Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundeskanzlei BK
Kompetenzzentrum Amtliche Veröffentlichungen KAV

Daniel Gabi 09.06.2009

Transkript des Podium des Swiss E-Voting Workshop, Münchenwiler, 5.6.2009

Untertitel

16.00–16.30

Systèmes de vote électronique ouverts et transparents pour la Suisse: une utopie?

Moderator: Peter Fischer, Delegierter Informatikstrategieorgan Bund

Panel: *Prof. Dr. Rüdiger Grimm*
Dr. Wolter Pieters
Dr. Martin Hirt
Michel Warynski
Danilo Rota
Dr. Felix Bosshard

Das Panel ist interdisziplinär aufgestellt; es wurden verschiedene Sprachen gesprochen. Dauer: 35'

Während die ersten drei Panelteilnehmer die theoretische Seite und die Forschung vertreten,

- *Prof. Dr. Rüdiger Grimm: IT-Risk Management, Universität Koblenz-Landau*
- *Dr. Wolter Pieters: Information Security, University of Twente*
- *Dr. Martin Hirt: Kryptographie, ETH Zürich*

Vertreten die weiteren Panelteilnehmer die aktuell im Einsatz stehenden E-Voting-Systeme.

- *Michel Warynski (E-Voting-System GE)*
- *Danilo Rota (E-Voting-System NE)*
- *Dr. Felix Bosshard (E-Voting-System ZH)*

E-Wahl-Vertrauen?

Was ist es, was die Panelteilnehmer derart gelassen, ja beinahe schon unterhaltsam diskutieren lässt? Fatalismus, oder doch eher Optimismus, der aber noch etwas auf sich warten lässt; vielleicht die insgeheime Vermutung, kurz vor dem grossen Wurf zu stehen? Oder doch eher die Abwesenheit der Juristen? Und welchen Einfluss hatte die Abwesenheit von politischen Amtsträgern auf das Panel? Die Vertreter aus Wissenschaft, Forschung und Praxis stellten jedenfalls klar, dass sie nicht die Absicht haben, sich für ein Amt (der Exekutive in ihrer Gemeinde) aufstellen zu lassen. Die Vertreter der zur Zeit in den Kantonen bei Pilotabstimmungen[1] eingesetzten E-Voting-Systeme würden einer Wahl, welche ausschliesslich über solche elektronischen Wahl- und Abstimmungssysteme durchgeführt würde, ohne zögern vertrauen, während die Vertreter der Universitäten zur Zeit eher keine solche voll elektronische Wahl veranstalten würden. Immerhin würden sie sich insofern zu einer E-Wahl stellen, als sie weitgehend Vertrauen haben und: man hat nie so gute Chancen, zu gewinnen… Die erste Frage des Moderators steckte also sogleich die Fronten ab. Es ist anzunehmen, dass sich auch die Juristen, die Politiker, die Politologen und natürlich die Soziologen differenziert positioniert hätten. Alle sie haben je eine spezielle Sicht des Begriffs Vertrauen[2] und haben Erfahrungen aus Anwendungen von komplexen technischen Systemen, welche eine hohe technische Glaubwürdigkeit liefern und auch ausstrahlen müssen, jedoch für den einzelnen Menschen kaum durchschaubar und verständlich sind: der Mathematiker mit Axiomen, der Soziologe mit Statistiken, der Politiker mit Massnahmenpaketen (und Wahlen), etc. und der IT-Riskmanager eben mit implementierten Sicherheitstechnologien. Der E-Voting-Architekt vereint dies und versucht, Vertrauen in ein virtuelles Wahl- und Abstimmungssystem zu gewinnen, indem dieses den höchsten Informatik- und Sicherheitsstandards entspricht, den schärfsten gesetzlichen Grundlagen genügt, 100% zuverlässig und transparent und auch noch bezahlbar (bzw. effizient) ist. Offensichtlich ist dies beim E-Voting deutlich schwieriger als beim Homebanking oder etwa dem vereinbaren eines Termins, einer Hotelreservation, etc. über das offene und unsichere (und von Piraten bevölkerte) Kommunikationsnetz Internet. Oder doch nicht?

