Sicherheitsprobleme elektronischer Wahlauszählungssysteme in der Praxis

Christian Hessmann
christian@hessmann.de

Martin Pittenauer
martin@pittenauer.de

Yacine Gasmi
Marcel Winandy
Horst Görtz Institut für IT-Sicherheit
Ruhr-Universität Bochum
{yacine.gasmi, marcel.winandy}@trust.rub.de

Abstract: Elektronische Wahlgeräte werden zunehmend bei politischen Wahlen eingesetzt. Während Wahlcomputer den gesamten Wahlvorgang elektronisch erfassen und keine manuelle Nachvollziehbarkeit mehr ermöglichen, besitzen elektronische Hilfsmittel zur reinen Wahlauszählung weiterhin diesen Vorteil, da diese wie bisher mit Papierstimmzetteln arbeiten. Allerdings gibt es auch bei der IT-gestützten Wahlauszählung einige Sicherheitsrisiken, die Wahlmanipulationen zur Folge haben können, wenn den Ergebnissen der Geräte blind vertraut wird. Diese Arbeit beleuchtet praktische Erfahrungen mit einem elektronischen Wahlauszählungssystem, die während einer Wahlbeobachtung gemacht wurden. Wir zeigen, dass der Einsatz in der Praxis einige IT-sicherheitsrelevante Aspekte unzureichend behandelt. Wir diskutieren kurz Lösungsansätze zur Reduzierung der Probleme, wobei Kosten und Nutzen sich jedoch mit dem bewährten manuellen Auszählen von Stimmzetteln messen lassen müssen.

1 Einleitung

Wahlen sind ein zentraler Baustein unserer Demokratie. Daher ist deren sicherer und unverfälschter Ablauf von großer Bedeutung. Im Laufe der Zeit wurden Wahlvorgang und Auswertung durch verschiedene organisatorische Maßnahmen so optimiert, dass eine Manipulation äußerst unwahrscheinlich bzw. nur mit großem Aufwand zu realisieren ist.

Im Zeitalter der Digitalisierung, in dem IT in praktisch alle Bereiche unseres privaten und gesellschaftlichen Lebens Einzug erhalten hat, erscheint es nur konsequent, dass auch bei der Durchführung und Auswertung von Wahlen der Einsatz elektronischer Komponenten ins Gespräch kommt. Der rasante technologische Fortschritt wirft allerdings die Frage auf, ob die hohen Sicherheitsanforderungen weiterhin erfüllt bleiben, oder ob durch die Integration modernster Technik nicht bestehende Sicherheitsmechanismen ausgehöhlt werden.

In dieser Arbeit wird der Einsatz von Wahlauszählungssystemen aus IT-sicherheitstechnischer Sicht betrachtet. Wir beschränken uns dabei auf elektronische Hilfsmittel, die bei der Auszählung abgegebener Papierstimmzettel zum Einsatz kommen. Zunächst beleuchten wir die rechtlichen Anforderungen (Abschnitt 2) und geben einen Überblick über elektronische Wahlgeräte sowie frühere Arbeiten zu deren Sicherheitsproblemen (Abschnitt 3). Der Hauptbeitrag dieser Arbeit beschreibt praktische Erfahrungen, die während einer Wahl-

beobachtung der Kommunalwahl in Bayern gemacht wurde (Abschnitt 4). Es zeigte sich, dass derartige Systeme in der Praxis einige Sicherheitsrisiken aufwerfen. Abschließend skizzieren wir Lösungsansätze zur Verbesserung der beobachteten Probleme (Abschnitt 5).

