



Richard Sietmann

E-Voting – ein Spiel mit dem Feuer

Elektronische Wahlsysteme bei den US-Präsidentenwahlen 2004

Die Präsidentenwahlen des Jahres 2000 waren für die USA bereits ein Debakel. Jetzt fürchten Wissenschaftler und Bürgerrechtler, dass die überstürzt eingeführten elektronischen Wahlsysteme alles noch verschlimmern.

Ständige Wachsamkeit ist der Preis der Freiheit.“ Über diese Mahnung Thomas Jeffersons kann die US-Bürgerrechtlerin Victoria Collier nur bitter lachen. In den siebziger Jahren hatten ihr Vater James Collier und sein Bruder Kenneth systembedingte Schwächen des amerikanischen Wahlsystems anhand von Manipulationen in Florida aufgezeigt und in dem Buch „Votescam“ dokumentiert. Jetzt kämpft die Tochter dagegen, dass das „Hütchenspiel mit den Wählerstimmen“ eine neue Dimension erreicht.

„Der Souverän ist am Steuer eingeschlafen“, meint die Aktivistin und befürchtet, dass der

politisch forcierte Einsatz von Computern in den Wahlkabinen das demokratische System an die Wand fährt. Mit dieser Befürchtung steht sie nicht allein. Überall im Land schießen Bürgergruppen aus dem Boden, die der elektronischen Zählung zutiefst misstrauen und sich den Ruf nach transparenten und nachprüfbareren Wahlen auf die Fahnen geschrieben haben.

Als Reaktion auf das Wahldebakel in Florida vor vier Jahren, bei dem Lochkartenmaschinen ungewöhnlich viele Stimmen als ungültig zählten, weil sich die perforierten Kästchen auf den „Punch Cards“ nicht vollständig abgelöst hatten, und der

Supreme Court schließlich nach einer wochenlangen Hängepartie die sich immer mehr zu Gunsten des Demokraten Al Gore neigende manuelle Nachzählung stoppte, hatte der Kongress im Oktober 2002 den „Help America Vote Act“ beschlossen. Er stellte Bundesmittel in Höhe von 3,8 Milliarden Dollar zur technischen Aufrüstung der 185 000 Wahllokale des Landes bereit.

Vergebens warnte die Informatik-Professorin Rebecca Mercuri von der Harvard University, eine ausgewiesene Expertin für Computer-Wahlsysteme: „Wer meint, Technik könne die Probleme des Wahlsystems lösen, hat weder die Probleme noch die Technik verstanden.“ Eine Abschätzung der Auswirkungen auf die Wähler und das Wahlsystem stand im Kongress nicht zur Debatte. Das Office for Technology Assessment, einst beispielgebend für die Technikfolgenabschätzung in anderen Ländern, wurde durch die republikanische Mehrheit schon 1995 abgeschafft. Und über die vermeintlichen Bedenkenträger aus den Reihen der Wissenschaft setzte sich der Gesetzgeber hinweg. Doch von denen gab es einige. Als David Dill, Professor für Informatik an der Stanford University und Herausgeber der Computer-Fachzeitschrift *Security & Privacy*, einen Aufruf gegen die voreilige informationstechnische Aufrüstung stellte – Tenor: „Computerisierte Wahlgeräte sind inhärent anfällig für Programmierfehler, Fehlfunktionen und böswillige Manipulationen“ –, unterzeichneten die Resolution innerhalb weniger Wochen mehr als 1200 Fachkollegen.

Ohne Kreuzchen

Kreuze auf Zetteln, die Helfer dann von Hand auszählen, spielen diesmal kaum noch eine Rolle, weniger als ein Prozent wählt auf diese Weise; 32 Prozent markieren ihre Entscheidung zwar noch auf Papier, aber – wie man es von statistischen Fragebogen kennt – durch das Schwärzen bestimmter Felder, die optischen Scannern das automatische Einlesen ermöglichen. Von den rund 154 Millionen Wahlberechtigten geben etwa 50 Millionen – dreimal mehr als vor vier Jahren – ihr Votum am 2. November an

einem Touchscreen oder auf Knopfdruck direkt in einen Wahlcomputer ein, der per „Direct Recording Electronic“ (DRE) unmittelbar die Stimmen zählt. Die diskreditierten Stanzkarten wird noch ein Fünftel der Wählerschaft vorfinden, 13 Prozent wählen ihren Kandidaten an Hebelmaschinen, die schon gar nicht mehr hergestellt und kaum noch gewartet werden.

