International Working Group
on Data Protection
in Telecommunications

Arbeitspapier

Datenschutz und internetgestützter Stimmabgabe bei Wahlen zu Parlamenten und anderen staatlichen Einrichtungen[1]

angenommen bei der 30. Sitzung der Arbeitsgruppe am 28. August 2001 in Berlin

- Übersetzung -

Moderne Kommunikationstechnologien, insbesondere das Internet, können möglicherweise einen zusätzlichen Weg zur Vorbereitung und Erleichterung der Teilnahme an Wahlen auf örtlicher, staatlicher und weltweiter Ebene eröffnen. "Online Voting" (Stimmabgabe online), "Electronic Voting" (Elektronische Stimmabgabe) und "e-democracy" (Elektronische Demokratie) sind Schlagwörter in der jüngsten öffentlichen Diskussion. In einer Reihe von Ländern wird gegenwärtig der Rechtsrahmen verändert, um elektronische Abstimmungsmethoden zuzulassen. Universitäten und andere Körperschaften haben interne internetgestützte Wahlen für Vertretungskörperschaften von Studenten durchgeführt.

Zwei Formen der elektronischen Abstimmung können unterschieden werden:

- elektronische Abstimmung mit zertifizierter Hard- und Software in offiziellen Abstimmungslokalen ("Geschlossene" oder "Ende-zu-Ende-Systeme");
- elektronische Abstimmung von jedem Eingabegerät (z. B. private PC's, Handies) mit nichtzertifizierter Software ("Offene Systeme").

Die zweite Variante führt zu dem allgemeinen Problem der Briefwahl, da das Wahlgeheimnis nicht in der gleichen Weise in einer Privatwohnung oder am Arbeitsplatz gesichert ist wie in einer Abstimmungskabine.

Jede Technologie, die in diesem Zusammenhang eingesetzt wird, muss grundlegende verfassungsrechtliche Bedingungen für ein demokratisches Wahlverfahren erfüllen. Es ist allgemein akzeptiert, dass Wahlen zu Parlamenten und anderen staatlichen Einrichtungen frei, gleich und geheim sein müssen. Gleichzeitig muss das Wahlverfahren transparent und für die Öffentlichkeit überprüfbar sein.

Im Fall von bindenden Wahlen zu Parlamenten und anderen repräsentativen Körperschaften ist das Erfordernis des Wahlgeheimnisses entscheidend. Gleichzeitig muss das Wahlgeheimnis mit der Transparenz und Überprüfbarkeit des gesamten Wahlverfahrens in Einklang gebracht werden. Die

[1] Das Arbeitspapier beschränkt sich auf Wahlen zu repräsentativen Körperschaften und öffentlichen Ämtern. Der Begriff "staatlich" umfasst alle (also legislative, exekutive und justizielle) Zweige der Staatsorganisation.

Secretariat
Berliner Beauftragter für
Datenschutz und Informationsfreiheit
An der Urania 4- 10
D-10787 Berlin
Phone +49 / 30 / 13889 0
Fax: +49 / 30 / 215 5050

E-Mail:
IWGDPT@datenschutz-berlin.de

Internet:
http://www.berlin-privacy-group.org

The Working Group has been initiated
by Data Protection Commissioners
from different countries in order
to improve privacy and data protection
in telecommunications and media

Erfahrung der Überwachung und Manipulation von Wahlen in nichtdemokratischen Staaten hat unterstrichen, dass die Vertrauenswürdigkeit jedes politischen Systems hier auf dem Spiel steht. Während papiergestützte Wahlen transparent sind, trifft dies für elektronische Wahlverfahren nicht in gleicher Weise zu. Elektronische Abstimmungsverfahren können sogar sicherer sein als konventionelle Abstimmungsmethoden. Die Wahl muss aber nicht nur sicher sein, sondern ihre Sicherheit muss auch sichtbar werden. Verschlüsselungsmethoden (z. B. blinde Signaturen) und die informationelle Trennung von Befugnissen und Funktionen (informationelle Gewaltenteilung) zwischen Rechnern, die die Wahlberechtigung überprüfen und die Stimmen sammeln und zählen, werden gegenwärtig diskutiert. Sie sind äußerst komplex, müssen aber zugleich einen Ausgleich für den Mangel an Transparenz schaffen. Diese Vorschläge werden sorgfältig zu prüfen und öffentlich zu diskutieren sein. Da das Vertrauen der Wählerschaft für den demokratischen Prozess entscheidend ist, sollte hier mit erheblicher Vorsicht vorgegangen werden. Die US-Präsidentschaftswahlen 2000 haben die bei der Abstimmung eingesetzte Technik zum Gegenstand einer intensiven öffentlichen Auseinandersetzung gemacht. Öffentlicher Unmut kann entstehen, wenn die bei Abstimmungen eingesetzte Technologie nicht vertrauenswürdig ist oder den Willen der Öffentlichkeit bei Abstimmungs-, Zähl- und Prüfverfahren zu vereiteln scheint.

Die Arbeitsgruppe gibt deshalb die folgenden Empfehlungen:

1. Die komplizierten technischen Fragen bezüglich der Verlässlichkeit einschl. der Sicherheit und Verfügbarkeit von elektronischen Wahlsystemen (Schutz gegen unbefugten Zugriff und Überflutungsangriffe) sollten beantwortet werden, bevor ein derartiges System bei Wahlen zu gesetzgebenden oder anderen staatlichen Körperschaften auf irgendeiner Ebene eingesetzt wird; diese Systeme sollten einer gründlichen Risikoanalyse und Testverfahren unterzogen werden[2].

2. Authentifizierungsverfahren für Wähler bei elektronischen Abstimmungen, die vor der Stimmabgabe eingesetzt werden, um das Wahlrecht zu prüfen, eine mehrfache Stimmabgabe zu unterbinden und gleichzeitig das Wahlgeheimnis zu sichern, sollten nicht weniger sicher sein als die Verfahren, die bei papiergestützten Abstimmungen angewandt werden.

3. Während das System einerseits den Wähler warnen sollte, wenn die Stimme nicht registriert oder korrekt übermittelt worden ist, muss andererseits eine quittungsfreie Stimmabgabe sichergestellt sein, um die Gefahr der Beeinflussung zukünftiger Wähler und der Erpressung solcher Personen, die ihre Stimme abgegeben haben, zu verringern. Eine Zwischenspeicherung oder elektronische Registrierung von individuellen abgegebenen Stimmen sollte nach ihrer Zählung nicht zugelassen werden.

4. Die gesamte Hard- und Software einschl. des Quellcodes muss dokumentiert und einer Prüfung zugänglich gemacht werden.

5. Vertrauenswürdige Zertifizierungsverfahren für Hard- und Software müssen eingesetzt werden.

---

[2] Neuere Forschungsergebnisse in den Vereinigten Staaten deuten darauf hin, dass es zumindest 10 Jahre dauern kann, bevor dieses Ziel erreicht ist; vgl. den Bericht des California Institute of Technology/Massachusetts Institute of Technology, Voting Technology Project, Voting - What Is – What Could Be, July 2001, http://www.vote.caltech.edu/Reports/index.html