2 Rechtliche Anforderungen

Die Durchführung demokratischer Wahlen ist in Deutschland durch eine Reihe von Gesetzen und Verordnungen auf Bundes-, Landes- sowie kommunaler Ebene geregelt. Die Grundlage bildet auch hier das Grundgesetz, das in Art. 38 Abs. 1 S. 1 GG verlangt, dass die „Abgeordneten des Deutschen Bundestages [...] in allgemeiner, unmittelbarer, freier, gleicher und geheimer Wahl gewählt" werden. Genauso muss in den „Ländern, Kreisen und Gemeinden [...] das Volk eine Vertretung haben, die aus allgemeinen, unmittelbaren, freien, gleichen und geheimen Wahlen hervorgegangen ist" (Art. 28 Abs. 1 S. 2 GG).

Zur Umsetzung der im Grundgesetz verankerten Vorgaben sind im Bundeswahlgesetz (BWG) und der Bundeswahlordnung (BWO) (sowie deren Pendants auf Landes- und kommunaler Ebene) konkrete Anforderungen und Maßnahmen bezüglich der Vorbereitung, Durchführung und Auswertung von Bundes- bzw. Landes- oder Kommunalwahlen formuliert. Unter anderem ist darin festgelegt, dass „anstatt von Stimmzetteln und Wahlurnen (amtlich zugelassene) Wahlgeräte benutzt werden" können (§35 Abs. 1 BWG). Deren Einsatz ist wiederum insbesondere in der Bundeswahlgeräteverordnung (BWahlGV) geregelt[1], die u.a. konkrete Anforderungen an die zu verwendenden Wahlgeräte definiert. Diese sehen u.a. vor, dass Wahlgeräte die Geheimhaltung der Stimmabgabe sowie eine vollständige, eindeutige und richtige Zählung der Stimmen gewährleisten müssen (Anlage 1 zu §2 Teil B Abs. 3.4 BWahlGV).

Um sicherzustellen, dass sich ein Wahlgerät in ordnungsgemäßem Zustand befindet, muss das Gerät u.a. eine „eindeutige Identifikation der installierten Software" (Anlage 1 zu §2 Teil B Abs. 1 BWahlGV) gewährleisten. Einer Manipulation des Gerätes soll dadurch entgegengewirkt werden, dass „das Wahlgerät [...] so aufgebaut (sein muss), daß eine Veränderung des technischen Aufbaus und [...] der installierten Software durch unbefugte Dritte nicht unbemerkt bleibt" (Anlage 1 zu §2 Teil B Abs. 2.1 BWahlGV). Dazu muss „das Wahlgerät [...] die Kontrolle seiner Funktionalität (sowie) die Anzeige von [...] Funktionsfehlern seiner Komponenten" (Anlage 1 zu §2 Teil B Abs. 3.2 BWahlGV) ermöglichen.

Die derzeit gültige Fassung der BWahlGV stammt vom 20.4.1999, ein Umstand, der verdeutlicht, dass der rasante Fortschritt im IT-Bereich nur unzureichend Berücksichtigung findet. Die genannten Anforderungen zeigen jedoch, dass der Einsatz elektronischer Wahlgeräte den korrekten und unverfälschten Ablauf der Wahl nicht gefährden darf. Soweit die Theorie – wie dies in der Praxis aussieht, wird im folgenden Abschnitt beschrieben.

[1] Änderungen der BWahlGV sind in der *Verordnung zur Änderung der Bundeswahlgeräteverordnung und der Europawahlordung* vom 20.4.1999 festgehalten.

3 Einsatz von Wahlgeräten und elektronischer Hilfsmittel

Wahlcomputer sind Geräte, die den Wahlvorgang und die Auszählung komplett elektronisch erfassen. In Deutschland werden bereits seit mehreren Jahren in einigen Städten (z.B. Köln [Sta]) solche Systeme für Kommunal-, Landtags-, Bundestags- und Europawahl eingesetzt. Die Stimmenabgabe und Auszählung erfolgt vollständig elektronisch. Für eine nachträgliche Prüfung der Wahlergebnisse muss man sich ganz auf die elektronisch erzeugte Ausgabe verlassen. Eine manuelle Nachvollziehbarkeit ist nicht möglich.