Für die knappe Hand voll von Herstellern, die hauptsächlich zum Zuge kommen, bedeutet der „Help America Vote Act“ einen warmen Geldregen – Schätzungen zufolge kontrollieren die Computer von Diebold, Election Systems & Software (ES&S), Sequoia Voting Systems

und Hart InterCivic etwa 80 Prozent der Stimmauszählung. Diese Firmen verfügen über beste Verbindungen ins politische Establishment. Einer der führenden Investoren von Hart InterCivic, Tom Hicks, ist bekanntermaßen der Familie Bush finanziell eng verbunden. Der CEO von Diebold Election Systems, Walden O'Dell, bekannte im August 2003 in dem Einladungsschreiben zu einem Spenden-Dinner für die Republikaner, er wolle dabei mithelfen, „dass Ohio seine Stimmen nächstes Jahr beim Präsidenten abliefern“. Und bei den letzten beiden Wahlen, aus denen der republikanische Senator Chuck Hagel aus Nebraska siegreich hervorging, re-

gistrierten 80 Prozent der Wählerstimmen Maschinen der in Nebraska beheimateten Firma ES&S, deren früherer Anteilseigner und CEO Hagel war – ein Umstand, den er bei Amtsantritt dem Kongress gegenüber verschwiegen.

Die Zukunft soll nach dem Willen der Politik den DRE-Verfahren gehören. Mit der Unterstützung aus Washington schaffte Georgia für 54 Millionen Dollar 19 000 Touchscreen-Geräte an und stellte komplett auf papierloses E-Voting um; eine von der Elektronik unabhängige Nachzählung ist in dem Bundesstaat nicht mehr möglich. Ebenso mit den 11 000 Systemen in Maryland nicht: Als dort die de-

mokratische Senatorin Barbara Mikulski kürzlich einen der „AccuVote TS“-Touchscreens von Diebold testete, beobachtete sie, wie eine unbedachtsame Handbewegung eine „Yes“-Stimme plötzlich in ein „No“ verwandelte. Ähnliches war einem Wähler in Crozet (Virginia) bei der letzten Wahl vor vier Jahren auch schon widerfahren. „Als ich die „No“-Taste neben dem Wahlvorschlag drückte, zeigte die Maschine ein „Yes“ an“, beschrieb er die Tücken der Technik. „Wann immer ich eine Wahl traf, leuchtete die entgegengesetzte Anzeige auf. Als ich den Wahlhelfer fragte, was zu tun sei, riet er mir, einfach den falschen Knopf zu drücken.“

In der Hightech-Falle

Die US-Präsidentenwahl 2004 wird erstmals von einer etwa hundertköpfigen Kommission von Wahlbeobachtern der Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE) überwacht. Zu den 55 Mitgliedsstaaten der OSZE gehören auch die USA und Kanada. Eine Wahlbeobachtung durch die UN, wie von den Demokraten beantragt, hatte die republikanische Mehrheit im Kongress abgelehnt. c't sprach mit der Leiterin der OSZE-Wahlbeobachtungskommission, der sozialdemokratischen Schweizer Nationalrätin Dr. Barbara Haering.

c't: Frau Haering, rund ein Drittel der US-Wähler wird bei den Präsidentschaftswahlen sein Votum an elektronischen Wahlmaschinen abgeben. Wie können Sie überprüfen, dass die elektronische Stimmzählung den tatsächlichen Wählerwillen widerspiegelt?

Barbara Haering: Es ist zum ersten Mal, dass wir Wahlen beobachten, bei denen in diesem Ausmaß elektronische Wahlsysteme zum Einsatz kommen. Die OSZE ist eine politische und keine fachtechnische Organisation. Sie hat sehr viel Erfahrung, wie Wahlen „fair and free“ abgewickelt werden können und sollen, sie hat aber kein computertechnisches Know-how.

c't: Das heißt, Sie müssen die Wahlgeräte als eine Blackbox behandeln?

Haering: Wir müssen darauf hinweisen, dass es die Länder sind, die in der Verantwortung stehen.

Es braucht unabhängige, staatlich lizenzierte Prüfstellen, die das Recht und die Pflicht haben, solche elektronischen Wahlsysteme – bei denen sich die Hard- und Software ja ständig weiterentwickelt – unabhängig zu überprüfen. Ich denke, das ist der einzige Weg, wie die OSZE mit dieser Frage umgehen kann. Wir hätten als internationale politische Organisation nie die Möglichkeit, Software selbst zu analysieren. Dies müssen staatlich anerkannte und lizenzierte Prüfstellen tun.

c't: Ist das in den USA befriedigend geregelt?