Verbriefte Sicherheit?

Weshalb können die Aussagen der Sicherheitsexperten über die höhere Sicherheit des E-Voting gegenüber der Papier- / Briefwahl nur schwer das erforderliche Vertrauen bewirken? Anscheinend bewirkt hier die Komplexität der Technik und der Vorgänge eine reduzierte Glaubwürdigkeit, während sich etwa die Briefwahl kaum je bezüglich der Sicherheit und Zuverlässigkeit rechtfertigen muss. Die Teilnehmer des Podiums vermuten mehrere Ursachen: bei den hergebrachten Gewohnheiten stellt man sich die Sicherheitsfragen nicht mehr, neue Gewohnheiten haben sich noch nicht gefestigt (es besteht noch nicht genügend Zutrauen), für den Bürger ist bereits das Medium Internet unsicher, eine elektronische Wählmaschine / ein E-Voting-System ist eine Blackbox und die Sicherheitsbedenken werden noch dadurch verstärkt, dass Angriffe in der elektronischen Welt skalierbar sind, sich also umfangreicher und verheerender auswirken können. Gerade der letzte Punkt hat sich zu einem Schlagwort der Tagung entwickelt und wurde dem Panel auch von mehreren Zuhörerinnen und Zuhörern mehrmals zugesteckt. Der Vorwurf hat etwas Rationales und kann denn auch nur schwer beseitigt werden: Solange keine 100%-ige Sicherheit gewährleistet werden kann (auch in Bezug auf verborgene Server, die Heim-PCs, etc.), genügt ein Pirat und dessen Angriff auf das System resp. auf dessen Vertrauenswürdigkeit.

Wahlschaden?

Beim Internetbanking ist bekannt, dass es zu Angriffen und dementsprechend schädigenden Transaktionen kommt. Hier handelt es sich jedoch um Einzelpersonen, welche sich beklagen und oft

[1] Dabei handelt es sich um echte Wahlen und Abstimmungen, aber ein auf jeweils wenige Gemeinden beschränkter Einsatz des remote electronic voting.

[2] Der Begriff Vertrauen umfasst im Deutschen neben weiteren Bedeutungen sowohl die unbewusste (Menge an) Bereitschaft des Adressaten, mit einem komplexen System zu interagieren («confidence»; Zutrauen, Vertrauen aufbringen) als auch die bewusste, aktive Entscheidung (festes Überzeugt sein), an die vom System behauptete Glaubwürdigkeit, Verlässlichkeit und Authentizität zu glauben («trust»; Vertrauen haben, in etwas / jemandem vertrauen).

durch kulante Banken schadlos gehalten werden, bevor die schwierige Suche und Auswertung möglicher Beweismittel beginnt. In der Praxis des E-Voting sind keine Klagen von einzelnen Stimmbürgerinnen und Stimmbürger möglich, weil diese in der Regel gar nicht prüfen können, ob Unstimmigkeiten vorliegen. Die Kontrolle durch die Behörden resp. die Polizei ist gleichfalls kaum möglich, was durchaus zu der Vorstellung verleitet, ein Pirat würde sich eine entscheidende Gemeinde und ein E-Voting-System aussuchen und darauf eine wahlentscheidende Manipulation auszuführen können – ohne, dass dies bemerkt wird. Dies sowie die (wie auch beim herkömmlichen Verfahren existierende) Möglichkeit des Stimmenkaufs könnten nicht nur das Aus für das E-Voting bedeuten, sondern nicht abschätzbare Schäden am demokratischen politischen System bewirken. Ob allerdings grössere Angriffe bisher ausblieben, weil es aufgrund der Beschränkung der Pilote auf ein kleines Gebiet / Elektorat nicht viel (geldwertes) zu holen gab, oder ob die System bereits heute genügend sicher sind, bleibt vorderhand offen.