Dill et al. [DSS03] haben bereits auf die generelle Problematik mit papierlosen Wahlmaschinen aufmerksam gemacht: Die gesamten internen Vorgänge sind vor dem Wähler versteckt. Kohno et al. [KSRW04] haben den Quellcode der eingesetzten Software eines Wahlcomputers von Diebold analysiert und zahlreiche Sicherheitsprobleme entdeckt, die sowohl Angriffe von Außen- als auch Innentätern (z.B. Wahlhelfer) ermöglichen. Feldman et al. [FHF07] haben die Hardware des Diebold-Wahlcomputers untersucht und herausgefunden, dass ein Angreifer in der Lage sei, innerhalb einer Minute Schadsoftware auf dem Wahlcomputer zu installieren, die die Wahlergebnisse manipulieren könnte. Kurz und Rieger [KR07] beschreiben Manipulationsmöglichkeiten an Hard- und Software des Nedap-Wahlcomputers, der vor allem in Deutschland und Europa eingesetzt wird.

Um die Anforderung der Nachvollziehbarkeit aufrecht zu erhalten, gibt es verschiedene Ansätze für Geräte zur *Wahlunterstützung*. Diese werden nur bei der Stimmenauszählung eingesetzt und verwenden weiterhin einen Papierstimmzettel. Der Digitale Wahlstift [dot] ist beispielsweise eine Art Kugelschreiber mit eingebauter Kamera, der das Ankreuzen auf dem Stimmzettel digital einscannt und an einen PC zur Auszählung übermittelt. Der Wahlstift wurde ursprünglich für den Einsatz bei der Bürgerschaftswahl 2008 in Hamburg geplant und wird derzeit gemäß einem Common Criteria Schutzprofil [Wah07] evaluiert.

Während der Wahlstift bereits bei der Stimmabgabe zum Einsatz kommt, wird das Wahlunterstützungssystem OK.Wahl [Ans07] ausschließlich von den Wahlhelfern zur Stimmenauszählung eingesetzt. Diese erfolgt mittels Barcode-Scanner, der an einen gewöhnlichen PC mit Windows-Betriebssystem und darauf laufender OK.Wahl-Software angeschlossen ist. Die Stimmzettel werden wie gewohnt vom Wähler angekreuzt, besitzen aber neben jedem ankreuzbaren Feld zusätzlich einen Barcode. Die Auszählung erfolgt über Einscannen der Barcodes neben den angekreuzten Feldern. Die Software summiert die eingescannten Stimmen und berechnet somit elektronisch das Wahlergebnis. Die Bedienung der Software ist unterteilt in eine Eingabeansicht für den aktuellen Stimmzettel und eine Übersichtsansicht für die akkumulierten Stimmen aller bisher eingegebenen Zettel.

4 Wahlbeobachtung in Bayern

Ein Teil der Autoren hat am 02.03.2008 die Kommunalwahl in Bayern beobachtet, mit besonderem Augenmerk auf den Einsatz der beschriebenen IT und damit verbundene Vor- und Nachteile gegenüber der konventionellen Methode. Die Beobachtung fand dabei in Germering in ungefähr der Hälfte der Wahllokale statt. Durch Austausch mit anderen Wahlbeobachtern konnten wir auch Stimmungsbilder aus den Wahlbezirken Ahorn, Coburg, Pfaffenhofen an der Ilm, Kleinaitingen und Murnau gewinnen.

In Germering kann man unserer Einschätzung nach von optimalen Bedingungen und vorbildlicher Umsetzung sprechen: Die nötigen Rechner wurden zeitnah für die örtliche Schule beschafft und erzeugten so weder wesentliche Kosten, noch hatte die Gemeinde ein Problem mit der Bereitstellung ausreichender Kapazitäten. Trotz unterschiedlich gut geschulter Wahlhelfer (von Computerlaie bis Fachkraft) im Umgang mit der eingesetzten Software OK.Wahl stellte sich durchwegs ein Zeitvorteil bei der Auszählung ein. Nach Rücksprache mit erfahrenen Wahlhelfern kann man hier realistisch eine Auszähldauer von im Mittel 4,5 Stunden statt der bei Kommunalwahlen üblichen sechs Stunden annehmen.