Haering: Dazu werde ich im Vorfeld keine Stellungnahme abgeben.

c't: Die Wahlbeobachter werden auch nicht vor Ort überprüfen, ob die Hard- und Software in den verwendeten Wahlgeräten tatsächlich der Konfiguration entspricht, die von der National Association of State Election Directors (NASED) zertifiziert wurde?

Haering: Das geschieht teilweise im Vorfeld, aber vor Ort werden die Parlamentarierinnen und Parlamentarier die Maschinen nicht untersuchen, denn die sind ja dann im Gebrauch. Sonst müsste man sie abstellen und analysieren können – das kann ein Parlamentarier nicht.

c't: Der Informatiker Douglas Jones, ein ehemaliges Beiratsmitglied zur Prüfung elektronischer Wahlsysteme im US-Bundesstaat Iowa, hat vorgeschlagen, am

Wahltag stichprobenartig Geräte unangemeldet aus dem Wahlprozess herauszunehmen und daran mit Testwählern zu überprüfen, ob die Eingaben korrekt gezählt werden. Wäre solch ein „Parallel Testing“ eine Lösung?

Haering: Das könnte eine der Empfehlungen in dem Bericht sein.

c't: Wie gehen Sie bei konventionellen Wahlen vor?

Haering: Wir können immer nur Stichprobenkontrollen machen. Je nach Wahlsystem und Situation begleitet ein Team von zwei bis sechs Beobachtern in zufällig ausgewählten Wahlbezirken die Auszählung bis zum Schluss.

c't: Zählen die Wahlbeobachter auch nach?

Haering: Wir haben keinerlei Eingriffsmöglichkeiten; wir beobachten nur und zählen nicht nach.

c't: Nimmt Ihnen die elektronische Stimmabgabe und -auszählung nicht auch die Beobachtungsmöglichkeit?

Haering: Die Einführung elektronischer Wahlsysteme stellt alle Länder vor neue Probleme, und damit wird natürlich auch die Wahlbeobachtung schwieriger. Deshalb die Empfehlung, dass die Länder dafür staatlich lizenzierte Prüfstellen einrichten. Die Wahlbeobachtung beschränkt sich jedoch bei weitem nicht nur auf das Problem der elektronischen Wahlmaschinen: In unserem Bericht werden wir



Die Schweizer Nationalrätin Dr. Barbara Haering ist Leiterin der OSZE-Beobachtungskommission für die US-Präsidentenwahlen 2004.

Aussagen zur Wahlkampagne, über die Zugänglichkeit der Kandidaten zu den Medien, zur Registrierung der Wähler, zur Identifikation der Wählerinnen und Wähler am Wahltag, zum Ablauf des Wahltages, zu den Wahlverfahren und zur Auszählung machen.

c't: Wie beurteilen Sie die „paperless ballots“, die in den USA vielfach zum Einsatz kommen? Der völlige Verzicht auf papierne Stimmzettel macht eine herstellerunabhängige Nachzählung unmöglich.

Haering: Auch dazu werde ich im Voraus kein Urteil abgeben.



Wählen à la WebPad – „eslate 3000“ von Hart InterCivic.



Die portable Wahlkabine „AVC Edge“ von Sequoia Voting Systems (Touchscreen)

Zehn Tage nach den Kongresswahlen im November 2002 fiel dem demokratischen Kandidaten Richard Romero im Bernalillo County (New Mexico) auf, dass zwar 48 000 Wähler ihr Votum abgegeben hatten, insgesamt aber nur 36 000 Stimmen gezählt worden waren. Daraufhin wurde ein Software-Patch installiert, und die Sequoia-Techniker übermittelten aus Denver die „korrekten“ Resultate. Sequoia-Vice President Howard Cramer musste später zugeben, dass dasselbe Problem im Clark County in Nevada ebenfalls aufgetreten war.

Bei einer Gemeindewahl im Boone County (Indiana) registrierten die Wahlcomputer vor einem Jahr 140 000 Stimmen – in einer Kommune mit 50 000 Einwohnern und 19 000 Wahlberechtigten, von denen sich nur rund ein Viertel an der Abstimmung beteiligt hatte. Im Montgomery County (Maryland) beschwerte sich im März ein Wähler, dass er nicht den kompletten Wahlvorschlag bekommen und deshalb ein unvollständiges Votum abgegeben hatte; ihm war nur ein Teilausschnitt auf dem Bildschirm präsentiert worden. Bei den Vorwahlen im Frühjahr konnten in Kalifornien wegen defekter Steuerungsmodulen, die die Eingabe nicht freischalteten, und Systemen, die nicht booten wollten, zahlreiche Bürger in Alameda und San Diego nicht wählen. In San Diego ergab der Abgleich des Wahlregisters mit den registrierten Voten, dass zehn Stimmen verlustig gegangen waren. Eine Wählerin hatte bei

der Korrektur einer irrtümlichen Eingabe plötzlich zweimal gewählt, was die Smartcard eigentlich verhindern sollte.

