E-Voting-Systeme: für mehr Transparenz

Die heutigen Internettechnologien ermöglichen neue Formen des Einbezugs der Bürgerinnen und Bürger in die politischen Entscheidungsprozesse. Informationsverbreitung, E-Petition und E-Voting wecken die Hoffnung auf eine aktivere Beteiligung der Bevölkerung und vereinfachen die Mitwirkung, insbesondere für Auslandschweizerinnen und -schweizer. Aus grundsätzlichen Sicherheitsüberlegungen und um den Gefahren im Internet zu begegnen, fordern wir aber, dass E-Voting-Systeme transparent sind.

Eric Dubuis, Stephan Fischli, Rolf Haenni

Prof. Dr. Eric Dubuis
Research Institute for Security in the Information Society
Berner Fachhochschule
eric.dubuis@bfh.ch

Prof. Dr. Stephan Fischli
Research Institute for Security in the Information Society
Berner Fachhochschule
stephan.fischli@bfh.ch

Prof. Dr. Rolf Haenni
Research Institute for Security in the Information Society
Berner Fachhochschule
rolf.haenni@bfh.ch

Mit dem Internet ergeben sich neue Möglichkeiten, die Bürgerinnen und Bürger in die politischen Entscheidungsprozesse aktiv einzubeziehen. Diese Art der Nutzung der Internettechnologien wird unter dem Begriff E-Demokratie zusammengefasst. Dabei unterscheidet man drei verschiedene Stufen. Die erste ist diejenige der Informationsverbreitung mit sogenannten «Push»-Verfahren (Mail, Newsletter) oder sozialen Netzwerken (Facebook, Twitter). Die Sicherheitsanforderungen dieser Stufe sind relativ gering; es genügt, die Authentizität der Informationen sicherzustellen. Bei der zweiten Stufe, der E-Partizipation, beteiligen sich die Bürgerinnen und Bürger aktiv am politischen Entscheidungsprozess, indem sie ihre Meinung in mehr oder weniger verbindlicher Form kundtun. Bei dieser Stufe sind die Sicherheitsanforderungen etwas höher, denn je nach Art der Partizipation muss sichergestellt werden, dass die Bürgerinnen und Bürger Regeln befolgen wie beispielsweise das einmalige Unterzeichnen einer Initiative oder eines Referendums.

Bei der dritten Stufe, dem sogenannten E-Voting, nehmen die Bürgerinnen und Bürger übers Internet an rechtlich bindenden Wahlen oder Abstimmungen teil. Nebst dem offenbaren Nutzen des E-Votings (Komfort, erleichterter Zugang) sehen viele Fachleute auch Gefahren wie diejenigen der einfacheren Manipulation von Stimmen und der Verletzung der Geheimhaltung. Deshalb ist es nicht erstaunlich, dass die Sicherheitsanforderungen an die Systeme der dritten Stufe am höchsten sind. Im Folgenden treten wir auf einige dieser Sicherheitsanforderungen ein und zeigen die Schwierigkeiten bei deren Umsetzung. Daraus leiten wir die Forderung der Transparenz von E-Voting-Systemen ab.

Einfache Anforderungen – einfacher Prozess

Das Wählen und Abstimmen gehört zu den Grundrechten in einer Demokratie und ist in entsprechenden Verfassungs- und Gesetzestexten verankert. Aus diesen ergeben sich folgende Grundprinzipien:

- Nur berechtigte Personen dürfen stimmen.
- Eine berechtigte Person kann maximal eine Stimme abgeben.
- Jede korrekt abgegebene Stimme wird gezählt.
- Die Stimme ist geheim.
- Das Resultat bleibt bis zum Ende der Wahl oder Abstimmung geheim.

Diese Grundprinzipien lassen sich mit Stimm- oder Wahlzettel und dem klassischen Wahllokal mit Wahlkabine relativ einfach bewerkstelligen. Der Ablauf, der von Wahlbeobachtern oder anderen interessierten Personen überwacht werden kann, lässt sich in drei Phasen aufteilen:

- In der ersten Phase werden mit dem Stimmregister die Stimmberechtigten festgelegt, die Stimmausweise gedruckt und den Stimmbürgerinnen und -bürgern verschickt.
- In der zweiten Phase geben die Stimmberechtigten ihre Stimme im Wahllokal ab (siehe Abbildung 1). Der vorgelegte Stimmausweis zeigt, dass eine Person wahl- oder stimmberechtigt ist. Das Stimmgeheimnis wird durch das Ausfüllen des Stimmzettels in der Wahlkabine gewahrt, und der Wahlhelfer bei der Urne garantiert schliesslich, dass jede beziehungsweise jeder Stimmberechtigte nur eine Stimme in die Urne legt.
- Nach Ablauf des Wahl- oder Abstimmungsvorgangs wird durch die Mitglieder der Wahlkommission der Inhalt der Urne ausgezählt und das Ergebnis publiziert.

