

E-Voting:

Vom Wahlmaschinen-Debakel zum europäischen Sicherheitsstandard

Ein Bericht über die OCG-Tagung „Electronic Voting in Europe“, 7.-9. Juli 2004, Schloss Hofen, Brenz

MAG. ROBERT KRIMMER, AO. UNIV.-PROF. DR. ALEXANDER PROSSER

Forschung braucht internationale Vernetzung und Diskussion, gerade in einem neuen Forschungsfeld wie der elektronischen Durchführung von Wahlen. Aus diesem Grund veranstaltete der Arbeitskreis „e-Democracy/e-Voting“ der OCG die Tagung „Electronic Voting in Europe“, die auch von der European Science Foundation ESF gefördert wurde.

Vortragende aus elf europäischen Staaten, den USA sowie Vertreter des Europarates diskutierten Chancen und Risiken der elektronischen Stimmabgabe, vor allem aber das breite Spektrum an Ausgestaltungsmöglichkeiten. Die diskutierten Systeme reichten von Wahlmaschinen für den Einsatz in der Wahlzelle über Kiosksysteme bis hin zur Internet-basierten Stimmabgabe.

Dabei wurde den Teilnehmern auch die Vielgestaltigkeit der europäischen Wahlsysteme bewusst gemacht: Wahlordnungen ohne anonyme Stimmabgabe, bei der Wählende nachvollziehbar sein muss, mehrfache Stimmabgabe, wobei die jeweils letzte Stimme zählt, vorzeitige Stimmabgabe, Stimmabgabe durch einen Vertreter und verschiedene Ausgestaltungsvarianten der Briefwahl, um nur einige Beispiele zu nennen. Hinzu kommen unterschiedliche Traditionen und Einstellungen zu Aspekten des Wahlrechts, etwa am Beispiel der Briefwahl: Während in einigen Ländern die voraussetzungslose Briefwahl gilt, und die Mehrzahl der Stimmen auch im Inland über diese abgegeben wird, steht in anderen Staaten vorrangig die Präsenzwahl solchen Überlegungen entgegen.

In der Diskussion zeigte sich, dass die

Rechtswissenschaften und die Politik den Rahmen und die Anforderungen auch im internationalen Kontext vorgeben und es dann an der Forschung im Bereich Kryptographie liegt, diese Anforderungen abzubilden. Schließlich ist es Aufgabe der IT-Implementierung, die definierten Verfahren methodisch sauber abzubilden.

Letzteres ist nicht losgelöst vom kryptographischen Hintergrund zu sehen, wie aktuelle Beispiele zeigen: So schrieb etwa ein bekannter US-amerikanischer Wahlmaschinen-Hersteller seine geheimen privaten Kryptoschlüssel in den Source-Code – ein Beispiel, wie durch die „naive“ Implementierung kryptographischer Verfahren die angestrebte Sicherheit wieder zunichte gemacht werden kann.

Die Tagung war daher bewusst interdisziplinär zwischen Recht, Politik, Kryptographie und IT-Implementierung angesiedelt, was auch am fachlichen Hintergrund der rund 50 Teilnehmer zu merken war. Auch zahlreiche potenzielle „Anwender“ von E-Voting aus dem öffentlichen Bereich nahmen teil. Dies spiegelte sich auch in den beiden Keynotes wider.

Die Keynotes wurden von Michael Remmert (E-Voting-Koordinator im Europarat) und Christian Rupp (E-Government-

Exekutivsekretär im Bundeskanzleramt) gehalten. Michael Remmert ging dabei insbesondere auf die am Vortag verabschiedete Draft Recommendation für das Ministerkomitee des Europarates zum Thema E-Voting ein. Nach Verabschiedung wird diese Empfehlung die europaweiten Minimalstandards für E-Voting-Systeme definieren, wobei die Standards sehr anspruchsvoll gestaltet wurden, um ein Maximum an Sicherheit und Transparenz im verwendeten System sicherzustellen. Gleichzeitig werden auch Empfehlungen gegeben, um die Interoperabilität von Systemen auch über nationale Initiativen hinweg sicherzustellen.

Christian Rupp schilderte in seiner Keynote Speech die Positionierung von E-Voting im Rahmen des österreichischen E-Government Masterplans, wobei mit der Existenz der Bürgerkarte bereits ein wesentlicher Baustein für Internet-Voting, nämlich Identifizierung und Authentisierung des Wählenden im Internet, vorhanden ist. Rupp betonte auch die Wichtigkeit einer einfachen und intuitiven Benutzbarkeit sowie der barrierefreien Gestaltung eines solchen Systems; nur so können der „Digital Divide“ überwunden und die breite Akzeptanz sichergestellt werden.

In den Fachvorträgen wurden Implementierungen aus verschiedenen europäischen Staaten und Erfahrungen aus Feldversuchen und Pilotprojekten diskutiert; die Forschungsgruppe „e-Voting.at“ der Wirtschaftsuniversität präsentierte die an der WU durchgeführten Wahltests und den dahinter stehenden Prototypen. Christopher Soghoian (Forschungsgruppe Avi Rubin, die vielen aus der Diebold-Wahlmaschinen-Debatte bekannt ist) berichtete über die aktuelle Sicherheitsdiskussion in den USA.