Backup

Die peinlichen Pannen mit dem DRE-Equipment lassen sich vor der Öffentlichkeit nicht mehr verbergen. Die Dokumentationen, die Wissenschaftler wie David Dill auf www.verifiedvoting.org oder die Journalistin Bev Harris auf www.blackboxvoting.com und andere zusammengetragen haben, werden immer länger. Ob „Ausrutscher“, wie es die Firmen in der Regel nennen, oder die Spitze eines Eisbergs – ohne die Möglichkeit zur parallelen Aus-

zählung herkömmlicher Stimmzettel lässt sich nicht entscheiden, ob die elektronische Erfassung zuverlässig den Wählerwillen widerspiegelt. Deshalb fordern engagierte Bürgergruppen von der „Electronic Frontier Foundation“ über „Votescam“ und „Verified Voting“ bis zu „SAVE – Secure, Accurate and Verified Elections“ und „National Ballot Integrity Project“ einhellig den „Voter-Verified Paper Audit Trail“ (VVPAT). Mitte Juli hatten 13 000 Wähler in Maryland eine Petition unterzeichnet, die für die November-Wahlen solch eine papierne „Buchungskontrolle“ verlangte – nicht mehr machbar, wie der Gouverneur erklären ließ.

Angesichts der wachsenden Besorgnis, dass die Computer-Urnen Manipulationen Tür und Tor öffnen, hatte Kalifornien im Herbst vergangenen Jahres beschlossen, den „Paper Trail“ bis 2006 einzuführen. Auf Bundesebene brachte der demokratische Abgeordnete Rush Holt im Repräsentantenhaus, unterstützt durch eine entsprechende Initiative Hillary Clintons im Senat, den Entwurf eines „Voter Confidence and Increased Accessibility Act“ ein, der – sofern sich dafür eine Mehrheit findet – bis zu den nächsten Kongresswahlen im November 2006 das angeschlagene Vertrauen in die Integrität der Stimmabgabe durch ein obligatorisches Paper-Backup wiederherstellen soll.

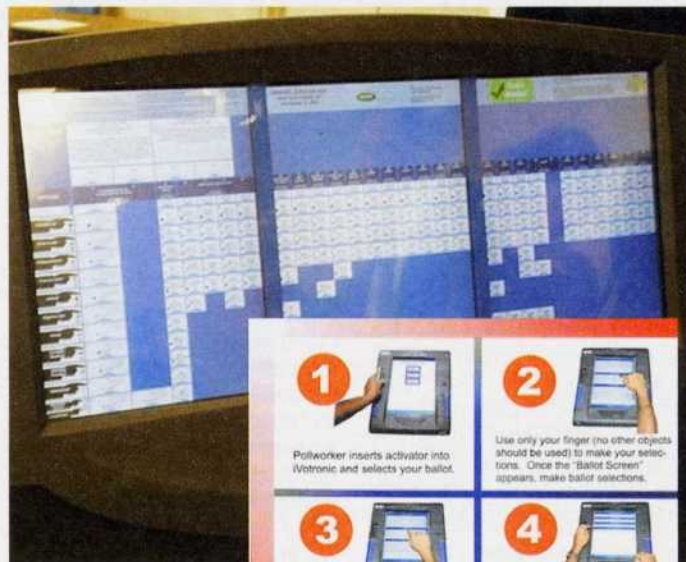
Aber „Paper Trail“ ist nicht gleich „Paper Trail“. Einige Her-



Wählen per Touchscreen statt mit dem Kugelschreiber

steller versuchen, den Forderungen mit Geräten zu entsprechen, die einen Ausdruck der intern gespeicherten Stimmen nach der Wahl ermöglichen. Sie sind der Meinung, dass die redundante Speicherung und kryptographische Verschlüsselung zur Sicherung der Daten ausreichen. Doch die „Zweitauszählung“ der Datensatzkopie reproduziert letztlich nur die Ergebnisse des ersten Datensatzes und kann kaum etwas anderes liefern als die erste Zählung. „Die Voten können – absichtlich oder zufällig – schon vorher in dem Verfahren verfälscht worden sein, sodass die abgespeicherten Daten korrekt erscheinen, es aber nicht sind“, sagt Rebecca Mercuri. Sie beharrt unerbittlich auf einem Paper Audit Trail. In ihren Augen macht das Belegwesen nur dann Sinn, wenn es tatsächlich einer zweiten, unabhängigen Auszählung dient.

