Schriftliche Stellungnahme zur Anhörung Digitaler Wahlstift im Verfassungsausschuß der Hamburger Bürgerschaft

ROP GONGGRIJP, CONSTANZE KURZ, FRANK RIEGER[1]

15. November 2007

Einleitung

Diese schriftliche Stellungnahme für den Verfassungsausschuß der Freien und Hansestadt Hamburg kann notwendigerweise nur eine Wiedergabe des derzeit noch unvollständigen Erkenntnisstandes zu den vielfältigen und komplexen Risiken sein, die sich durch den Einsatz des Digitalen Wahlstift-Systems (DWS) ergeben. Durch den enormen Zeitdruck, unter dem die relevanten Entscheidungen gefällt werden sollen, und die bis dato immer noch nicht vorliegenden Evaluierungsberichte zu allen wesentlichen Zertifizierungen sowie die nicht verfügbare technische Dokumentation des Systems kann diese Stellungnahme daher nur schlaglichtartig einige Aspekte der mit dem DWS entstehenden Probleme beleuchten.

Die vielfältigen Risiken des DWS werden in dieser Stellungnahme an einem ausgewählten Beispiel, der Angreifbarkeit der dem Wahlstift zugrundeliegenden Digitalstifttechnologie, aufgezeigt. Das positionsbestimmende feine Muster auf dem Wahlzettel, das den Kern des DWS darstellt, ist entgegen den Behauptungen des Herstellers nicht gegen Kopie und Manipulation zu sichern. Die weitreichenden Folgen für die Sicherheit und die Vertrauenswürdigkeit des DWS werden entsprechend exemplarisch erläutert.

Schon die aus der derzeit noch knappen Informationslage erkennbaren Risiken des DWS sind so schwerwiegend und systemimmanent, daß dringend vor dem Einsatz des DWS bei demokratischen Wahlen gewarnt werden muß. Die Einführung eines so intransparenten, komplexen und

---

[1] Mitarbeit an der Stellungnahme: Dirk Engling, Hendrik Fulda, Karsten Schmidt.

sicherheitstechnisch riskanten Systems ist für den Wähler gleichbedeutend mit der Abschaffung seines Rechts auf ein transparentes, von ihm selbst überprüfbares Wahlsystem.

Im Kern stellt das DWS eine Computerwahl dar, bei der beim Wähler durch Verwendung der Digitalstifttechnologie nur die Illusion einer Papierwahl erzeugt wird. Der Wähler erwartet jedoch mit Recht, daß seine Stimme auf dem Papier der Ausdruck seines Wählerwillens ist. Daß stattdessen ausschließlich eine manipulierbare digitale Abbildung als Stimme gewertet wird, ist ein tiefgreifender Vertrauensbruch, der eine ernste Gefahr für die Demokratie darstellt. Die Legitimität des politischen Mandats sollte in einer Demokratie jedoch über jeden Zweifel erhaben sein. Die aus dem DWS resultierende Abschaffung der vollständigen Nachprüfbarkeit des Wahlergebnisses durch den Wähler unterminiert diese Legitimität nachhaltig.

Der Chaos Computer Club (CCC) empfiehlt mit Nachdruck, die Papierstimme als alleinigen Ausdruck des Wählerwillens dauerhaft festzuschreiben. Auch der Einsatz des DWS als bloße Zählhilfe ist nur dann zu rechtfertigen, wenn eine Festschreibung des Primats der Papierstimme erfolgt. Selbst ein vermeintlich erfolgreicher Testlauf des DWS als Zählhilfe mit möglicherweise nur wenigen Diskrepanzen zwischen Papier- und Computerergebnis belegt keine Manipulationssicherheit des Systems. Die Möglichkeit einer digitalen Wahlfälschung wird erst sicherheitskritisch, sofern das vollständige Nachzählen unterbleibt.