Dabei kristallisierten sich sehr rasch die entscheidenden Erfolgsfaktoren für E-Voting heraus:

Wahlrechtsgrundsätze

Als wichtigster Entwicklungsgrundsatz für E-Voting-Systeme stellte sich die Garantie der Einhaltung der Wahlrechtsgrundsätze durch transparente technologische Sicherungen heraus.

Zweifache Nachvollziehbarkeit der Wahl

Die Wahl muss für die Wahlkommission in jedem Schritt nachvollziehbar und das Ergebnis jederzeit transparent reproduzierbar sein.

Gleichzeitig muss der Wählende die Möglichkeit haben, nachzuprüfen, ob seine Stimme korrekt und ohne Veränderung übermittelt und gezählt wurde; diese Forderung wird international unter dem Schlagwort „voter-verifiable audit trail“ erhoben. Dabei darf es jedoch nicht möglich sein, dass der Wähler einem Dritten gegenüber beweisen kann, wie er gewählt hat. Dies würde Stimmenkauf ermöglichen.

Diese zweifache Nachvollziehbarkeit zu realisieren, ist eine der wesentlichen Forschungsaufgaben im Bereich E-Voting, der sich die Forschungscommunity wird stellen müssen.

Nachvollziehbarkeit der Programmierung

Für den Wählenden sind ein E-Voting-System und dessen Sicherungen wesentlich schwerer zu durchschauen als ein konventionelles Wahlsystem. Vertrauen bedingt hier maximale Transparenz. Dies bedeutet im Konkreten:

- die Offenlegung des Source Codes durch die Entwickler (Open Source)
- die Zertifizierung anhand internationaler Standards (Common Criteria)
- die Signierung des zertifizierten Codes durch die Zertifizierungsbehörde, was dem Wählenden die Sicherheit gibt, dass er im Augenblick der Wahl auch tatsächlich den korrekten Code verwendet.
- die Offenlegung des wirtschaftlichen Hintergrunds entsprechender Soft-

wareanbieter; so sind Medienberichten zufolge einige US-amerikanische Hersteller auch bedeutende Parteispender. Europäische Projekte im Bereich E-Voting werden hingegen meist von Universitäten betrieben und haben daher einen neutralen Hintergrund.

Schutz vor Viren und Trojanern

Bei E-Voting über Internet ist das Wahlterminal der PC des Wählenden, der aber Viren, Trojanern und anderen Schadprogrammen ausgesetzt und oft nur mangelhaft gesichert ist. Derartige Schadprogramme können für das Ausspionieren oder die Manipulation von Stimmen verwendet werden. Unter diesen Bedingungen ist E-Voting nur sehr schwer vorstellbar.

Als ein Lösungsansatz wurde der Einsatz von Smart Cards vorgeschlagen, etwa einer digitalen Signaturkarte. Dabei wurden die sensiblen Teile des E-Voting-Protokolls in die Smart Card verlagert. Diese stellte daher nicht nur die Authentisierung des Wählenden über das Internet bereit, sondern diente dann auch als Trägermedium für das Wahlprotokoll.

Stufenweiser Erfahrungsaufbau

Niemand wird ernsthaft vorschlagen wollen, ohne vorherige ausführliche Tests E-Voting für rechtsgültige Wahlen einzusetzen. Der Erfahrungsaufbau erfolgt über unverbindliche Feldversuche und Usability-Labors, Wahltests parallel zu echten Wahlen bis hin zur realen E-Wahl. Hier leistet ein nationaler Aktionsplan wertvolle Orientierung. Die Erfahrung zeigt, dass selbst finanziell hochdotierte einzelne Pilotprojekte eine solche nationale Strategie nicht ersetzen können.

Der Best Paper Award des Program Committee ging an Anne-Marie Oostveen und Peter van den Besselaar für ihr Paper über „Security as Belief: User Perceptions on Security of E-Voting Systems“, in dem über eine in mehreren europäischen



li: Mag. Robert Krimmer, Chair Local Organising Committee, re: Ao. Univ.-Prof. Dr. Alexander Prosser, Chair Program Committee



Die wunderschöne Kulisse von Schloss Hofen, Bregenz

Staaten parallel durchgeführte Studie berichtet wurde, in der mit einem E-Voting-System Wählende angeben sollten, wie sicher sie verschiedene Aspekte des Systems beurteilen. Diese Beurteilung wurde mit den tatsächlichen (und für den Benutzer auch durchaus erkennbaren) Sicherheitsparametern verglichen.

Aufgrund des sehr positiven Echos der Teilnehmer und der Entwicklungen auf diesem Gebiet wurde für 2.-4. August 2006 bereits die „2nd International Conference on Electronic Voting in Europe“ avisiert. Auf Grund der perfekten lokalen Organisation und der Vorarlberger Gastlichkeit war man sich über den Ort dieser Nachfolgetagung rasch einig: es wird wieder Schloss Hofen bei Bregenz sein. ■

Weitere Informationen

Alle Beiträge erschienen zur Konferenz in einem Tagungsband, der im Rahmen der Lecture Notes in Informatics (LNI) der Gesellschaft für Informatik erschienen ist. Alle Vorträge und Information zum Bezug des Tagungsbands finden sich auch auf

<http://www.e-voting.at/ted>