Zeitschrift für Datenrecht und Informationssicherheit

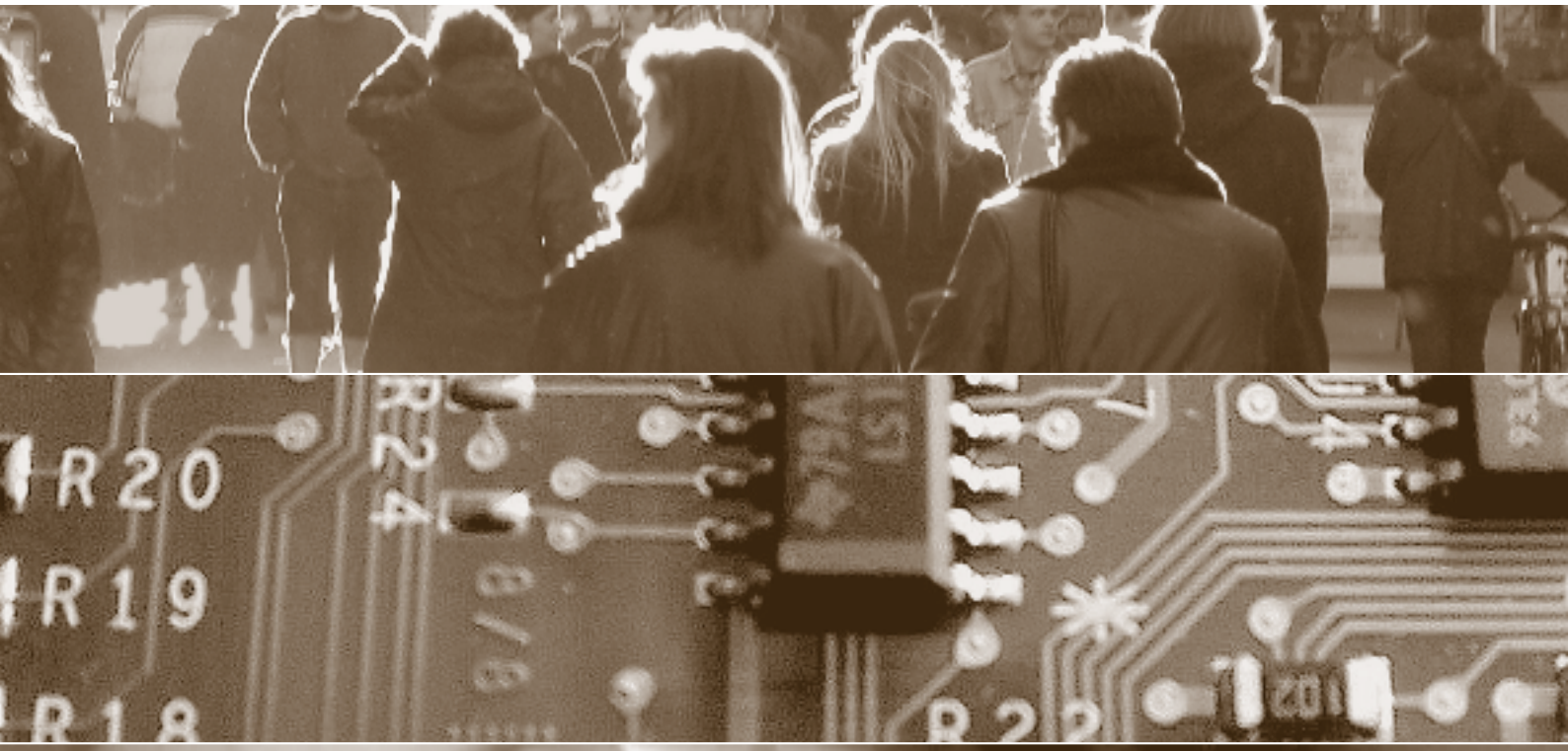
digma

www.digma.info 11. Jahrgang, Heft 3, September 2011

Schwerpunkt:

