem ist selbst bei einer erfolgreichen Verschwörung lediglich das Ergebnis einer einzelnen Wahl-Urne verfälschbar. Jeder Bürger

kann den Wahl-Vorgang zudem beobachten und hat somit die Möglichkeit, den korrekten Wahl-Ablauf in seinem Wahllokal persönlich zu verifizieren.

Die Glaubwürdigkeit der korrekten Durchführung der Wahl, der obligatorischen Einhaltung des Wahl-Geheimnisses, sowie der korrekten Ermittlung des Wahlergebnisses ist entscheidend für die Legitimation der bei dem Vorgang gewählten Staatsorgane verantwortlich.

Es ist somit nicht ausreichend, für einen korrekten Wahl-Ablauf und einer korrekten Ergebnis-Ermittlung zu sorgen. Jeder wahlberechtigte Bürger will von der Korrektheit überzeugt werden, soll das Ergebnis nicht nur vom Bundes- oder jeweiligem Landeswahlleiter, sondern auch allgemein anerkannt werden.

Dieser Artikel will zumindest eine Teilmenge der notwendigen technischen Anforderungen an ein eVoting-System ermitteln, soll es eine Qualität aufweisen, das dem jetzigen System ebenbürtig ist.

2 Notwendige technische Anforderungen

Art. 38 Abs. 1 Satz 1 GG [Par49] nennt fünf Anforderungen an eine Volksvertreter-Wahl: „Die Abgeordneten des Deutschen Bundestages werden in allgemeiner, unmittelbarer, freier, gleicher und geheimer Wahl gewählt.“

Es gibt einige Veröffentlichungen zu den rechtlichen Folgen der Vorgaben des Grundgesetz-Artikels für mögliche eVoting-Systeme. Hier sollen jedoch technische Implikationen aufgeführt werden.

2.1 Wahl-Geheimnis

ANF 1 Das Wahl-Geheimnis muss gewahrt werden. Niemand außer dem Wähler selber darf in Erfahrung bringen dürfen, was dieser gewählt hat.

Der Schutz des Wahl-Geheimnisses soll gegenüber Jedermann gelten:

ANF 2 Auch Administratoren des eVoting-Systems dürfen nicht die technischen Möglichkeiten haben, das Wahl-Geheimnis zu brechen.

Soll der Wähler seine Wahl frei von privatem und öffentlichem Druck abgeben können, so muss gewährleistet sein, dass es der Wähler nicht käuflich, oder erpressbar sein kann, er also seine Wahl nicht nachweisen kann.

ANF 3 Der Wähler darf nach dem Wahl-Vorgang nicht nachweisen können, was er gewählt hat (Quittungsfreiheit). Gibt ihm das System Informationen in die Hand, mit der er die Zählung seiner Stimme überprüfen kann, so muss mathematisch nachgewiesen worden sein, dass aus diesen Informationen keine Quittung über den Inhalt seines

Stimmzettels generiert werden kann. Dabei ist es unerheblich, ob der Wahl-Client vom Wahl-Amt signierte Informationen dem Wähler vorenthält. Es muss sichergestellt werden, dass der Wähler auch bei Manipulation seines Wahl-Clients keine Möglichkeit hat, in den Besitz einer durch eine an der Wahl beteiligten Instanz signierte Quittung seiner Wahl zu gelangen.

Beim heutigen Wahlsystem gilt das Wahl-Geheimnis zeitlich absolut. Dies sollte es bei einem neu einzuführenden eVoting-System zumindest für einen ausreichenden Zeitraum (von vielen Jahrzehnten), so dass auch Persönlichkeiten des öffentlichen Lebens keine Angst vor einer späteren Veröffentlichung ihres Abstimmungsverhaltens zu haben brauchen.