Jeweils zwei Helfer waren mit der Auszählung von Stadtrat- bzw. Kreistagsstimmen beschäftigt. Daraus ergab sich durch Schichtbetrieb ein niedriges Arbeitsvolumen für den einzelnen Wahlhelfer. Allerdings gestaltete sich die Durchführung von Kontrollen im Sinne des Zwei-Augen-Prinzips nicht unproblematisch: Während ein Helfer mit dem Scanner die Stimmen erfasste, musste der zweite Helfer sicherstellen, dass die eingelesene Stimme dem Wählerwillen entsprach und von der Software korrekt erfasst wurde. Dabei war ständiges Wechseln zwischen Wahlzettel und Monitor unvermeidlich.

Die korrekte Durchführung dieser Kontrolle wurde sehr unterschiedlich wahrgenommen. Es gab Teams von Wahlhelfern, die zu dritt oder viert das Auslesen beobachteten, sich jede Stimme laut vorlasen und mit „OK“ quittierten. Andere saßen zu zweit vor dem Computer, beide mit den Augen auf dem Stimmzettel auf der Suche nach Stimmen, während der Barcodeleser sehr schnell vor sich hin piepte und niemand den Bildschirm beobachtete. Solche Szenen konnten wir in ca. einem Drittel der besuchten Wahllokale beobachten - uns war es hier nicht mehr möglich mitzuverfolgen, ob das Einlesen der Stimmen korrekt erfolgte. Mehrfach bemerkte man erst nach dem fertigen Einlesen eines Stimmzettels, dass bereits seit geraumer Zeit eine Fehlermeldung auf dem Bildschirm stand und alle Eingaben vom Computer nicht angenommen wurden. Der Barcodeleser quittierte alle abgefahrenen Barcodes mit einem akustischen Signal, unabhängig vom Zustand der Software.

Nicht ein einziges Mal wurde der Fall beobachtet, dass die im Laufe der Auszählung addierten Ergebnisse auf ihre Korrektheit hin überprüft wurden. Vielen Wahlhelfern war die dazu nötige (und von der Software angebotene) Übersichtsansicht sogar unbekannt.

Im abschließenden Gespräch mit einem Wahlvorstand wurde uns von einigen Fällen berichtet, in denen beim Abfahren eines Kandidaten die Stimme fälschlicherweise für einen, in der Liste benachbarten, anderen Kandidaten gezählt wurde. Ob es sich hier um ein Problem mit der Software, einen Druckfehler oder menschliches Versagen handelte sei dahingestellt - es verdeutlicht aber die, auch bei der IT gestützten Auszählung gegebene essentielle Notwendigkeit von Sorgfalt und Kontrolle. Das Barcode Auszählverfahren erschwert dies unseren Beobachtungen nach, da automatisiert Abläufe entstehen, in denen Wahlhelfer sich auf eine möglichst schnelle Erfassung der Stimmen konzentrieren.

Ein weiterer Problemkomplex ergab sich unseren und anderen Beobachtungen nach im Bereich der Rechnerbeschaffung und -installation. In vielen Gemeinden wurden Rechner aus verschiedensten Einrichtungen sowie Privatbesitz zum Auszählen herangezogen. In Pfaffenhofen wurde z.B. auf 58 stadteigene PCs, 3 PCs von Behörden, Schulen und Kindergärten, 15 PCs von Stadtbediensteten, 4 PCs von amtierenden Stadträten und 8 PCs von Wahlhelfern zurückgegriffen. Die Stadt Starnberg suchte im Vorfeld der Wahl sogar

per Zeitungsinserat [Zei08] „rund 50 Wahlhelfer, die ihren eigenen PC oder ihr Notebook mitbringen und für die Stimmenerfassung zur Verfügung stellen".