Mit dem Internet wird es schwieriger

Das Abstimmen übers Internet macht alles komplizierter. Wir greifen zwei Probleme heraus. Das erste ist die scheinbare Unvereinbarkeit des Stimmgeheimnisses mit der Forderung, dass nur berechtigte Personen stimmen dürfen. Denn um Letzteres zu erreichen, muss das E-Voting-System die Stimmbürgerin oder den Stimmbürger zuerst identifizieren. Das E-Voting-System «kennt» also die Person und könnte somit die abgegebene Stimme mit der entsprechenden Identität verknüpfen. Gerade dies muss aber verhindert werden, um das Stimmgeheimnis zu wahren.

Ein anderes Problem ist die fehlende Transparenz. Bei vielen E-Voting-Systemen werden die abgegebenen Stimmen irgendwo gespeichert und sind anschliessend nicht mehr öffentlich einsehbar. Somit lässt sich weder überprüfen, ob nur berechtigte Stimmen im E-Voting-System gezählt werden, noch, ob die Stimmen nachträglich manipuliert worden sind.

Transparenz schafft Vertrauen

Transparenz bedeutet, dass die Bürgerinnen und Bürger sehen, was mit ihren Stimmen passiert, und dass sie nachprüfen können, ob das Wahlergebnis korrekt ermittelt worden ist. Diese beiden Eigenschaften nennt man auch individuelle und universelle Verifizierbarkeit. Mit der physischen Abgabe des Stimm- oder Wahlzettels an der Urne im Wahllokal hat man die Gewähr, dass die Stimme unverfälscht erfasst wird. Beobachtet man in der nachfolgenden Phase die Auszählung (viele Wahlgesetze und -verordnungen lassen dies zu), so ist man am Ende von der korrekten Ermittlung des Ergebnisses überzeugt. Unter Transparenz versteht man zudem die Möglichkeit, festzustellen, ob sich nur Stimmen in der Urne befinden, die von berechtigten Stimmenden abgegeben worden sind. Dass dies nicht nur ein Problem der E-Voting-Systeme ist, zeigen jüngste Diskussionen um Wahlergebnisse im Ausland.

Die Transparenz von Wahlsystemen ist wichtig, damit auch bei einem knappen Ergebnis keine Zweifel an der korrekten Durchführung aufkommen und dieses auch von der unterlegenen Partei akzeptiert wird. Andererseits ist Transparenz auch für die Administration, welche die Abstimmung oder Wahl durchführt, wichtig. Denn sollte jemand Zweifel an der korrekten Durchführung haben, so können dank der Transparenz die Ergebnisse vollständig nachgeprüft werden. Wie aber lässt sich Transparenz in E-Voting-Systemen bewerkstelligen, wenn man doch nicht in die Computer «hineinsehen» kann?

Kryptografie und öffentlich einsehbare Anschlagbretter

Für die Gewährleistung der Sicherheit werden Methoden der modernen Kryptografie eingesetzt. Transparenz wird dadurch erreicht, dass die Daten in jeder Phase der Abstimmung übers Web einsehbar sind, wobei kritische Daten verschlüsselt werden. Wir unterscheiden drei verschiedene Verfahren:

Beim Verfahren mittels *blinder Signaturen* erzeugen die Stimmberechtigten ein geheimes Pseudonym und lassen es von der Wahlbehörde blind signieren. In einem zweiten Schritt verschlüsseln sie die Stimme und schicken sie, zusammen mit dem signierten Pseudonym, an die übers Web jederzeit einsehbare Urne. Den Schlüssel schicken sie an den Kollektor (eine Art Schlüsselbrett). Am Ende des Wahlvorgangs werden die Stimmen mit den Schlüsseln des Kollektors entschlüsselt und gezählt. Das Ergebnis kann von allen Beteiligten verifiziert werden.

Beim Verfahren mittels *homomorpher Verschlüsselung* entfällt die komplexe Aufgabe der Trennung der Stimme von der Identität des Stimmenden. Die Stimme wird vom Stimmenden verschlüsselt – und bleibt verschlüsselt, auch beim Zählen.