Reputation im Internet

fokus: Der Ruf nach einem Recht auf Vergessen
fokus: Rufmord im Internet bedroht Unternehmen
report: Datenschutzaspekte smarter Überwachung



Herausgegeben von
Bruno Baeriswyl
Beat Rudin
Bernhard M. Hämmerli
Rainer J. Schweizer
Günter Karjoth

Schulthess §

inhalt

fokus

Schwerpunkt:
Reputation im Internet

Der Ruf nach einem Recht auf Vergessen

Das auf europäischer Ebene postulierte «Recht auf Vergessen» will dem Einzelnen das Recht einräumen, Daten auf dem Internet «zum Verschwinden» zu bringen. Die gegenwärtige Diskussion erweist sich aber noch als zu vage: Die Schaffung eines neuen Grundrechts allein genügt nicht; ein neues Grundrecht erfordert die konkrete Umsetzung in ein spezifisches Anspruchssystem.

Nutzen und Risiken von Internetreputation

Bewertungssysteme im Internet sind hilfreich – sie können aber auch missbraucht werden. Es sind deshalb datenschutzfreundliche Designoptionen für Reputationssysteme zu entwickeln, die sowohl die Integrität der Informationen als auch die datenschutzrechtlichen Anforderungen erfüllen. Die Autorin plädiert deshalb für die Verknüpfung solcher Systeme mit Identitätsmanagementsystemen.

Rufmord im Internet bedroht Unternehmen

Rufmord im Internet betrifft nicht allein Facebook-Anwender: Blogs, Bewertungsportale und soziale Netzwerke können auch Firmen in existenzielle Krisen stürzen. Jeder kann Opfer werden – jeder kann Täter werden. Was kann man dagegen unternehmen?

impressum

digma: Zeitschrift für Datenrecht und Informationssicherheit, ISSN: 1424-9944, Website: www.digma.info

Herausgeber: Dr. iur. Bruno Baeriswyl, Dr. iur. Beat Rudin, Prof. Dr. Bernhard M. Hämmerli, Prof. Dr. iur. Rainer J. Schweizer, Dr. Günter Karjoth

Redaktion: Dr. iur. Bruno Baeriswyl und Dr. iur. Beat Rudin

Zustelladresse: Redaktion digma, per Adr. Datenschutzbeauftragter des Kantons Basel-Stadt, Postfach 205, CH-4010 Basel
Tel. +41 (0)61 201 16 42, Fax +41 (0)61 201 16 41, redaktion@digma.info

Erscheinungsplan: jeweils im März, Juni, September und Dezember

Abonnementspreise: Jahresabo Schweiz: CHF 158.00, Jahresabo Ausland: Euro 131.00 (inkl. Versandspesen), Einzelheft: CHF 42.00

Anzeigenmarketing: Publicitas Publimag AG, Mürtschenstrasse 39, Postfach, CH-8010 Zürich
Tel. +41 (0)44 250 31 31, Fax +41 (0)44 250 31 32, www.publimag.ch, service.zh@publimag.ch

Herstellung: Schulthess Juristische Medien AG, Arbenzstrasse 20, Postfach, CH-8034 Zürich

Verlag und Abonnementsverwaltung: Schulthess Juristische Medien AG, Zwingliplatz 2, Postfach, CH-8022 Zürich
Tel. +41 (0)44 200 29 99, Fax +41 (0)44 200 29 98, www.schulthess.com, zs.verlag@schulthess.com

Skimming – Tatphasen und Haftung

Das Skimming ist zu einem einträglichen Geschäft geworden. Weil sich die Formen, in denen sich die Kriminellen der Informationstechnik und des Internets bedienen, immer mehr annähern, werden sich die «klassische» und die Cyberkriminalität wegen ihrer Methoden und Vorgehensweisen kaum noch unterscheiden. Die deutsche Rechtsprechung hatte sich schon mit Skimming zu befassen.