ANF 4 Es muss sichergestellt werden, dass auch bei einem Mitschnitt der Kommunikation zwischen Wahl-Client und Wahl-Amt ein potentieller Angreifer aller Voraussicht nach frühestens nach Ablauf einer Zeitspanne von vielen Jahrzehnten in den Besitz von Technologie gelangen können, um den Klartext des ermittelten Stimmzettels entschlüsseln zu können.

2.2 Korrektheit des Ergebnisses

ANF 5 Das System muss ein korrektes Ergebnis ermitteln.

Dazu muss jede wahlberechtigte Person einen Stimmzettel abgeben dürfen, jedoch nicht mehrfach wählen dürfen:

ANF 6 Das System muss exakt einen Wahlzettel pro wahlberechtigter Person pro Wahlgang annehmen.

Es ist davon auszugehen, dass bei einem derart großen System, auch bei Verwendung von besonders ausfallsicherer Hardware eine hohe Wahrscheinlichkeit besteht, dass Teilsysteme ausfallen. Dies darf das Wahlergebnis nicht beeinflussen. Es muss also bei einer redundanten Ausfall-Sicherung von Teilsystemen das übernehmende Teilsystem den Zustand des ausgefallenen Teilsystem on the fly und Bit-genau übernehmen.

ANF 7 Fällt ein beliebiges Teilsystem aus, so muss dessen Zustand exakt rekonstruiert werden können. Der plötzliche Totalausfall einer beliebigen Teilkomponente (z.B: zu simulieren durch das Ziehen sämtlicher Strom- und Netzwerkstecker) in einer beliebigen Situation darf das Wahlergebnis nicht um eine Stimme verändern. Jeder vom System angenommene Stimmzettel muss genau einmal gezählt werden.

Es ist ebenfalls davon auszugehen, dass Netz-Verbindungen zwischen dem Client-Rechner und den Wahl-Servern unterbrochen werden können:

ANF 8 Wurde ein Stimmzettel vom System nicht angenommen, so ist dies dem Wähler zweifelsfrei mitzuteilen. Er ist deutlich aufzufordern, die Wahl zu wiederholen.

Mögliche Missverständnisse, ob der Stimmzettel gezählt wurde oder nicht, sind unter allen Umständen auszuschließen.

Die Korrektheit des Wahlergebnisses darf nicht von der moralischen Integrität einzelner System-Administratoren abhängig sein.

ANF 9 Kein System-Administrator darf in der Lage sein, das Ergebnis zu manipulieren. Dazu muss es mindestens eine Verschwörung von n System-Administratoren bedürfen (bei vorab frei wählbarem n), falls nicht ein Wahl-Protokoll zum Einsatz kommen soll, dass eine universelle Verifizierbarkeit des Wahlergebnisses durch alle Wahlteilnehmer zulässt – in diesem Fall ist jedoch auf die Einhaltung von **ANF 3** zu achten.

Die Wahl-Server stellen für Außenstehende sicherlich ein besonders attraktives Angriffsziel dar.

ANF 10 Sämtliche Server der Wahl-Instanzen müssen einbruchsicher sein. Die gesamte eingesetzte Wahl-Software und sämtliche darunterliegende System-Software muss fehlerfrei sein. Dies muss nachgewiesen werden (zumindest durch exzessive vollständige Code-Audits). Reklame-Aussagen oder sogar eidesstattliche Versicherungen von Herstellern über deren System-Eigenschaften sind nicht ausreichend.

Das aktuelle Wahlrecht sieht in Zweifelsfällen Neuauszählungen vor. Dies macht für ein eVoting-System wenig Sinn, da im Falle einer Manipulation ebenso gut die gespeicherten Wahlzettel manipuliert worden sein können. Es besteht die Gefahr, dass durch die Möglichkeit von Neuauszählungen suggeriert wird, Zweifel am ermittelten Wahlergebnis seien minder gravierend, da das Ergebnis ja neu ermittelt werden könne.