Ein System, das die echte Stimmenverifizierung per Papier ermöglicht, ist der Vote-Tracker EVC-308SPR von Avante International Technology, Inc. Der Wähler initialisiert die Stimmabgabe durch eine kontaktlose Smartcard; geschrieben wird das DRE-Votum auf Flashspeicher und Festplatte, und parallel dazu wird der vom Wähler verifizierte Wahlzettel in einer Urne gesammelt. Nach der Schließung werden die elektronischen Daten auf eine einmal beschreibbare CD-R kopiert und diese mit der Urne ins Wahlamt gebracht. Mit diesem System sind, so die Electronic Frontier Foundation, bisher keine Probleme bekannt ge-



Das Wahlsystem „iVotronic“ von ES&S mit Anleitung dazu

- 1**
Pollworker inserts activator into iVotronic and selects your ballot.
- 2**
Use only your finger (no other objects should be used) to make your selections. Once the "Ballot Screen" appears, make ballot selections.
- 3**
If you wish to change a selection, retouch your first choice to cancel it and then touch your new choice.
- 4**
Review your final ballot selections on "Review Screen."
- 5**
Once you are satisfied with your choices, press the "Vote" button. You have just cast your ballot!

Touch VOTE the future

worden. Die Frage ist nur, wie eine derartige Zweigleisigkeit von Papier und Elektronik in der Praxis gehandhabt werden soll. Der Holt-Gesetzentwurf strebt die Zweitauszählung nur in Stichproben von 0,5 Prozent aller Wahlbezirke an; Aktivisten wie Victoria Collier halten das für Augenwischerei und bestehen auf der vollständigen und öffentlichen Auszählung aller Stimmzettel, um die Transparenz des Verfahrens zu retten.

Blackbox

Computer sind undurchsichtige Kästen. „Nur Techniker verstehen diese Systeme.“ So brachte unlängst Ann McGeehan unfreiwillig ihre Hilflosigkeit zum Ausdruck – dabei ist sie die Wahlamtsleiterin im texanischen Innenministerium. „Die Techniker müssen bestätigen, dass die Systeme sicher sind und ihren Zweck erfüllen“, forderte McGeehan. Vor dem Blackbox-Problem müssen auch die internationalen Wahlbeobachter passen, die im Auftrag der OSZE die-



Der Abgeordnete Rush Holt will mit seiner Gesetzesinitiative Papierbelege, die Offenlegung des Quellcodes und ein Verbot der Funkvernetzung von Wahlcomputern erreichen.

fizierungsprozess ist das Vertrauen nicht wert, das in ihn gesetzt wird“, beschreibt der Informatiker David Jefferson aus der DRE-Taskforce des kalifornischen Innenministeriums die Lage. „Er ist kaputt, er war nicht für die Ära softwaregesteuerter Wahlen konzipiert und funktioniert nicht“.

Selbst wenn Aufkleber auf den Geräten ein Zertifikat ausweisen, kann der Wähler nicht sicher sein, dass sich das zertifizierte System tatsächlich auch darin befindet. Bislang gibt es offenbar keine Garantie dafür, was genau am Wahltag zum Einsatz kommt. Als im November 2002 Wahlhelfer in South Dakota bemerkten, dass ein Gerät Stimmen doppelt zählte, machten die Techniker von ES&S als Fehlerquelle einen defekten Chip aus, doch anstatt

ses Mal die Präsidentenwahl verfolgen und am 4. November eine vorläufige Einschätzung abgeben werden (siehe dazu das Interview auf S. 101).

Während die Geräte munter angeschafft wurden, konnte die Regelung der Anforderungen, Prüfverfahren und Zertifizierungen mit der Technikgläubigkeit der politischen Akteure nicht Schritt halten. In den föderalistisch zweigeteilten Zuständigkeiten hat der „Help America Vote Act“ das Durcheinander eher noch vergrößert. „Der Zerti-

das Gerät aus dem Verkehr zu ziehen, wechselten sie kurzerhand vor Ort den Baustein aus. Die Journalistin Bev Harris hat in ihrem Buch „Blackbox Voting“ den lockeren Umgang mit Software-Updates und Patches dokumentiert. Eine Wahlvorsteherin im San Juan County im Bundesstaat Washington berichtete ihr, dass sie Updates ohne weitere Installationsanweisungen auf Diskette mit der Post bekam und dann einfach einspielte.