Dynamik neuer Angriffsmethoden

Die Einführung von computergestützten Wahlverfahren wie dem DWS eröffnet einen dynamischen Prozeß der Entwicklung von Angriffs- und Manipulationsmethoden, bei dem die im folgenden dargelegten Beispiele erst der Anfang einer langen Reihe sind. Für Wahlen mit Papier und Stift sind mögliche Manipulationsverfahren seit Jahrzehnten bekannt und werden mit sehr einfach zu befolgenden und von jedem Wähler logisch erschließbaren prozeduralen Methoden verhindert. Die einfache Überprüfbarkeit von Papier-und-Stift-Wahlen durch jeden Wähler bildet den entscheidenden Sicherheitsfaktor unseres Wahlsystems, der in der Vergangenheit die Entdeckung von Wahlfälschungen auch unter widrigen Umständen erlaubte. Die Einfachheit und Transparenz des Wahlverfahrens bildet mithin die Grundlage des Vertrauens zwischen Wähler und Gewähltem.

So entsendet die Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE) international Wahlbeobachter, um Unregelmäßigkeiten im Verlauf eines Wahlverfahrens feststellen zu können. Eine effektive Kontrolle des Wahlprozesses ist mit dem Einsatz von Computern als zentralem Element der Wahl jedoch nicht mehr möglich. Ebenso wie der Wähler muß auch der Wahlbeobachter wesentliche Teile des computerisierten Wahlverfahrens als intransparente „Black Box“ hinnehmen, in die kein Einblick möglich ist.

Demgegenüber ist die Entwicklung von Angriffsmethoden und Manipulationsverfahren in der Computertechnik ein hochdynamischer Prozeß, bei dem in sehr kurzen Zeiträumen neue Erkenntnisse entstehen. Vorherige Annahmen über die notwendigen Sicherheitsmaßnahmen eines Computerwahlverfahren werden damit schnell obsolet. Das kontinuierliche Verfolgen aktueller Entwicklungen, das Nachvollziehen der Angriffsmethoden und die Beurteilung der Risikoentwicklung ist nur von Experten zu leisten. Dies erfordert erhebliche Aufwendungen und führt in der Praxis immer nur zu einem beschränkten Erfolg, da Hersteller und Betreiber des DWS stets in der Defensive sind. Die Überprüfbarkeit des Vorhandenseins und der Wirksamkeit etwaiger Schutzmaßnahmen durch den Wähler ist nicht zu realisieren – und beim Digitalen Wahlstift offenbar auch nicht vorgesehen.

Die Publikation eines neuen Angriffsverfahrens kurz vor der Wahl im Februar kann dazu führen, daß kurzfristig eine Umrüstung von DWS-Komponenten erforderlich würde, die bedingt durch die Notwendigkeit der Durchführung einer Nachzertifizierung nach jeder noch so geringfügigen Änderung am System in der Kürze der Zeit nicht zu leisten wäre. Auch eine Ausmusterung des DWS kann in Frage kommen. Eine solche Situation ist in anderen Staaten bereits entstanden. So wurde in den Niederlanden bei den letzten Parlamentswahlen, nachdem die Sicherheitsmängel an den dort verwendeten Wahlcomputern der Firmen NEDAP und SDU bekannt wurden, kurzfristig wieder auf Papier und Stift umgestellt. Die Kosten mußten selbstverständlich die Gemeinden tragen.

Die benötigte Zeitspanne der von der Physikalisch-Technischen Bundesanstalt (PTB) für die Bauartzulassung der NEDAP-Wahlcomputer durchgeführten Prüfungen ist ein Beispiel dafür, wie schnell Sicherheitsannahmen von der Publikation neuer Angriffe überholt werden, ohne daß eine adäquate und schnelle Reaktion erfolgen kann. Das DWS ist dabei wesentlich komplexer als die NEDAP-Wahlcomputer. Das heißt, daß das DWS deutlich mehr Komponenten hat, die Sicherheitsprobleme und Manipulationsrisiken aufwerfen. Zudem ist eine Nachzertifizierung

des Systems nach erfolgter Problembehebung aufwendiger und dauert länger.