Den Beobachtungen nach gab es für die Installation und den Zustand der jeweiligen Rechner keinerlei Vorgaben. Eine bunte Mischung an verschiedensten Windows-Versionen mit unterschiedlichster installierter Software kam zum Einsatz. Es ist uns kein Fall bekannt, in dem ein mitgebrachter Rechner zumindest auf Schadprogramme überprüft wurde.

Allen Beobachtungen gemein war das nahezu vollständige und unkritische Vertrauen der Helfer in die Software und die Technik. Die befragten Personen waren sich einig, dass die Software korrekt funktioniere und ausreichend getestet und zertifiziert worden sei. Der Gedanke, dass die Software Fehler enthalten könnte, die unentdeckt zu falschen Ergebnissen führen könnten, lag im Regelfall nicht nahe. In anschließenden Diskussionen mit Wahlvorständen wurden Kritikpunkte bezüglich der Durchführung der Wahl und der Erstellung und Zertifizierung der eingesetzten Software allerdings äußerst positiv aufgenommen.

5 Lösungsmöglichkeiten

Die Wahlbeobachtung in Bayern hat gezeigt, dass aus Kostengründen gerne auf bestehende, zum Teil sehr unterschiedliche Hardware zurückgegriffen wird. Um die aufgezeigten Probleme zu reduzieren, müssen zumindest eine Reihe von technischen Mindestanforderungen erfüllt sein. Zunächst muss sichergestellt sein, dass die Software zur Stimmenabgabe oder -auszählung ihre Aufgabe korrekt erfüllt. Da die elektronische Erfassung der Stimme für den Anwender nicht nachvollziehbar ist, bietet sich nur eine Vorabprüfung der Software an, z.B. im Zuge eines Zertifizierungsverfahrens. Ein einfaches aber probates Mittel, mehr Transparenz bzgl. der eingesetzten Software herzustellen, stellt zudem die Offenlegung des Quellcodes dar. In beiden Fällen muss allerdings sichergestellt werden, dass die tatsächlich zum Einsatz kommende Software auch der Überprüften entspricht.

Eine Überprüfung der Wahlsoftware reicht jedoch nicht aus, da eine Manipulation durch andere Komponenten erfolgen kann, z.B. durch Schadprogramme, die Ein- und Ausgabewerte der Wahlsoftware modifizieren und so heimlich das Auszählungsergebnis verfälschen. Um dies zu verhindern, könnten in einem ersten Schritt bootfähige CDs eingesetzt werden, die neben der eigentlichen Software zur Stimmenauszählung ein komplettes Betriebssystem beinhalten. Da die Software auf der CD nicht verändert werden kann, wäre beim Starten des Systems von CD ein vordefinierter Systemzustand gewährleistet.

Allerdings können Schadprogramme bereits im BIOS, d.h. vor Starten der Boot-CD, aktiv werden. Insbesondere könnte durch den Einsatz von Virtualisierungstechnologien im BIOS eine Zwischenschicht (sog. „Hypervisor") zwischen das "sichere" Betriebssystem auf der CD und die Hardware eingefügt werden, die dann die Stimmabgabe oder -auszählung für den Anwender unbemerkt manipulieren könnte. Dass derartige Angriffe nicht unrealistisch sind, zeigen aktuelle Entwicklungen bei führenden BIOS-Herstellern (z.B. [Pho07]) sowie erfolgreich demonstrierte Angriffe mit Virtualisierungstechnologie (z.B. [Blu]).

