heise online

22C3: Pro und Kontra e-Voting

29.12.2005 18:47 Uhr
Richard Sietmann

Ein Kontrastprogramm bot der 22C3 am heutigen Donnerstag zum Thema e-Voting. Der Frankfurter Software-Spezialist Ulrich Wiesner begründete, warum die in Deutschland vielfach bereits eingesetzten elektronischen Wahlgeräte sowohl gegen demokratische Grundprinzipien als auch gegen geltendes Recht verstoßen. Aus Estland war Tarvi Martens angereist, der Kopf hinter dem **Internetwahl-Projekt [1]** in der baltischen Republik.

Das estnische Parlament hatte im Sommer **mit knapper Mehrheit [2]** den Weg für die Stimmabgabe über das Internet freigemacht, und im Oktober kam das System bei den **Kommunalwahlen [3]** erstmals zum praktischen Einsatz. Bei einer Wahlbeteiligung von insgesamt 47 Prozent hatten von den 502.000 Wählern knapp 10.000 von der Möglichkeit Gebrauch gemacht, meist an Kiosk-Terminals in Banken, öffentlichen Einrichtungen und Telekomläden. "Eine Killer-Applikation ist Internet-Voting nicht, und es bringt keine neuen Wähler", berichtete Marten; "es ist nur eine andere Art des Wählens, die auch etwas mit dem Lifestyle zu tun hat".

Den Kern des der Briefwahl nachgebildeten Systems bildet die nach dem Private/Public-Key-Verfahren verschlüsselte Kommunikation zwischen Wähler und Wahlamt. Von den 1,35 Millionen Einwohnern der Baltenrepublik besitzen mehr als 850.000 bereits eine Smartcard als **Personalausweis [4]**, der auch als Signaturkarte dient. Anhand des Zertifikats authentifiziert das System den Wähler und prüft den Eintrag in das Wählerverzeichnis. Der Wahlberechtigte bekommt dann den Stimmzettel seines Wahlkreises als HTML-Seite auf das Display, zusammen mit einem ActiveX- oder Java-Applet als Wahlclient. Der Client ermöglicht, das Votum mit dem Public Key des Wahlamtes zu verschlüsseln und mit der Ausweiskarte zu signieren. Um die Anonymität zu wahren, trennt der Server im Wahlamt die Signatur vom verschlüsselten Stimmzettel; bei der späteren Auszählung werden die Voten dann mit dem geheimen Schlüssel des Wahlamtes decodiert.

Der Este, der dem Nationalen Wahlausschuss angehört und im Hauptberuf Mitarbeiter des in Tallinn ansässigen Trustcenters und ID-Card-Betreibers **AS Sertifitseerimiskeskus (SK) [5]** ist, zeigte sich überzeugt, dass Internet-Wahlen die Zukunft gehört. "Dagegen anzukämpfen ist sinnlos". Auf Fragen aus dem Auditorium musste er allerdings zugeben, dass das System keinen Schutz vor Angriffen mit Spyware oder Trojanern aus dem Internet auf den PC des Users bieten kann; so kommt es beispielsweise mit einem einfachen Kartenleser für die Authentifizierung mit der Signaturkarte aus, ein Klasse-3-Leser mit eigenem Display und Keypad ist nicht vorgeschrieben. "Solange man es mit Standard-PCs zu tun hat, kann man diese Bedrohung nicht ausschliessen", gestand Martens ein. Zur Wahlzeit wären aber "alle wichtigen Internet-Security-Spezialisten für das Network-Monitoring auf DoS-Attacken und Trojaner im Einsatz gewesen. In

der Diskussion bedankte sich jedenfalls schon mal ein Hacker für die Herausforderung – "zum ersten Mal gibt es jetzt einen ganzen Staat als Testfall".

Dass schon bei nicht-vernetzten, Software-gesteuerten Wahlgeräten, an denen hierzulande bei der letzten **Bundestagswahl [6]** bereits mehr als zwei Millionen Wähler ihre Stimme abgeben mussten, das grundlegende Wahlprinzip der öffentlichen Stimmauszählung auf der Strecke bleibt, bemängelte Ulrich Wiesner in seinem Vortrag "Der schleichende Verfall der öffentlichen Kontrolle". "Aus deutschen Quellen ist sehr wenig über die eingesetzten Geräte der niederländischen Firma Nedap in Erfahrung zu bringen", kritisierte er. Anfragen ans Bundesinnenministerium seien mit dem Hinweis auf den Schutz von Firmengeheimnissen abschlägig beschieden worden. "Das Sicherheitskonzept basiert auf dem seit langen diskreditierten Ansatz 'Security by Obscurity'", meint Wiesner.

Er führte die Untersuchungsberichte einer irischen Kommission an, die bei einer baugleichen Version zu dem Ergebnis gekommen war, dass die Elektronik auf dem Stand von 1980 sei und dass es nur schätzungsweise zwei Minuten eines unauthorisierten Zugangs bedürfte, um den Chip mit dem eingebetteten Steuerungsprogramm durch eine manipulierte Version zu ersetzen. "Es ist unmöglich festzustellen", so Wiesner, "ob es sich bei der installierten Software um die zertifizierte handelt und ob sie korrekt zählt". Für ihn war das einer der Gründe, weshalb er gegen das Ergebnis der Bundestagswahl **Einspruch [7]** erhoben hat. Dem auch **verfassungsrechtlich umstrittenen [8]** elektronischen Hütchenspiel mit den Wählerstimmen will sich der CCC jetzt verstärkt annehmen; auf einer neugeschaffenen **Web-Seite [9]** gibt es nähere Informationen zum Thema. (*Richard Sietmann*) / (**pmz [10]**)

URL dieses Artikels:

`http://www.heise.de/-161678`

Links in diesem Artikel:

[1] `http://www.vvk.ee/engindex.html`

[2] `https://www.heise.de/meldung/Streit-um-Stimmabgabe-per-Internet-in-Estland-111945.html`

[3] `https://www.heise.de/meldung/Demokratie-per-Internet-Esten-koennen-elektronisch-waehlen-135853.html`

[4] `http://www.id.ee/pages.php/0303`

[5] `http://www.sk.ee/pages.php/0203`

[6] `http://www.heise.de/ct/05/19/054/`

[7] `https://www.heise.de/meldung/e-Voting-Anfechtung-der-Bundestagswahl-wegen-Wahlcomputern-147939.html`

[8] `https://www.heise.de/meldung/Verfassungsrechtler-kritisiert-E-Voting-160852.html`

[9] `https://berlin.ccc.de/index.php/Wahlmaschinen`

[10] `mailto:pmz@ct.de`