Als Referenz für die Dauer von Nachzertifizierungen können hier beispielhaft die Nachbesserungen an den NEDAP-Wahlcomputern dienen. Von der Publikation der Sicherheitslücken bis zur erneuten Bauartzulassung und Verwendungsgenehmigung für eine nur notdürftig und unzulänglich nachgebesserte Version verging mehr als ein Jahr. Das DWS ist jedoch nicht nur technisch angreifbarer als die NEDAP-Wahlcomputer, seine Verwendbarkeit hängt auch von mehreren und weitaus komplexeren Zertifizierungen als nur der PTB-Bauartzulassung ab. Daher ist absehbar, daß es beim DWS zu kritischen Situationen kommen wird, in denen der Wahlleiter entscheiden muß, ob er eine zertifizierte, aber bekannt manipulierbare Version des DWS einsetzt. Die Möglichkeit, eine fehlerkorrigierte Version, die nicht vollständig zertifiziert und zugelassen ist, einzusetzen, besteht nicht, denn dies würde die Wahl anfechtbar machen.

Die grundlegende Dynamik der Angriffe gegen computerisierte Wahlen ist ein wesentlicher Risikofaktor, der ohne eine tatsächliche Notwendigkeit durch den Einsatz des DWS in Kauf genommen wird. Im Gegensatz zum altbewährten Verfahren mit Papier und Stift können jederzeit auch bislang unbekannte, nicht vorhersehbare Angriffsmethoden entwickelt werden, die unerkannt bleiben und eine Wahlfälschung ermöglichen. Selbst ein sehr gründlicher Zertifizierungsprozeß ermöglicht es nicht, diesen Risikofaktor zu eliminieren, und ersetzt ohnehin nicht die rechtlich vorgeschriebene Nachprüfbarkeit durch den Wähler.

Beispielhafter Angriff gegen das Anoto-Muster auf dem Stimmzettel

Das für die korrekte digitale Erfassung der Stimme auf dem Wahlzettel bestimmende Merkmal ist das kaum sichtbare, auf dem gesamten Wahlzettel aufgedruckte Punktemuster. Dieses Muster wird von der schwedischen Firma Anoto hergestellt und an Dienstleister wie etwa den Lieferanten des Wahlstift-Systems bereichsweise lizenziert. Mit Hilfe des Musters kann der Wahlstift identifizieren, auf welcher Seite und an welcher genauen Position des mehrseitigen Wahlzettels er sich befindet. Dazu nimmt eine in den Stift eingebaute Kamera im Infrarotbereich einen kleinen Teilbereich des Musters auf, sobald die Stiftmine auf das Papier aufgesetzt wird. Da die Kamera nur infrarotes Licht aufzeichnet,

entsteht ein Bild, das sich von einem mit bloßem Auge sichtbaren Bild unterscheidet. In diesem Bild sucht der in den Stift eingebaute Computerchip nach den charakteristischen Punkten, die er zur Positionsbestimmung benötigt. Dabei folgt der Stift einem vorprogrammierten Code, der es ihm erlaubt, das Muster in eine genaue Position umzurechnen.

Der vom CCC vorgestellte Angriff zielt auf den Kern des Wahlstift-Systems, eben jenes positionsbestimmende Muster. Dazu wird im ersten Schritt eine digitale Kopie des Musters und der Beschriftung auf dem Wahlzettel erzeugt, indem der Wahlzettel mit einem leicht modifizierten Flachbettscanner in sehr hoher Auflösung erfaßt wird. Dabei werden zwei Arbeitsgänge durchgeführt. Zunächst wird das optischen Aussehen des Wahlzettels im sichtbaren Bereich ermittelt, danach die präzise Erfassung des Musters im Infrarotbereich vorgenommen. Mit Hilfe eines Filteralgorithmus werden nun beide Bilder voneinander subtrahiert. Als Ergebnis liegt nun einerseits der für den Stift sichtbare Bereich im Infrarotlicht und andererseits der für den Stift unsichtbare Bereich im normalen Licht als hochauflösende Bilddatei vor. Anschließend kopiert der Wahlfälscher nach Belieben die positionsbestimmenden Muster aus dem Feld der zu begünstigenden Partei in eine oder mehrere andere Felder, so daß der Wahlstift in diesen Feldern eine falsche Positionsinformation erhält. Zum Schluß werden beide Bilddateien übereinandergedruckt. Dabei wird das positionsbestimmende Muster für die Erfassung durch den Stift in kohlenstoffhaltiger, Infrarot-absorbierender Tinte gedruckt, genau wie beim Stimmzettel-Original.