Datenschutzaspekte smarter Überwachung

Moderne «intelligente» Überwachungssysteme sollen den Bürger besser vor Terrorismus und organisierter Kriminalität schützen, greifen potenziell aber tief in die Privatsphäre des Einzelnen ein. Das EU-Forschungsprojekt SAPIENT untersucht die Risiken solcher intelligenten Überwachungstechniken und erarbeitet Verfahren, um diese im Einklang mit Menschenrechten und unter Beachtung des sozialen und gemeinschaftlichen Zusammenhalts gestalten zu können.

Vertrauensbildung bei Internetwahlen

Nicht nur, dass die Hacker-Gruppe «Anonymous» möglicherweise E-Voting angreifen will – E-Voting sieht sich auch sonst vielen Zweifeln gegenüber: Zweifeln am Nutzen, Zweifeln an der Sicherheit der Technologie, Zweifeln an der Nachvollziehbarkeit des Wahlprozesses, insbesondere bezüglich der Korrektheit des berechneten Wahlergebnisses. Kurz: Kann man E-Voting vertrauen? Die Autoren schlagen vertrauensbildende Massnahmen vor.

Das Risiko «Risk-Management»

Die vorbildliche Firma führt seit Jahren ein IT-Risikomanagement. Die alten Risiken hat sie immer besser im Griff – aber kennt sie auch die neuen? Und kann sie die IT-Risiken auch bewerten? Der Autor weist aufgrund seiner Erfahrung als externer Fachexperte bei ISO/IEC 27001-Zertifizierungen auf die Risiken beim Risikomanagement hin.

Aus den Datenschutzbehörden

Wer ist neu zur Datenschutzbeauftragten gewählt worden? Welche Themen haben Datenschutzbehörden im letzten Quartal bearbeitet? Die neue Unterrubrik berichtet über Personelles und Aktuelles aus der Datenschutzszene.

report

forum

Forschung

Vertrauensbildung bei Internetwahlen

Eric Dubuis, Prof. Dr., Berner Fachhochschule, Research Institute for Security in the Information Society, Professor für Informatik und Koordinator der Forschungsgruppe E-Voting, Biel/Bienne
eric.dubuis@bfh.ch

Oliver Spycher, Berner Fachhochschule und Universität Fribourg, Wissenschaftlicher Mitarbeiter, Biel/Bienne
oliver.spycher@bfh.ch

Elektronische Hilfsmittel bei Wahlen und Abstimmungen (kurz E-Voting) erfreuen sich weltweit immer breiterer Beliebtheit. So können beispielsweise in einigen Kantonen der Schweiz Teile der Wählerschaft bereits seit 2003 bei Referenden und Initiativen ihre Stimme übers Internet abgeben. Einige schweizerische Wahlsysteme sind auch bereits für Wahlen via Internet ausgerichtet und könnten für die Parlamentswahlen diesen Herbst zum Einsatz kommen. Auch in Norwegen sind für diesen Herbst Internetwahlen geplant.

In estnischen Parlamentswahlen wurde bereits zweimal über das Internet gewählt und in einigen Ländern, beispielsweise in Armenien und den USA, steht der Einsatz des Internets bei Wahlen konkret zur Debatte. Dieses breite Interesse erklärt sich durch zahlreiche Vorteile, die Internetwahlen versprechen: schnellere Auszählung, flexible Teilnahme, Unterstützung bei der Stimmabgabe, beispielsweise in der Form von Warnungen bei einer ungültigen Stimmabgabe oder der Unterstützung von Sehbehinderten, die dadurch ihre Stimme ohne Hilfe einer weiteren Person abgeben können.

In anderen Ländern, beispielsweise in Deutschland, kommen Internetwahlen zwar immer öfter zum Einsatz, allerdings nicht im öffentlichen Bereich. Diese Einschränkung gründet auf Zweifeln gegenüber der Technologie. Kritik äussert sich dabei vorwiegend aufgrund der mangelhaften Nachvollziehbarkeit des Wahlprozesses, insbesondere bezüglich der Korrektheit des berechneten Wahlergebnisses.

Damit existierenden und geplanten Internetwahlprojekten nicht ein ähnliches Schicksal widerfährt wie den gescheiterten Wahlgeräten in Deutschland, Irland und den Niederlanden, sind die Umsetzung von vertrauensbildenden Massnahmen vonseiten der Wahlausrichter und der Projektorganisatoren von grosser Bedeutung.