Beim Verfahren mit sogenannten *Mixnetzwerken* werden die abgegebenen, verschlüsselten Stimmen von ihren Identitäten getrennt, mehrfach hintereinander von unabhängigen Instanzen gemischt und neu verschlüsselt. Dabei wird durch entsprechende kryptografische Beweisverfahren garantiert, dass das Mischen der Stimmen korrekt durchgeführt wurde. Am Ende des Mixnetzwerkes können die resultierenden, verschlüsselten Stimmen nicht mehr mit den ursprünglichen Identitäten in Verbindung gebracht werden. Das heisst, sie können gefahrlos entschlüsselt und zusammengezählt werden.

E-Voting an der BFH

Aus unserer Sicht ist es nur eine Frage der Zeit, bis E-Voting-Systeme in weiteren Kantonen und ohne die 10%-Beschränkung eingesetzt werden. Bis es so weit ist, wird die E-Voting-Gruppe der Berner Fachhochschule die Zeit nutzen, um zu klären, ob und wie transparente E-Voting-Systeme in der Schweiz eingesetzt werden könnten. Nebst der Beantwortung von technischen und ergonomischen Fragestellungen gilt es auch, die rechtlichen Aspekte von E-Voting zu berücksichtigen. Für Letzteres stehen wir in engem Kontakt mit der Schweizerischen Bundeskanzlei.

Am 6. September 2010 organisiert die E-Voting-Gruppe der Berner Fachhochschule in Zusammenarbeit mit der Schweizerischen Bundeskanzlei und der Universität Fribourg die zweite Ausgabe des *Swiss E-Voting Workshop* (siehe http://www.e-voting-cc.ch). Verschiedene international renommierte Referenten werden über den aktuellen Stand der Forschung im Bereich der elektronischen Abstimmungen berichten. Den Fokus der diesjährigen Veranstaltung bilden existierende E-Voting-Systeme, welche die im Artikel genannte Transparenzeigenschaft aufweisen und sich dadurch grundsätzlich von den in der Schweiz eingesetzten Systemen unterscheiden.

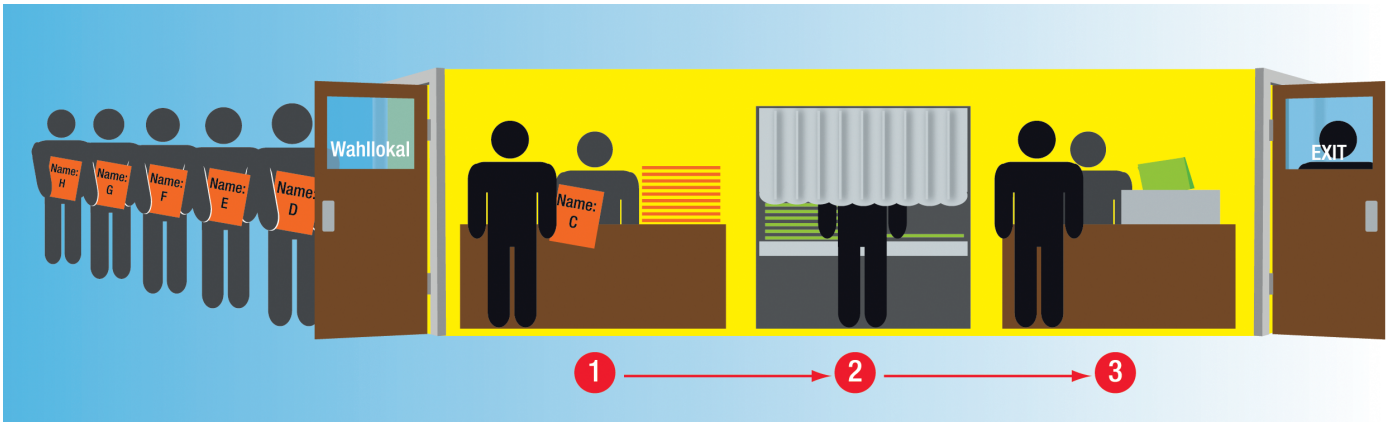

Abbildung 1: Der oder die Stimmberechtigte gibt den Stimmausweis dem Wahlhelfer ab (1). Danach geht er oder sie in die Wahlkabine (2), füllt einen leeren Stimmzettel aus, faltet ihn und verlässt die Wahlkabine. Er oder sie geht zur Urne und legt den Stimmzettel hinein (3) und verlässt danach das Wahllokal