ANF 11 Sollen Mehrfachauszählungen zwecks Wahlprüfungen zugelassen werden, so ist die Unmöglichkeit eines erfolgten Entfernens, Hinzufügens oder Manipulierens von Stimmzetteln mathematisch zweifelsfrei nachzuweisen. Dieser Nachweis ist gegenüber der Wahlprüfungskommission zu führen.

Um auch Fehlerquellen durch Hardware-Fehler auszuschließen muss gelten:

ANF 12 Ergebnisse sind so zu berechnen, dass selbst bei durch Hardware erzeugten Bit-Fehlern das Ergebnis nicht beeinflusst wird.

2.3 Client-Rechner-Sicherheit

Oftmals wird bei der Entwicklung von Prototypen von Internet-basierten eVoting-Systemen für staatliche Volksvertreter-Wahlen die Sicherheit der Clients vernachlässigt.

Unterschwellig wird damit argumentiert, dass durch einen Angriff auf den Wahl-Client maximal ein einzelner Stimmzettel gefälscht werden kann. Dies ist im Zeitalter von Viren,

Trojanern und Würmern jedoch nicht mehr der Fall. Attacken auf eine große Anzahl von Rechnern lassen sich automatisieren. Ist ein System angreifbar, so sind es mit nahezu konstantem Aufwand auch alle baugleichen.

Es muss also gelten:

ANF 13 Der Wahl-Client ist Teil des eVoting-Systems. Sämtliche Anforderungen an die Sicherheit des eVoting-Systems müssen auch durch den Wahl-Client erfüllt werden.

Um die Sicherheit des Clients zu gewährleisten, muss bei der heutigen Architektur der meisten Anwender-Rechner die Sicherheit in vier Bereichen kontrolliert werden:

1. Hardware – Die Hardware und ihre physische Sicherheit stellt die Grundvoraussetzung an ein sicheres System. Denkbare Angriffs-Möglichkeiten könnten u.a. Wanzen sein, die Tastatur-Eingaben per Funk weitergeben, Monitor-Abstrahlungen, die aufgezeichnet werden, oder Design-Fehler in der Architektur, die es Angreifern ermöglichen, Zugang zu Daten oder Kontrolle über Software zu erlangen.
2. BIOS – ursprünglich als „Basic Input Output System“ bezeichnet, war das BIOS ein System, das dem Betriebssystem eine einheitliche Schnittstelle zu unterschiedlichen Hardware-Produkten bieten sollte. Heute dient es dazu, den Boot-Loader eines Systems zu starten, der wiederum das Betriebssystem eines Rechners startet. Durch Bestrebungen der BIOS-Hersteller, ihre Produkte vor dem Aussterben zu bewahren, werden jedoch immer mehr Funktionalitäten in das BIOS eingebaut. So plant der Hersteller Phoenix eine Integration eines Web-Browsers in sein BIOS. Denkbar sind also in Zukunft möglicherweise auch Angriffs-Möglichkeiten auf das BIOS.
3. Betriebssystem und sonstige Software-Umgebung – Das Betriebssystem und sämtliche Software, die neben dem eigentlichen Voting-Client auf dem Rechner läuft ist ebenfalls angreifbar. Solange der Anwender seine sonstige Software nicht abgesichert hat und deren Funktionsweise bis ins Detail kennt, kann der Voting-Client keine Annahmen über seine Umgebung machen.
4. Anwendungssoftware – Die Voting-Client-Software selber bietet sicherlich die meisten Möglichkeiten eines Angriffs.

Oftmals wird beim Entwurf von Internet-basierten Voting-Systemen die Notwendigkeit der Gewährleistung der Sicherheit des Systems in den ersten drei Schichten nicht ernst genommen. Teilweise wird dem Wähler eine Java-Software zur Verfügung gestellt, dass dieser mit Hilfe seines Web-Browsers aus dem Internet laden muss und mit Hilfe seiner selbst installierten Java Virtual Machine ausführen muss. Dabei werden eine ganze Reihe von Annahmen über den Browser, die Java Virtual Machine und das Betriebssystem des Wählers gemacht. Jede dieser Komponenten kann jedoch bereits vorab von Angreifern manipuliert worden sein. Diese Manipulation könnte im großen Stil automatisiert erfolgen.