Einen Lösungsansatz für derartige Sicherheitsprobleme bietet die Trusted Computing Technologie der Trusted Computing Group [Tru]. Ein zentrales Prinzip der Technologie besteht darin, sämtliche Hard- und Softwarekomponenten eines Rechensystems vom initia-

len Bootvorgang an, d.h. inklusive Firmware und BIOS, vor der jeweiligen Ausführung zu überprüfen. Damit ließe sich feststellen, ob beim Hochfahren des Systems nur unmanipulierte und daher vertrauenswürdige Komponenten geladen wurden. Doch auch Trusted Computing ist nicht der Weisheit letzter Schluss, da zum einen kein wirksamer Schutz vor Angriffen auf Hardwareebene besteht und zum anderen unmodifizierte Soft- oder Hardwarekomponenten eine „korrekte" Stimmenabgabe oder -auszählung nicht per se garantieren.

6 Fazit

Wahlauszählungssysteme wie OK.Wahl, die weiterhin mit Papierstimmzetteln arbeiten, erfüllen im Gegensatz zu Wahlcomputern die Anforderung der Nachvollziehbarkeit. Die Beobachtung des Systems im praktischen Einsatz hat jedoch gezeigt, dass es sowohl Probleme bezüglich der Benutzerfreundlichkeit der Software als auch Sicherheitsrisiken bei der Ausführung gibt. Auch wenn prinzipiell die Wahlergebnisse manuell nachgezählt werden können, bleibt das Risiko bestehen, dass den Ergebnissen des Wahlauszählungssystems blind vertraut wird. Bereits verfügbare Sicherheitstechniken könnten die angesprochenen Probleme reduzieren, allerdings müssen ggf. steigende Kosten bei deren Einsatz gegenüber dem bewährten manuellen Auszählen von Stimmzetteln abgewogen werden.

Literatur

[Ans07] Anstalt für Kommunale Datenvearbeitung in Bayern (AKDB). OK.Wahl Wahlauswertung - Verfahrensinformation. `http://www.akdb.de/fileadmin/akdb/docs/okwahl_1.pdf`, August 2007.

[Blu] Blue Pill Project. `http://www.bluepillproject.org/`.

[dot] dotVote. Digitales Wahlstift-System dotVote. `http://www.dotvote.de/`.

[DSS03] David L. Dill, Bruce Schneier und Barbara Simons. Voting and Technology: Who Gets to Count Your Vote? *Commun. ACM*, 46(8):29–31, 2003.

[FHF07] Ariel J. Feldman, J. Alex Halderman und Edward W. Felten. Security Analysis of the Diebold AccuVote-TS Voting Machine. In *EVT'07: Proceedings of the USENIX/Accurate Electronic Voting Technology on USENIX/Accurate Electronic Voting Technology Workshop*, Seiten 2–2, Berkeley, CA, USA, 2007. USENIX Association.

[KR07] Constanze Kurz und Frank Rieger. NEDAP-Wahlcomputer - Manipulationsmethoden an Hard- und Software. *Informatik-Spektrum*, 30(5), 2007.

[KSRW04] Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin und Dan S. Wallach. Analysis of an Electronic Voting System. In *Proceedings of the IEEE Symposium on Security and Privacy*. IEEE Computer Society, 2004.

[Pho07] Phoenix Technologies Ltd. Phoenix HyperSpace Data Sheet, 2007. `http://www.phoenix.com/NR/rdonlyres/179EBA15-A24E-4D27-BD52-B4B7BEF80FA%6/0/HyperSpace_ds.pdf`.

[Sta] Stadt Köln. Wahlen in Köln: Elektronische Wahlgeräte. `http://www.stadt-koeln.de/wahleninkoeln/wahlgeraete/index.html`.

[Tru] Trusted Computing Group. `http://www.trustedcomputinggroup.org/`.

[Wah07] Common Criteria Schutzprofil Digitales Wahlstift-System, Version 1.0.1. `http://www.bsi.de/zertifiz/zert/reporte/PP0031b.pdf`, Februar 2007.

[Zei08] „Helfer mit PC gesucht". Kreisbote Landkreis Starnberg, 30. Januar, 2008.