



Workshop eDemocracy

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

Peter Wilm

wilm@elektronische-wahlen.de

02. Oktober 2003

Motivation

- Das jetzige Wahlsystem der BRD funktioniert hervorragend
 - kaum bekannte Wahlbetrugsfälle/Streitigkeiten
 - Enorme Transparenz für den Bürger in allen Phasen der Wahl
 - Dadurch praktisch vollkommenes Vertrauen der Wähler in Korrektheit des Wahlergebnisses
- Wahlsystem zentraler Stützpfeiler unseres Staatssystems
- Sicherheitsanforderungen, so dass die Qualität des aktuellen Systems zumindest erreicht wird.
- Vergleich Online-Banking – eVoting nicht statthaft!

Wahlgeheimnis

- 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 eVoting-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.

Korrektheit des Ergebnisses (1)

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.

Korrektheit des Ergebnisses (2)

ANF 9 Kein System-Administrator darf in der Lage sein, das Ergebnis zu manipulieren. Dazu muss es mindestens einer 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.

Korrektheit des Ergebnisses (3)

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.

Client-Rechnersicherheit

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.

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.

Verfügbarkeit

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.

Transparenz (1)

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.

Transparenz (2)

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.

Ende