Das gleiche Risiko wird z.B. beim Online-Banking eingegangen. Die Bank und der Kunde verständigen sich dabei darauf, dass der Kunde ein ordentlich gewartetes System zur Verfügung stellt, auf dem er die Online-Banking-Software nutzt. Ist dies nicht der Fall und

entsteht ein Schaden durch einen Angreifer, so liegt dies in der Verantwortung des Kunden – nicht der Bank. Beim eVoting können die Verantwortungen nicht analog verteilt werden, da ein erfolgreicher Angriff nicht nur den einzelnen Wähler, dessen Stimmzettel manipuliert wurde, betrifft, sondern – erfolgt der Angriff bei einer Vielzahl von Wählern im großen Stil – den gesamten Staat schädigt. Es liegt also in der Verantwortung der Betreiber des Wahlvorgangs für eine ausreichende Sicherheit der Rechnersysteme der Wähler zu sorgen:

ANF 14 Es muss für eine ausreichende Sicherheit der Konfiguration des Rechners, auf dem die Wahl-Client-Software laufen soll gesorgt werden. Die Verantwortung hierfür liegt beim Betreiber der Wahl und nicht beim Wähler.

Zudem ist – um die Allgemeinheit der Wahl zu gewährleisten – dem Wähler nicht zuzumuten selbstständig Software- oder Hardware- Installationen oder -Konfigurationen an seinem Rechner vorzunehmen.

ANF 15 Soll der Wähler von beliebigen Rechnern aus wählen können (nicht nur von zuvor präparierten Wahl-Kiosken), so ist ihm dies zu ermöglichen, ohne dass Annahmen über seine Betriebssystem- oder Software-Konfiguration zu machen sind. Spezielle Web-Browser, Java Virtual Machines o.ä. sind nicht vorauszusetzen.

2.3.1 Smartcards

Seit einigen Jahren sind so genannte Smartcards oder Chip-Karten auf dem Markt. Es handelt sich um rechteckige Plastik-Karten, die das vertraute Format einer Kreditkarte, jedoch in ihrem Innern einen Mikrochip eingebaut haben. Dieser oder diese Mikrochip(s) verfügen über eine recht geringe Rechenleistung und ein klein wenig festen Speicher (ROM), Arbeitsspeicher (RAM), sowie veränderbaren Festspeicher (EPROM, EEPROM). Über auf der Oberfläche der Karte angebrachte elektrische Kontakte können derartige Karten mit der Außenwelt kommunizieren.

Smartcards sind zunächst prinzipiell universell einsetzbar. Sehr sinnvolle Einsatzmöglichkeiten sind die Verwendung als Zahlungsmittel, wie etwa als Telefonkarte und als Geldkarte der Sparkassen, als Authentifikationswerkzeug bei Türschlössern und als Speichermedium, wie etwa bei Versicherten-Karten, die die Krankenkassen in Deutschland ausgeben.

Vielfach wird der Einsatz von Chip-Karten zur Identifizierung des Wählers bei der Entwicklung von Voting-Systemen propagiert, oder sogar gefordert, wie durch die Initiatoren des Projektes i-vote /vgl. [Ott02]/. Im EU-Projekt Cybervote wird sogar der Einsatz von Chip-Karten zur Wähler-Identifizierung als Anforderung festgeschrieben /vgl. [Cyb00] S.19/, ohne dass die Notwendigkeit hierzu begründet wird.

Der Grund für diese Empfehlungen ist psychologischer Natur: Es erscheint zunächst enorm sicher, ein geschlossenes Hardware-Gerät einzuführen, das die Schlüssel des jeweiligen Wählers hält. Damit lässt sich dann natürlich sehr gut Marketing betreiben und potentiellen Wählern und auch Entscheidungsträgern zum Einsatz dieses Systems eine Sicherheit des angebotenen Voting-Systems suggerieren.