In diesem Jahr musste Diebold einräumen, bei den Vorwahlen in 17 kalifornischen Abstimmungsbezirken nichtzertifizierte Software eingesetzt zu haben; damit stand die Firma nicht allein – Konkurrent ES&S hatte das in 41 Counties des Staates Indiana ebenso gehandhabt. Der Skandal öffnete vielen Bürgern die Augen. Unter dem Druck der Öffentlichkeit griff der kalifornische Innenminister Kevin Shelley im April zur Notbremse und untersagte den Einsatz der rund 14 000 AccuVote-Touchscreen-Systeme, die Diebold an vier Landkreise verkauft hatte, weil deren Soft-

Monitors of Modern Art. LG.

Kunst und Technik in Aktion. TFT-Flachbildschirme von LG machen jedes Bild zu einem Meisterwerk. In jedem Detail zeigen sich die Erfahrung und Kompetenz eines weltweit führenden Monitorherstellers. LG steht für bestechende Produktqualität und zuverlässige Performance. Innovative Technologie und herausragendes Design von LG machen Ihren Arbeitsplatz zur Modern Art-Galerie. LG. Life's Good.

www.lge.de

Life's Good  LG

FLATRON
freedom of mind

red dot design award
winner 2007

iF
award
winner
2007

Das „Vote-Trakker EVC-308SPR“ von Avante bietet einen verifizierbaren Ausdruck auf Papier (unter Glas) als „Paper Audit Trail“.



ware nicht mit der lizenzierten Version übereinstimmte. Im Juli bestätigte ein Gericht die Rechtmäßigkeit der Entscheidung und wies die von den betroffenen Counties Riverside, San Bernardino, Kern und Plumas sowie von einem Behindertenverband beantragte einstweilige Verfügung gegen Shelleys Vorgehen ab.

Die Update-Zwänge sind unvermeidlich; sie bei rund einer Million Wahlcomputern unterschiedlicher Hersteller in landesweit 185 000 Wahllokalen unter Kontrolle zu halten, ist alles andere als eine triviale Aufgabe. Viele Fachleute halten sie nicht für beherrschbar. Auch noch so gründliche Prüfungen der Geräte vor, während oder nach einer Wahl, meint beispielsweise Rebecca Mercuri, können keinen

hinreichenden Schutz vor absichtlichem Hacking, Hardware-Fehlfunktionen oder Programmierfehlern gewährleisten. „Das liegt teilweise an der inhärent unlösbaren Aufgabe sicherzustellen, dass computerisierte Produkte keine unbekanntenen, zusätzlichen Features enthalten.“ Selbst Pioniere des Open-Source-e-Vo-

ting haben inzwischen ernüchtert festgestellt, dass die Offenlegung des Quellcodes wenig zur Lösung beiträgt. Dass „ein gut platzierter Microcode-Bug nahezu unmöglich zu entdecken“ ist und „kein Aufwand an Prüfung oder Verifikation auf Quellebene“ verlässlich vor Angriffen schützen kann, hat bereits vor zwei Jahr-

zehnten der Unix-Schöpfer Ken Thompson bei der Verleihung des Alan-Turing-Preises eindrucksvoll demonstriert.

Vertrauen

Eine Antwort auf das Blackbox-Problem hat der Informatik-Professor Douglas Jones von der University of Iowa vorgeschlagen: Am Wahltag nehmen die Prüfer unangemeldet in stichprobenartig ausgewählten Wahllokalen Maschinen aus dem tatsächlichen Wahlgang heraus und lassen daran Testwähler ein Votum abgeben, das separat protokolliert und mit der elektronischen Zählung der betreffenden Maschine verglichen wird. Mit repräsentativen Stichproben könnten solche Input-/Output-Analysen Vertrauen in die korrekte Zählung schaffen.

Auch dieser Ansatz überzeugt nicht jeden. Denn derartige Stichproben sind naturgemäß nur in geringem Umfang durchführbar, und wie eine Studien-Gruppe an der Yale University zeigte, können schon Manipula-

Open Source Voting

Wenn proprietärer Code und Blackbox-Systeme das Problem sind, ist dann Open Source die Lösung? Jason Kitcat von der Science Policy Research Unit (SPRU) an der britischen University of Sussex hat das eine Zeitlang geglaubt. Ende der 90er Jahre initiierte er GNU.FREE, das erste freie Software-Projekt zum E-Voting. Inzwischen hat er das Projekt aufgegeben. „Der Gewinn an Systemqualität, den die Offenlegung des Quellcodes bewirken könnte, reicht nicht aus, um die beträchtlichen Risiken für den Wahlprozess aufzuwiegen, die alle Formen des E-Voting bergen“, meint Kitcat heute.