Dieser Artikel stellt eine Auswahl an Massnahmen vor, die bei der Bevölkerung Vertrauen schaffen können. Jede der folgenden Massnahmen wird vorgestellt und diskutiert:

- Transparenz
- Aufgabentrennung
- Verifizierbarkeit
- Stimme überschreiben
- Unabhängige Software
- Sicherheitsevaluierung.

Transparenz

Beschreibung

Sie bildet das Schlüsselelement bei der Bildung von Vertrauen. Nur eine breit ausgelegte Informationspolitik erlaubt der Wählerschaft, das verwendete System zu verstehen oder es sich von unabhängigen Experten erklären zu lassen. Die folgenden Vorkehrungen sind dabei dienlich:

- Die Veröffentlichung des Sicherheitskonzepts: Es soll insbesondere aufzeigen, wie und inwiefern das System die korrekte Ermittlung des Wahlresultats und die Einhaltung des Wahlgeheimnisses garantiert.
- Die Veröffentlichung einer Übersicht der verwendeten Komponenten und der organisatorischen Prozesse, welche von der Vorbereitung des Systems bis hin zur Veröffentlichung des Wahlresultats führen: Die Dokumentation soll insbesondere auch einen Bezug zum Sicherheitskonzept erstellen und die organisatorischen Massnahmen verdeutlichen, welche zu dessen Umsetzung beitragen.
- Die Veröffentlichung der kryptografischen Mechanismen und der Software, inklusive Programmcode: Auch sie soll sich auf das Sicherheitskonzept beziehen.
- Die Veröffentlichung der Dokumente, die im Rahmen der Evaluation verwendet oder erzeugt werden: Dazu zählt insbesondere der Evaluationsbericht.
- Die Veröffentlichung einer vereinfachten Kurzdokumentation, die sich an den interessierten IT-Laien richtet: Sie soll auf die Art und die Ausprägung von Restrisiken bei der Benutzung des Systems hinweisen. Um zusätzliches Vertrauen zu schaffen, sollte eine Plattform geschaffen werden, auf der unabhängige Experten bezeugen, dass die Kurzdokumentation korrekt aus der technischen Dokumentation abgeleitet worden ist.
- Einführung einer Hotline, die Fragen und Anregungen zum Projekt entgegennimmt und öffentlich beantwortet.

Diskussion

In der Vergangenheit war die verfügbare Information zu den meisten Internetwahlsystemen (im Folgenden nur kurz als Systeme bezeichnet) eher rar und beschränkte sich auf einzelne Systemaspekte. Dies liegt einerseits daran, dass private Unternehmen an der Entwicklung der Internetwahlsysteme beteiligt sind und ihr Produkt vor der Konkurrenz schützen wollen. Anderseits birgt Transparenz das Risiko, dass Wähler, die eigentlich dem System blind vertrauen würden, erst als Folge der öffentlichen Diskussion anfangen, Zweifel zu hegen.

Im estnischen Projekt wurde zwar grosser Wert darauf gelegt, das System jedem Wähler auf verständliche Weise zu erklären. Die Veröffentlichung der eigentlichen Systemdokumentation, insbesondere des Programmcodes, erfolgte allerdings fast ausschliesslich nach Unterzeichnung eines Geheimhaltungsversprechens und nur vor Ort. Das norwegische Projekt hingegen bekennt sich explizit zu Transparenz und veröffentlicht viele relevante Dokumente auf seiner Website.

Aufgabentrennung

Beschreibung

Die Trennung und die Aufteilung von Aufgaben unter mehreren möglichst unabhängigen Systemteilnehmern soll bezüglich der Geheimhaltung von sicherheitskritischen Informationen Vertrauen schaffen. Dadurch wird beispielsweise das Brechen des Wahlgeheimnisses erschwert, ebenso die Ermittlung eines vorzeitigen Teilresultats einer Wahl. Die wissenschaftliche Literatur beschreibt dazu kryptografische Mechanismen, die sicherstellen, dass kritische Informationen nur unter Teilnahme von mehreren Parteien berechnet werden können.