Technologisch gesehen bietet der Einsatz von Smartcards im Bereich der Wähler-Authentifikation bei elektronischen Wahlen, im Gegensatz zum Einsatz als elektronisches Zahlungsmittel, etc. jedoch keine zusätzliche Sicherheit gegenüber anderen Verfahren wie z.B. PIN/TAN-Verfahren dar. Zwar wird die Signatur auf der Chip-Karte selber vorgenommen, somit ist es nicht möglich, den Schlüssel, der auf der Chip-Karte ist, zu stehlen. Jedoch weiß der User immer noch nicht, was er signiert. Der Inhalt des Wahl-Zettels, der auf dem Bildschirm angezeigt wird, muss nicht mit dem Wahlzettel übereinstimmen, der signiert wird. Diese Annahmen können im Zeitalter von Trojanern, Viren und Würmern nur dann gemacht werden, wenn die Annahme, dass der Client-Rechner, an dem die Chip-Karte angeschlossen ist, ausreichend abgesichert ist, begründet werden kann. Bei privaten PCs ist dies nur in Einzelfällen der Fall, weshalb der Einsatz von Chip-Karten keine zusätzliche Sicherheit erbringt.

Sicherlich flößt es dem Wähler zunächst mehr Vertrauen in die Sicherheit ein, wenn er zur Wahl eine zusätzliche Hardware benötigt. Die Frage ist aber, was geschieht, wenn in der breiten Öffentlichkeit publik wird, dass die Sicherheit immer noch von der des angeschlossenen PCs abhängt. Das Vertrauen in das Voting-System könnte wohl deutlich abnehmen. Die Wirkung des Marketing-Effekts könnte somit also vorübergehend sein.

Um eine Client-seitige Sicherheit garantieren zu können, muss das gesamte System, auf dem das Ausfüllen des Wahl-Zettels vorgenommen wird, kontrolliert werden. Dies ist nicht mit einer reinen Chip-Karten-Lösung zu erreichen, dessen Einführung pro Wähler zudem beträchtliche Kosten verursacht.

2.3.2 Bootfähiges System auf CD

Eine Lösung für die Gewährleistung der Sicherheit des Betriebssystems, sowie der gesamten weiteren Software-Umgebung, ist das Starten des Voting-Clients von einer bootfähigen CD, die wohlkonfiguriert ist. Auf diese Weise ist die Wahl-Behörde in der Lage, die vollständige Software-Umgebung des Wählers zu kontrollieren. Dieser hat nicht mehr die Verantwortung, selber für die Sicherheit seiner Systemkonfiguration zu sorgen.

2.4 Verfügbarkeit

Um die Allgemeinheit der Wahl zu gewährleisten, muss gelten:

ANF 16 Den Wählern ist während des vollständigen Wahl-Zeitraumes der Wahl-Service ununterbrochen zur Verfügung zu stellen. Insbesondere sind technologische Gegenmaßnahmen zu Distributed Denial of Service-Attacken auf die Bandbreite der Internet-Anbindung der Wahl-Server, deren Prozessorlast und anderen System-Ressourcen vorzubereiten.

Da anzunehmen ist, dass es nicht möglich sein wird, eine Verfügbarkeit des Wahl-Services über den vollständigen Zeitraum mit absoluter Sicherheit zu garantieren, ist den Wählern

die Möglichkeit zu geben, im Notfall ein Wahl-Lokal nach fehlgeschlagenem Online-Wahlversuch persönlich zu besuchen:

ANF 17 Der Wähler muss die Möglichkeit haben, sich zu jedem Zeitpunkt des Wahl-Zeitraumes zwischen Online-Wahlen und Wahl in einem Wahl-Lokal zu entscheiden. Die Vernetzung der Wahl-Lokale zwecks Abgleich der Wählerlisten ist über dedizierte nicht-öffentliche Netzwerke (kein Internet, kein Virtual Private Network) vorzunehmen, um Distributed Denial Of Service-Attacken auf die Wahllokale auszuschließen.