Mit der Offenlegung des Quellcodes allein seien die Probleme mit Insider-Attacks, der korrekten Identifizierung von Wählern unter Wahrung der geheimen Stimmabgabe sowie der Schaffung vertrauenswürdiger Prüfmechanismen ohne Untergrabung der Wähler-Anonymität nicht zu lösen. „Auch mit noch so vielen pfiffigen technischen Vorkehrungen“, so sein Fazit, „verschleiert und vernebelt die Technologie den Wahlvorgang und

schafft dabei mannigfache Möglichkeiten für Betrügereien.“

Dass die offene Prüfung der Software-Architektur und des Quellcodes tendenziell die System-sicherheit voranbringt, glaubt Kitcat nach wie vor. Die eigentliche Schwachstelle liegt für ihn jedoch nicht beim Versionsmanagement in der Entwicklung, sondern beim Einsatzmanagement in der Praxis, wo es beispielsweise darum geht, welche Version am Wahltag wo zum Einsatz kommt.

Die Erfahrungen in Australien scheinen diese Einschätzung zu bestätigen. Als die Regierung in Canberra vor vier Jahren nach einem elektronischen Wahlsystem Ausschau hielt, rief das den Schöpfer des Samba-Servers Andrew Tridgell auf den Plan, der seinerzeit als Entwickler für die OzLabs von Linuxcare arbeitete. Weil Tridgell erkannte, dass Linuxcare für die Teilnahme an der öffentlichen Ausschreibung schlecht gerüstet war, ging er eine Kooperation mit dem Geschäftspartner Software Improvements Pty. Ltd. ein, die dann auch den Zuschlag erhielt. Die gemein-

sam entwickelte Software „Electronic Voting And Counting System“ (EVACS) wurde vom Auftraggeber, der Wahlkommission des Australian Capital Territory (ACT), unter die GNU GPL gestellt und in Pilotprojekten 2001 sowie im Oktober 2004 eingesetzt; auf der ACT-Webseite kann man das Paket noch downloaden.

Aber die Dinge kamen anders als erwartet. Weil Linuxcare in wirtschaftliche Schwierigkeiten geriet und Mitarbeiter entlassen musste, wurde die Steuerung des Projektes an den Geschäftspartner abgegeben. Zwar will Software Improvements an der GPL für EVACS nichts ändern, doch die Firma arbeitet inzwischen an einem „völlig neuen“, proprietären System. Tridgell hält die Geschäftspolitik der Firma für legitim und mag darin kein „Hijacking EVACS“ erkennen. Er findet es nur nicht in Ordnung, dass das neue System ebenfalls EVACS heißen soll. Die Fahne zur Weiterentwicklung der freien E-Voting-Software EVACS hält zurzeit noch Scott Ritchie, Student an der University of California Davis, mit der kürzlich von ihm

initiierten Open Voting Foundation hoch. „Open Source ist einfach ein Muss zur Schaffung vertrauenswürdiger elektronischer Wahlsysteme“, ist Ritchie überzeugt. „Obwohl noch einige technische Arbeiten zu leisten sind, um nachprüfbar Wahlbelege zu implementieren, steht jetzt vor allem das Krawatten-Marketing an, beispielsweise auf Zertifizierungsveranstaltungen Bürokraten zu erklären, wie man dem System trauen kann.“

Jason Kitcat sieht das alles etwas abgeklärter. Er kennt die OSS-Szene zu gut, um sie als Wundermittel zu betrachten, bei dem Heerscharen von Entwicklern sich auf das Ausmerzen von Bugs stürzen, nur weil der Quellcode offen liegt. „In Wirklichkeit zieht nur ein winziger Bruchteil von OSS-Projekten Beiträge an; dabei handelt es sich in der Regel um Software, die sehr häufig benutzt wird, während die meisten Projekte, bei denen sich nur ein einziger Entwickler um den Code kümmert, dahinschlummern. Deshalb ist E-Voting für die meisten potenziellen Entwickler nicht sonderlich attraktiv.“



Wahlvorbereitungen im Pasco County (Florida), iVotronics-Geräte werden installiert: Müssen die Wähler geschult werden oder kommen sie mit der Technik allein zurecht?

dem direkten Weg in eine Legitimationskrise seines politischen Systems befindet. (jk)