Ein mit genügend Mitteln ausgestatteter Pirat kann sich theoretisch alles kaufen, was für einen erfolgreichen Angriff auf ein E-Banking oder E-Voting-System notwendig ist. Welches sind die Gefahren für E-Voting-Systeme? Die Vertreter der eingesetzten kantonalen Systeme wehren sich gegen die Überlegung, man könne sich einfach die notwendige Technik kaufen und problemlos Wahlen manipulieren. Deshalb müssen die Systeme gehärtet werden (die Sicherheit muss laufend verbessert werden). Verhindern kann man einzelne (versuchte) Angriffe allerdings nicht, aber erschweren. Sie sind es denn auch nicht, welche eine Gefahr für das E-Voting in einem Kanton darstellen. Um trotz des Sicherheitsnetzes allfällige mögliche Manipulationen zu erkennen, werden Kohärenz-Vergleiche angestellt: zwischen den brieflichen und den elektronischen Stimmen oder zwischen Umfrage und Resultat[3].

Gefahr Heim-PC?

Bei der in der Schweiz eingesetzten Variante des E-Voting kann der Bürger von zu Hause aus an Wahlen und Abstimmungen teilnehmen. Dies wird er von einem PC (möglicherweise auch vom Handy / mobile phone) aus tun, der für die Gegenseite grundsätzlich als potentiell infiziert und damit unsicher gilt. Während dem die Praktiker davon ausgehen, dass in der Mehrheit der Fälle auch auf einem verseuchten PC eine korrekte Stimme abgegeben werden kann, sehen hier Theoretiker einen der grössten Hürden des E-Voting: etwa die Manipulation des PC, so dass die angezeigte und die übermittelte Information nicht übereinstimmen. Zwar wurden im Panel sowie auch in den vorangegangenen Beiträgen der Tagung einige Möglichkeiten vorgestellt, um der Gefahr des Heim-PCs zu begegnen: angefangen bei der Information der Teilnehmer, des Einsatzes eines Tunnels, welcher als gesichertes Applet die Interaktion durchführt, ohne installiert zu werden, Mehrfachstimmzettel und Code Voting, Echtzeit-Audits, den bereits erwähnten Plausibilisierungsvergleichen, bis hin zur Auswertung der Log-Files. Dies genügt jedoch nicht allen Wissenschaftlern: beim E-Voting werden systembedingt nicht alle Unregelmässigkeiten entdeckt. Immerhin wird dieser Befund dadurch gemildert, dass es praktisch sehr schwierig erscheint, ein System, welches über verschiedene Sicherheitsfaktoren verfügt und verteilt aufgesetzt ist, zu manipulieren, ohne Spuren zu hinterlassen.

Transparente Blackbox?

Um neben der Verwirklichung der technischen und juristischen Korrektheit einer elektronisch durchgeführten Wahl sowie der Erfüllung der speziellen (gesetzlichen) Anforderungen bei Wahlen und Abstimmungen auch die «sozialen Anforderungen» zu erfüllen («social trust»), ist jedoch mehr nötig, als IT-Sicherheit und die Redekunst von Architekten neuer technischer Systeme. Welche Möglichkeiten der Absicherung und der Gewinnung von Zutrauen gibt es aber noch neben den bisher Bekannten und Verwendeten? Es gibt die Möglichkeit, das Resultat auf ± 5% vorherzusagen und mit dem tatsächlichen Ergebnis zu vergleichen. Dieser im ersten Moment listige Ansatz überzeugt aber ebenso wenig, wie die Möglichkeit von Wahlbeobachtern, in einer fiktiven Gemeinde zu stimmen und ihre Stimmen im Nachhinein zu kontrollieren und vom Resultat auszunehmen. Vielleicht schon

[3] Oder zwischen Kanton und Testgemeinde oder dem Abstimmungsverhalten in der Testgemeinde mit und ohne E-Voting. Piloteinsätze des remote electronic voting sind nach dem Bundesrecht nur bis zu einem relativ kleinen maximalen Anteil der Stimmberechtigen möglich (Beschränkung des Elektorats), so dass sich Unregelmässigkeiten (z.B. bis hin zur Verwerfung des Resultats aller E-Stimmen) nicht / kaum auf das kantonale Ergebnis auswirken.

hilfreicher wäre es, die Architekten der eingesetzten Lösungen zu kennen oder wenigstens Bürger, die bereits erfolgreich ein solches System angewendet haben?