Die Dezentralisierung des Wahlvorgangs ist zwar bei Papier-basierten Wahl-Systemen ein Sicherheitsvorteil, nicht jedoch bei Internet-basierten. Da anzunehmen ist, dass jedes dezentrale System eine ähnliche Funktionsweise hat, macht es also für einen Angreifer kaum einen Unterschied ein Zentral-System, oder automatisiert eine große Anzahl dezentraler Systeme anzugreifen.

Gleichwohl darf bei einer Dezentralisierung nicht der wesentlich erhöhte Arbeitsaufwand der Administration der dezentralisierten Systeme vernachlässigt werden.

ANF 18 Auch bei einer Dezentralisierung des Systems dürfen keine Ausfallzeiten entstehen. Eine lückenlose kompetente Administration muss auch bei gleichzeitigem Ausfall verschiedener Systeme in verschiedenen Wahllokalen gewährleistet sein.

2.5 Transparenz

Soll die Legitimation der gewählten Volksvertreter in den Augen der Wähler nicht durch den Einsatz eines eVoting-Systems leiden, so muss dessen Funktionsweise mindestens ebenso transparent sein wie die des jetzigen Systems.

Dabei geht es nicht darum, ob jeder Bürger tatsächlich jeden Aspekt des Systems nachvollzogen hat – die Frage ist, ob er es könnte. Sicherlich ist eine formale Bauart-Zulassung des Bundesinnenministeriums notwendig, bei der das Ministerium eine Reihe von Gutachten einholt. Dies ist jedoch nicht ausreichend, soll wirkliches Vertrauen in der Bevölkerung aufgebaut werden. Dies kann nur mit einer rückhaltlosen Offenlegung jedes System-Details geschehen.

ANF 19 Eine deutliche Zeit vor dem Beginn des Einsatzes eines eVoting-Systems sind

- die Anforderungsdefinition
- die Beschreibung der Architektur in verschiedenen Abstraktionsebenen und mit Erläuterungen für Personen mit unterschiedlichem Kenntnisstand
- die Beschreibung des eingesetzten Wahl-Protokolls
- eine umfassende Sicherheitsrisiko-Analyse
- der vollständige Source-Code der eVoting-Software

- der vollständige Source-Code der sonstigen verwendeten Software (Betriebssystem, Compiler, System-Tools, etc.)
- sämtliche Konfigurationsdateien der eVoting-Software und des Betriebssystems
- die exakten Spezifikationen der eingesetzten Hardware

für jedermann offen zugänglich gemacht zu werden.

Eine Geheimhaltung der eingesetzten Software und Systemkonfiguration wäre kontraproduktiv, da dadurch dem Bürger der Eindruck vermittelt würde, dass die involvierten Behörden selber der Auffassung sind, das System sei unsicher und nur mittels Minimierung des Personenkreises, der Zugriff auf die System-Informationen hat, abzusichern. Es stellte sich dann aber die Frage, wie hoch das Risiko sei, dass die eingeweihten Personen ihr Wissen über die System-Details nutzen, um Wahlen zu manipulieren und damit den Staat an einem seiner empfindlichsten Stellen zu treffen.

Auch muss die Möglichkeit vorgesehen werden, die öffentlich gemachte Systemkonfiguration zu überprüfen. Das heißt, es muss nachgewiesen werden, dass tatsächlich der Programmcode und die Konfiguration die publiziert wurde auf den entsprechenden Rechnern läuft.

ANF 20 Es muss interessierten Bürgern oder Organisationen die Möglichkeit eingeräumt werden, sich davon zu überzeugen, dass das eingesetzte eVoting-System Bit-genau mit dem übereinstimmt, von dem vorgegeben wird, dass es eingesetzt wird. Dabei ist sicherzustellen, dass bei diesen Überprüfungen eine Manipulation des Systems ausgeschlossen wird.