Vertrauen wird zusätzlich durch die geeignete Wahl von unabhängigen Parteien gefördert, die der Wählerschaft auf einer öffentlichen Plattform ihr unabhängiges und pflichtbewusstes Mitwirken zusichern.

Diskussion

Die Schaffung eines hohen Masses an Unabhängigkeit ist in einem zentral geführten Projekt organisatorisch nicht leicht. Immerhin ist es im norwegischen Projekt gelungen, sicherheitskritische Aufgaben unter zwei staatlichen Institutionen aufzuteilen, die unabhängig agieren und geografisch weit auseinanderliegen.

Verifizierbarkeit

Beschreibung

Das Urteil des deutschen Bundesverfassungsgerichts vom 3. März 2009 (2 BvC 3/07 und 2 BvC 4/07) stellt klar, dass die Wählerschaft überprüfen können muss, dass ihre Stimme korrekt erfasst und im Ergebnis berücksichtigt wird. Die Forderung nach Transparenz betrifft somit nicht nur die Systemdokumentation, sondern auch die Daten selbst.

In der wissenschaftlichen Literatur sind Systeme beschrieben, welche dieser Anforderung gerecht werden. Zusätzlich erlauben sie der Öffentlichkeit nachzuprüfen, dass alle Stimmen in der elektronischen Urne von unterschiedlichen wahlberechtigten Personen stammen und dass sämtliche bei der Auszählung berücksichtigt werden. Um diese sogenannte End-To-End-Verifizierung (E2E) unter Einhaltung des Stimmgeheimnisses zu ermöglichen, wird die Verwendung verschiedener anerkannter Techniken aus der Kryptografie vorgeschlagen.

Diskussion

Auf den ersten Blick mag die Forderung nach Verifizierbarkeit unangemessen erscheinen, da doch in traditionellen Wahllokalen auch falsch ausgezählt werden kann. Die E-Voting-Kritiker weisen aber darauf hin, dass falsches Auszählen bei einem zentralisierten Internet-Wahlsystem viel stärkere Auswirkungen auf das Endresultat haben könne. Ausserdem sei in traditionellen Wahllokalen die Wahlbeobachtung durch unabhängige Personen auch möglich und nötig.

Eine Lösung durch den Einsatz von E2E-verifizierbaren Systemen klingt vielversprechend. Da im Hintergrund aber schwere kryptografische Techniken implementiert sind, bedarf es noch an Forschung, diese so zu gestalten, dass der durchschnittliche Nutzer diese auch ohne zusätzliche Hilfe verwenden kann. Als benutzerfreundliche Zwischenlösung könnte jedoch bereits heute Software von unabhängigen Institutionen verwendet werden.

Insbesondere neuere Systeme tragen der Forderung nach Verifizierbarkeit oft Rechnung. So steht ein erstes E2E-verifizierbares System bereits prototypisch als Open Source zur Verfügung (Helios); ein schweizerischer Prototyp ist zurzeit in Entwicklung (Selectio Helvetica). Das norwegische sowie das deutsche Polyas-System decken einen Teil der E2E-Verifizierbarkeit ab.

Melanie Volkamer, Dr., CASED und Technische Universität Darmstadt, Forschungsgruppenleiterin IT-Security, Usability and Society und Koordinatorin des Arbeitsbereichs Sichere Daten, Darmstadt volkamer@cased.de

Kurz&bündig

Vertrauensbildende Massnahmen für elektronische Verfahren bei Wahlen und Abstimmungen helfen, mögliche Zweifel der Wählerschaft an der Wahrung des Stimmgeheimnisses und der Korrektheit des Ergebnisses auszuräumen. Transparenz, Aufgabentrennung, Verifizierbarkeit, Überschreiben der Stimme, unabhängige Software und Sicherheitsevaluierung sind einige dieser Massnahmen. Diese gelangen insbesondere in neueren Internetwahlsystemen zur Anwendung.