In den aktuellen Systemen ist die Kontrolle des Wählenden sowohl in Bezug auf seine eigene Stimme (wurde sie gezählt, wurde sie korrekt gezählt), als auch in Bezug auf die Gesamtwahl kaum möglich. Deshalb setzt die Wissenschaft (wie auch der deutsche Bundesverfassungsgerichtshof[4]) auf Öffentlichkeit und Transparenz der Systeme (Kontrolle der Funktionstreue und Korrektheit des Systems resp. der Wahl sowie der Nachvollziehbarkeit der Vorgänge) sowie beispielsweise zertifizierte (teilblinde[5]) Intermediäre.

Ein weiteres Problem stellt die eingesetzte Hard- und Software dar. Diese System können zwar ausgiebig geprüft und danach plombiert und bis zum Wahltag nicht mehr berührt werden, aber das System bleibt trotzdem immer irgendwie intransparent, beispielsweise aufgrund des Betriebssystems oder den aufgespielten Sicherheitspatches bzw. den möglichen Sicherheitslecks, falls diese Patches nicht installiert werden.

Onion routing to the future?

Neuere Sicherheitstechniken werden von den Betreibern der kantonalen E-Voting-Systeme natürlich geprüft. Sie sind jedoch keine Wissenschaftler und versuchen, ihre Systeme rechtskonform zu gestalten. Daher sind hier auch die Juristen und die Politiker gefragt, um die Rahmenbedingungen anzupassen. Es ist durchaus sinnvoll, dass dies nicht überstürzt geschieht. Vorderhand – so sind die Betreiber überzeugt – werden die eingesetzten Systeme weiterhin eingesetzt werden.

Die parallele Entwicklung von E-Voting-Systemen in verschiedenen Ländern und in der Schweiz in verschiedenen Kantonen bringt verschiedene Vorteile. Der riskanteste Nachteil dabei ist allerdings der Umstand, dass sich Angreifer auf das schwächste System fokussieren könnten – egal in welchem Land – und so mit einem Angriff die anderen (vielleicht sehr sicheren) Systeme diskreditieren könnten. Da aber niemand zurück zur Landsgemeinde will, wo beispielsweise das Stimmgeheimnis nicht gegeben ist (mit der Folge der Möglichkeit des Stimmenkaufs oder auch nur des sozialen Drucks der Anwesenheitsüberwachung), wird die Entwicklung weitergehen.

Wie wird die Entwicklung verlaufen? Wann – so die letzte Frage des Moderators an die Podiumsteilnehmer – werden 50% der Stimmberechtigten aus Distanz elektronisch abstimmen oder wählen? Aufgrund der Erfahrung bezüglich Akzeptanz von neuen und relativ intransparenten Systemen, welche erst eine Generation benötigt, die damit aufgewachsen ist, wird das Jahr 2020 vorgeschlagen. Möglicherweise gilt diese Zahl für die Niederlande, die Schweiz kommt dann mit etwas Verspätung. Für andere Panelteilnehmer ist das E-Voting nur eine Alternative und es gibt daher (vorerst) kein Ziel, die Anzahl Teilnehmer derart zu erhöhen. Die Menschen werden dasjenige Medium wählen, welches ihnen entspricht, das für sie effizient ist und dem sie vertrauen. Fraglich ist also, ob die Grenze von 50% E-Votern überhaupt erreicht wird, oder ob vorher der grosse Gau eintritt…

Eine Entwicklung bleibt abzuwarten: nachdem die elektronischen Wählmaschinen in den Niederlanden aufgrund eines grossen Vertrauensverlustes nicht mehr eingesetzt werden, ist es interessant, zu analysieren, wie sich die Bürger, welche sich elektronisches Wählen in den Wahllokalen gewohnt waren, mit der (Sicherheits-)Situation abfinden, wenn wieder ausschliesslich auf Papier gewählt wird.