3 Ausblick

Die in diesem Beitrag beschriebenen Anforderungen stellen lediglich eine Teilmenge der absolut notwendigen technischen Anforderungen dar, die an ein eVoting-System für staatliche Volksvertreter-Wahlen zu stellen sind, soll sich die Qualität gegenüber dem jetzigen System nicht verschlechtern. Sicherlich gibt es noch weitere notwendige Anforderungen.

Es soll sich hierbei auch lediglich um eine Anregung handeln, vor dem Beginn konkreter Planungen für den Einsatz eines eVoting-Systems zu staatlichen Volksvertreter-Wahlen eine breite öffentliche Diskussion über die technischen Anforderungen zu führen, diese dann formal festzuhalten und vor dem Einsatz eines Systems dessen Features dann gegen die Anforderungsliste abzugleichen.

Systeme wie i-vote und Cybervote wurden als Prototypen für ein eVoting-System entwickelt, um die prinzipielle Machbarkeit eines solchen Systems zu erforschen. Keinesfalls waren sie für den Einsatz als Produktiv-System gedacht, oder sind dafür geeignet. Trotzdem besteht die große Gefahr, dass die Politik unter dem Druck, den Wahl-Vorgang modernisieren zu wollen, geneigt ist, einen derartigen Prototypen – nach dem Absolvieren einiger weiterer Test-Wahlen – als tatsächliches Produktiv-System einsetzen zu wollen.

Da es sich beim Wahlsystem um einen absolut vitalen Stützpfeiler für unser Staatssystem handelt, welches zur Zeit ausgezeichnet funktioniert, ist es von großer Bedeutung, dass dieses System nur durch ein gleichwertiges oder besseres ersetzt wird.

Dabei ist darauf zu achten, dass nicht nur die Sicherheit des Systems, sondern vor allem auch das Vertrauen der wahlberechtigten Bürger in die Sicherheit des Systems erhalten bleibt.

Aus diesem Grund ist es sehr wünschenswert, dass das Bundesinnenministerium im Falle der Entscheidung für den Einsatz eines eVoting-Systems (auch im Falle einer Entscheidung für eine stufenweise Einführung) einen transparenten Entwicklungsprozess wählt, an dessen Anfang die formale Definition der technischen Anforderungen an ein derartiges System steht.

Literatur

- [Cyb00] Cybervote. Report on mock-ups of architectures and overall system architecture. Technical Report D7 - Volume 2, Cybervote, 2000. <http://www.eucybervote.org> Stand: 03.08.2003.
- [For02] Forschungsgruppe Internetwahlen. i-vote Report - Chancen, Möglichkeiten und Gefahren der Internetwahl. Technical report, Forschungsgruppe Internetwahlen, 2002. <http://www.wahlkreis300.net/fgiw/uploader/data/Kurzfassung.pdf> Stand: 14.03.2003.
- [For03] Forschungsgruppe Internetwahlen. Strategische Initiative in der Bundesrepublik Deutschland: Wählen im Internet, 2003. <http://www.internetwahlen.de> Stand: 22.06.2003.
- [Kör01] Fritz Rudolf Körper. Voraussetzung für die Durchführung von Online-Wahlen, 2001. Rede des Parlamentarischen Staatssekretärs im Bundesministerium des Innern im Deutschen Bundestag am 11. Oktober 2001.
- [Ott02] Dieter Otten. *Modernisierung der Präsenzwahl durch das Internet*, chapter 5, pages 71–90. Online-Wahlen. Hubertus Buchstein, 2002.
- [Par49] Parlamentarischer Rat. Grundgesetz für die Bundesrepublik Deutschland, 1949. vom 23. Mai 1949 (BGBl. S. 1), zuletzt geändert durch Gesetz vom 26. Juli 2002 (BGBl. I S. 286).