Stimme überschreiben

Beschreibung

Die Idee ist entstanden, als Estland seiner Wählerschaft die Internetwahl als zusätzliche Alternative zur Präsenzwahl im Wahllokal anbot. Im Gegensatz zur Präsenzwahl kann bei der Internetwahl nur schwer ausgeschlossen werden, dass man bei der Stimmabgabe beobachtet wird. Um dieses Problem im privaten Umfeld zu umgehen, kann der Wähler seine Stimme beliebig oft elektronisch abgeben. Dabei wird die zuletzt eingegangene Stimme gezählt. Bei Bedarf kann die elektronische Stimme auch durch einen Gang an die Urne ersetzt werden.

Dieser Ansatz dient gleichzeitig auch als vertrauensbildende Massnahme. Denn der Wähler weiss, selbst wenn ihn jemand unerwartet beobachten sollte oder gar zwingen sollte, eine bestimmte Stimme abzugeben, kann er diese Stimme später noch einmal ändern. Ausserdem braucht der Wähler auch keine Angst vor möglichen Computerproblemen bei der Stimmabgabe zu haben. Falls ein solches Problem auftreten sollte, hat er damit nicht sein Stimmrecht verloren, sondern kann die Stimme zu einem späteren Zeitpunkt, gegebenenfalls von einem anderen Gerät oder im Wahllokal erneut abgeben.

Diskussion

Es gibt einige Gegner der mehrfachen Stimmabgabe. Sie argumentieren, dass die Ernsthaftigkeit des Wahlvorgangs in Gefahr ist, wenn Wähler ihre Stimme beliebig oft abgeben und dadurch die alte Stimme jederzeit überschreiben können. Dennoch ist diese Massnahme nebst Estland auch in Norwegen geplant.

Unabhängige Software

Beschreibung

In vielen Internetwahlsystemen bekommt die Stimmabgabesoftware, die auf dem Computer der Wähler läuft, alle notwendigen Informationen, die sie zum Brechen des Wahlgeheimnisses braucht, nämlich die Identifikation des Wählers und seine Stimme. Manipulierte Software könnte auch eine falsche Wahl abschicken, ganz ohne die Eingabe des Wählers zu berücksichtigen. Daher ist ein grosses Vertrauen in diese Stimmabgabesoftware erforderlich. Vertrauen kann geschaffen werden, indem dem Wähler freigestellt wird, welche Software er zur Stimmabgabe benutzt.

Diskussion

Dank dieser Massnahme könnte der Wähler zwar seine Software entweder selber programmieren oder sich zumindest aussuchen, von welcher Institution er sich die entsprechende Software beschafft. Allerdings birgt sie auch die Gefahr, dass manipulative Software unbemerkt in Umlauf kommt.

Sicherheitsevaluation

Beschreibung

Da viele Wähler die Sicherheitstechniken hinter den elektronischen Wahlsystemen nicht im Detail verstehen und prüfen können, ist eine weitere vertrauensbildende Massnahme die Evaluation des Internetwahlsystems und der technischen und organisatorischen Umgebung, in der es eingesetzt wird. Dabei sollte diese Evaluation nicht durch interne Experten und eigene Kriterien und Methoden erfolgen, sondern nach internationalen Standards wie der Common Criteria oder ISO 27001/IT-Grundschutz. Der Bezug zum Sicherheitskonzept muss klar sein.

Standardisierte Verfahren haben den Vorteil, dass transparent ist, welche Teile des Systems nach welchen Anforderungen unter welchen Annahmen in welcher Tiefe geprüft werden.

Neben diesen technischen Sicherheitsüberprüfungen sollten auch die kritischen organisatorischen Prozesse während der Durchführung der Wahl evaluiert werden. Ausserdem ist es wichtig, im Vorfeld nicht nur die IT-Sicherheit, sondern auch die Benutzerfreundlichkeit nach internationalen Standards zu evaluieren, damit das Vertrauen durch eine geeignete Benutzeroberfläche weiter gesteigert wird.