Literatur

[1] Kritische Aktivisten zu den US-Wahlsystemen:

- Electronic Frontier Foundation: www.eff.org/Activism/E-voting/
- Blackbox-Voting (Bev Harris): www.blackboxvoting.com
- Notable Software (Rebecca Mercuri): www.notablesoftware.com/evote.html
- Verified Voting (David Dill): www.verifiedvoting.org
- Votescam (Victoria Collier): www.votescam.com
- Secure, Accurate and Verified Elections (SAVE): www.wesave democracy.org
- National Ballot Integrity Project: www.ballotintegrity.org **ct**

tionen, die nur einen winzigen Bruchteil der Wählerstimmen verfälschen, zu einem völlig anderen Ergebnis führen. Wenn die Wahl des Jahres 2000 zu 90 Prozent an elektronischen Urnen durchgeführt worden wäre, so ihre Analyse, dann hätte pro Wahlmaschine bereits ein einziges zu Gunsten von Gore manipuliertes Votum ausgereicht, um in Florida und New Mexico den Demokraten klar siegen zu lassen. Bei zwei Fälschungen pro Maschine wären auch die Staaten Wisconsin und Iowa gekippt.

Besonders in einem Kopf-an-Kopf-Rennen brauche ein Saboteur nur Codeänderungen mit kaum wahrnehmbaren Auswirkungen in die Software einzuschleusen, um das Ergebnis in die gewünschte Richtung zu lenken. Die Schlussfolgerung des Yale-Teams: „Obwohl solche geringfügigen Manipulationen das Wahlergebnis wesentlich verändern, sind sie jeweils klein genug, um gänzlich unentdeckt zu bleiben und im inhärenten „Rauschen“ des Wahlvorgangs und der Wahlprüfung unterzugehen.“

Die Vereinigten Staaten haben offensichtlich ein Problem, und das liegt nicht allein in der Person des jetzigen oder künftigen Präsidenten: Aufgrund der ersten Erfahrungen mit der Stimmabgabe am Computer sind viele Bürger hellwach geworden. Zwei Jahre nach dem Inkrafttreten des „Help America Vote Act“ ist unverkennbar, auf welch ein Spiel mit dem Feuer sich ihr Land mit dem Verzicht auf die öffentliche, transparente Auszählung der Stimmen eingelassen hat und dass es sich auf

3ware RAID 2004

LEISTUNGS-GOLDMEDAILLE für die 3ware® 9000 Series

Sie brauchen mehr Leistung? Dann gewinnen Sie diese mit den neuen SATA RAID-Controllern der 3ware 9000-Serie von AMCC. Die Serie 9000 ermöglicht mit ihrer erstaunlichen Geschwindigkeit - mehr als 400 MByte/s sequentielle RAID 5 Leseoperationen¹ und über 110 MByte/s RAID 5 sequentielle Schreiboperationen - sowie der Sicherheit einer echten Hardware RAID-Architektur, eine völlig neue Qualität an SATA RAID-Speicherlösungen.

Sie haben grosse Anforderungen an die Speicherkapazität? Sie können Single Arrays bis 4,8 TByte über 64-bit-LBA-Adressierung über einen Controller und mehr als 16 TByte auf einem einzelnen Server² aufbauen. AMCC entwickelte die 3ware 9000 Serie zudem, um zusätzliche Vorteile zu bieten, wie volle Unterstützung für 64-bit-Betriebssysteme und 128 MByte ECC-geschützte SDRAM, zur Entlastung von Systemressourcen und Netzausfallschutz³ für erhöhte Fehlertoleranz.

Wählen Sie nur das Beste

und erfahren Sie mehr unter

www.3ware.com/9000

oder rufen Sie an unter +00-800-3927-3000



¹Getestet mit intel iometer-Benchmark-Programm auf einem Zwei-Prozessor-Intel-Xeon- (2,4 GHz) System mit Phoenix BIOS, 512 MByte System-RAM, Microsoft Windows 2000 Advanced Server, 66-MHz-SATA RAID-Controller 3ware 9500S-8 und Maxtor 7Y250MQ, 250G, 7200 RPM-Laufwerke. ²Unterstützung für bis zu vier 3ware 9000-Controller pro System ³Allgemeine Verfügbarkeit Sommer 2004

AMCC und 3ware sind eingetragene Warenzeichen der Applied Micro Circuits Corporation. Alle anderen Warenzeichen sind Eigentum ihres jeweiligen Besitzers. Copyright © 2004 Applied Micro Circuits Corporation. Alle Rechte vorbehalten.

