Notwendige technische Anforderungen an e-Voting-Systeme für staatliche Volksvertreter-Wahlen

Peter Wilm, wilm@elektronische-wahlen.de
Universität Oldenburg, Abt. Wirtschaftsinformatik

Abstract: Dieser Beitrag möchte eine Diskussion über die Konkretisierung von technischen Anforderungen an e-Voting-Systemen für staatliche Volksvertreter-Wahlen anstoßen.

Das jetzige Wahlsystem der Bundesrepublik Deutschland funktioniert hervorragend: Es basiert vor allem auf einer Dezentralisierung und einer vollständigen Transparenz für den Bürger.

Die Glaubwürdigkeit der korrekten Durchführung der Wahl, der obligatorischen Einhaltung des Wahl-Geheimnisses, sowie der korrekten Ermittlung des Wahlergebnisses sind 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 akzeptiert werden.

Spätestens seit dem Jahr 2001 verfolgt die Bundesregierung das Ziel, stufenweise Internetbasierte Volksvertreter-Wahlen einzuführen. Dazu wurde bereits im Oktober 2000 eine Arbeitsgruppe Online-Wahlen im Bundesinnenministerium eingerichtet [Kör01]. Eine hohe Priorität muss bei der Systemeinführung die Abwehr von langfristigen Gefahren für das Wahlsystem haben, die besonders durch einen drohenden Vertrauensverlust der Bürger in das System gegeben sind. Verlockend könnte es z.B. sein, ein System wie das von der Bundesregierung geförderte i-vote der Forschungsgruppe Internetwahlen [Int03] zu verwenden, zu dem bisher weder formale Anforderungsdefinitionen, noch Architekturdetails veröffentlicht wurden, was einer Vertrauensbildung der Bürger in das System zuwiderläuft.

Im Folgenden werden notwendige Anforderungen genannt, die an ein e-Voting-System für staatliche Volksvertreter-Wahlen zu stellen sind, wenn sich die Qualität gegenüber dem jetzigen System nicht verschlechtern soll.

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

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

ANF 3 Der Wähler darf nach dem Wahl-Vorgang nicht nachweisen können, was er gewählt

hat (Quittungsfreiheit). Dies muss selbst bei Manipulation des Wahl-Clients durch den Wähler gewährleistet sein.

ANF 4 Es muss sichergestellt werden, dass auch bei einem Mitschnitt der Kommunikation niemand innerhalb einer Zeitspanne von vielen Jahrzehnten in den Besitz von Technologie gelangen könnte, um den Stimmzettel entschlüsseln zu können.

ANF 5 Das System muss ein korrektes Ergebnis ermitteln.

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

ANF 7 Fällt ein beliebiges Teilsystem aus, so darf dieses Ereignis das ermittelte Wahlergebnis nicht um eine Stimme verändern.

ANF 8 Wurde ein Stimmzettel vom System nicht angenommen, so ist dies dem Wähler zweifelsfrei mitzuteilen, damit dieser seinen Wahlversuch wiederholen kann.

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, falls nicht ein universell verifizierbares Wahl-Protokoll zum Einsatz kommen soll, welches dann jedoch die Einhaltung von **ANF 3** voraussetzt.

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.

ANF 11 Sollen Mehrfachauszählungen zwecks Wahlprüfungen zugelassen werden, so ist die Unmöglichkeit eines erfolgten Entfernens, Hinzufügens oder Manipulierens von Stimmzetteln mathematisch zweifelsfrei nachzuweisen.

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

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

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. (Einige Sicherheitsprobleme könnten durch den Einsatz von bootfähigen Client-CDs gelöst werden.)

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.

ANF 16 Den Wählern ist während des vollständigen Wahl-Zeitraumes der Wahl-Service ununterbrochen zur Verfügung zu stellen.

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.

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.

ANF 19 Eine deutliche Zeit vor dem Beginn des Einsatzes eines e-Voting-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 e-Voting-Software
- der vollständige Source-Code der sonstigen verwendeten Software (Betriebssystem, Compiler, System-Tools, etc.)
- sämtliche Konfigurationsdateien der e-Voting-Software und des Betriebssystems
- die exakten Spezifikationen der eingesetzten Hardware

für jedermann offen zugänglich gemacht zu werden.

ANF 20 Es muss interessierten Bürgern oder Organisationen die Möglichkeit eingeräumt werden, sich davon zu überzeugen, dass das eingesetzte e-Voting-System Bit-genau mit dem übereinstimmt, von dem vorgegeben wird, dass es eingesetzt wird.

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 Modifikationen an diesem System dessen Qualität nicht mindern. Es ist sehr wünschenswert, dass das Bundesinnenministerium im Falle der Entscheidung für die Einführung eines e-Voting-Systems einen transparenten Entwicklungsprozess wählt, an dessen Anfang die formale Definition der technischen Anforderungen steht.

Literatur

[Int03] Forschungsgruppe Internetwahlen. Strategische Initiative in der Bundesrepublik Deutschland: Wählen im Internet, 2003. http://www.internetwahlen.de.

[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.