Diskussion

Alle international anerkannten standardisierten Evaluationen sind sehr aufwändig und teuer. Entsprechend viel Zeit muss hierfür eingeplant werden. Ausserdem bezieht sich ein Zertifikat nur auf eine Version der Software. Nach jeder noch so kleinen Änderung müsste die gesamte aufwändige Evaluation wiederholt werden.

Viele Internetwahlprojekte wurden internen Evaluationen durch Experten unterzogen. Dabei ist für Aussenstehende leider nicht ersichtlich, was jeweils tatsächlich geprüft wurde. Allerdings lassen sich in

Literatur, weiterführende Links

- Directorate general of democracy and political affairs: Guidelines on transparency of e-enabled elections. GGIS (2010) 5 E, Council of Europe.
- M. Volkamer, Evaluation of Electronic Voting – Requirements and Evaluation Procedures to Support Responsible Election Authorities (2009), volume 30 of LNBIP, Springer.
- E. Dubuis/S. Fischli/R. Haenni/U. Serdült/O. Spycher, «Selectio Helvetica: A Verifiable Remote E-Voting System», in CeDEM'11, Conference for E-Democracy and Open Government, Krems, Austria, 2011.
- Melanie Volkamer/Guido Schryen /Lucie Langer/Axel Schmidt/Johannes Buchmann, Elektronische
- Wahlen: Verifizierung vs. Zertifizierung, Informatik 2009, LNI, Vol. 154, 1827–1836.
- B. Adida, Helios: Web-based open-audit voting. In: In Proceedings of the 17th USENIX Security Symposium Security '08 (2008).
- O. Spycher/R. Haenni, «A Novel Protocol to Allow Revocation of Votes in a Hybrid Voting System», ISSA'10, 9th Annual Conference on Information Security, South Africa, Sandton, South Africa, 2010.

Deutschland und Norwegen erste Schritte in die gewünschte Richtung verzeichnen. Das Internetwahlsystem Polyas befindet sich zurzeit im Common-Criteria-Evaluationsverfahren. Das norwegische System soll nach der Wahl im Herbst 2011 im Hinblick auf weitere Einsätze auch nach den Common Criteria evaluiert werden.

Schluss

Vertrauensbildende Massnahmen dienen dazu, Zweifel bezüglich der Wahrung der Privatsphäre und der Korrektheit des berechneten Stimm- oder Wahlergebnisses auszuräumen. Die Massnahmen umfassen die Offenlegung der Funktionsweise der elektronischen Hilfsmittel und deren Handhabung, die transparente Auftrennung der Verantwortlichkeiten, die Möglichkeit des öffentlichen Korrektheitsnachweises durch die Offenlegung der entsprechenden Daten, wohlgemerkt unter Wahrung der Privatsphäre, die Freiheit, die eigene Stimme zu überschreiben, die Möglichkeit, eigene, unabhängige Software zur Stimmabgabe zu verwenden sowie die systematische und unabhängige Sicherheitsevaluation der elektronischen Wahlsysteme.

Sowohl die Misserfolge der Projekte in Deutschland und den Niederlanden als auch die vielversprechenden Anstrengungen im norwegischen Projekt weisen auf eine zunehmende Bedeutung von vertrauensbildenden Massnahmen hin. Entsprechend bemüht sich die Forschungsgemeinschaft um die Entwicklung von Systemen, welche sich besonders dazu eignen, Vertrauen zu schaffen. ■

Zeitschrift für Datenrecht und Informationssicherheit
digma
www.digma.info
erscheint vierteljährlich

Meine Bestellung

❑ 1 Jahresabonnement digma (4 Hefte des laufenden Jahrgangs)
à **CHF 158.00** bzw. bei Zustellung ins Ausland **EUR 131.00** (inkl. Versandkosten)

Name Vorname

Firma

Strasse

PLZ Ort Land

Datum Unterschrift

Bitte senden Sie Ihre Bestellung an:
Schulthess Juristische Medien AG, Zwingliplatz 2, CH-8022 Zürich
Telefon +41 44 200 29 19
Telefax +41 44 200 29 18
E-Mail: zs.verlag@schulthess.com
Homepage: www.schulthess.com

Schulthess §