Ist E-Voting erfolgreich?

Die kantonalen bzw. kommunalen Pilotabstimmungen sind «erfolgreich» durchgeführt worden. Bisher hat alles funktioniert, aber irgendwann kommt es vielleicht zu einem Gau und demzufolge zu einer Erschütterung oder gar Zerstörung des Vertrauens. Die schwarze Krawatte des Moderators sollte allerdings kein Symbol dafür sein, obwohl die Ernüchterung in einigen europäischen Ländern

---

[4] «Karlsruhe zieht Black-Box-Voting den Stecker» (heise.de): http://www.heise.de/newsticker/Karlsruhe-zieht-Black-Box-Voting-den-Stecker--/meldung/133893

[5] Blinde Signaturen ermöglichen, dass ein zertifizierter Teilnehmer eine Nachricht bzw. deren Umschlag signieren kann, ohne den Inhalt zu kennen oder je rekonstruieren zu können.

(Deutschland, Niederlande, Irland, Österreich) gewaltig ist. Bricht ein System und das Vertrauen in einem Land, so könnte die Glaubwürdigkeit aller aktuellen Systeme zerstört werden.

E-Voting ist immerhin in der Theorie bereits ein Erfolg. Gemeint ist die Tatsache, dass sich die Wissenschaft anhand dieses Themas zu Höchstleistungen anspornen lässt. Der Learning-by-Doing-Ansatz bewirkt einen Fortschritt auf der Basis bewährter Technologien, ohne allzu grosse Schadensgefahr. Allerdings erfüllen die aktuellen Systeme in der Schweiz die 10 Punkte[6] nicht, noch ist es trivial, ein System zu bauen, welches diese erfüllt. Offen bleibt, ob das elektronische Wählen und Abstimmen auch in der Praxis ein Erfolg wird, da hier der Bereich der exakten Wissenschaften verlassen wird.

Die Frage stellt sich, ob E-Voting erst erfolgreich ist, wenn die Sicherheit jederzeit zu 100% garantiert werden kann, sowohl in der Vorbereitung, Durchführung und Auszählung der Wahl wie auch bereits bei der Entwicklung der Systeme. Auch bei Briefwahlen geht ab und zu mal eine Stimme verloren, das kann man kaum verhindern. Sofern zentrale Punkte (wie etwa die Kontrolle des Clients, die End-zu-End-Nachprüfbarkeit unter Wahrung der Quittungsfreiheit oder die Sicherheit, dass die Anzeige auch dem Übermittelten entspricht) noch nicht erfüllt sind, ist allerdings fraglich, ob das Wählen übers Internet bereits mindestens gleich sicher ist, wie die Briefwahl – auch wenn das E-Voting theoretisch um einiges sicherer wäre…

==========

Daniel Gabi, 5. und 9.–12. Juni 2009

[6] Integrität des Systems, Fairness (keine Möglichkeit, laufende Vorgänge einzusehen), Korrektheit der Annahme und der Auszählung, Anonymität, Quittungsfreiheit, Wahlberechtigung der Teilnehmenden, Einmaligkeit der Stimme, individuelle und universelle Nachprüfbarkeit (Nachvollziehbar- und Beweisbarkeit). Weitere Basisanforderungen sind: Identifizierung (PIN) und Authentifizierung (TAN), Zertifikate, Autorisierung im System, Firewall, verschlüsselte Datenpakete und Kanäle, Verteilung von Wissen und Macht, virtuelle Identitäten und Rollen, Kontrollcode, Validierungscodes, etc.