Ergibt das erfaßte Muster auf einem Wahlzettel zusammen mit dem vorprogrammierten Muster-Code keine sinnvolle Koordinate, brummt der Stift vernehmlich. Das gleiche Brummen erzeugt der Stift, wenn das Muster auf dem Papier zu schlecht erkennbar ist. Da die Kamera aber nur einen sehr kleinen Ausschnitt des Musters auf dem Wahlzettel erfaßt, hat der Wahlstift keinen „Überblick“ und kann somit nicht erkennen, ob er sich auf einem Orignal-Wahlzettel oder einer gut gemachten manipulierten Kopie mit sich wiederholenden Musterblöcken befindet. Auf einem gut reproduzierten Muster im Erfassungsbereich der Kamera brummt der Stift demzufolge nicht. Dies wurde in mehreren Versuchsreihen erfolgreich getestet.

Mit dem beschriebenen Manipulationsverfahren lassen sich die Versuche einer Kopierschutztechnologie, wie sie etwa bei den Wahlzetteln im „Schnupperwahllokal“ beobachtet wurden, problemlos umgehen. Durch die Erfassung des positionsbestimmenden Musters im Infrarotbe-

reich, also mit der gleichen Lichtwellenlänge, in welcher der Wahlstift das Muster aufnimmt, werden Störmuster und vergleichbare Methoden, die einen Kopierschutz darstellen sollen, zuverlässig ausgeblendet.

Jürgen Dreesen, Vertreter des DWS-Herstellers, sagte am 18. August 2007 auf der Veranstaltung der Patriotischen Gesellschaft *Wie sicher ist elektronisches Wählen?* über die Manipulierbarkeit der Wahlzettel: „Zum Thema Stimmzettel: Sie haben vollkommen recht. Wenn es gelänge, einen Stimmzettel zu so manipulieren, dann würde das System falsch zählen. Wir haben uns sehr gewundert, wirklich sehr gewundert, als wir gesehen haben, daß das Papier, der Stimmzettel, nicht innerhalb der Zertifizierung umfaßt ist. [...] haben wir, die wir ja auch Verantwortung tragen für die Erstellung der Druckdaten, Maßnahmen ergriffen, die ein Manipulieren in der Papierform erschweren, wenn nicht gar ganz verhindern. Das bedeutet, der Stimmzettel, den sie kopieren, der wird funktionsuntüchtig.“[2]

Wie vom Chaos Computer Club in der Anhörung vor dem Verfassungssauschuß dargelegt hat, sind die von Herrn Dreesen angeführten Maßnahmen, wie etwa das Aufbringen eines Störmusters, die ein Kopieren und Manipulieren des Stimmzettels erschweren oder verhindern sollen, untauglich und bieten keinen wirksamen Schutz. Prinzipbedingt wird es immer möglich sein, das positionsbestimmende Muster aus einem Stimmzettel zu extrahieren, indem optische Aufzeichnungsgeräte verwendet werden, die in ihrer Lichtwellenlängen-Charakteristik denen des Wahlstifts entsprechen. Das so gewonnene Muster kann dann manipuliert und reproduziert werden. Man erhält so Stimmzettel, die ein manipuliertes digitales Ergebnis liefern.

Da ein Wahlfälscher durch die Versendung bei der Briefwahl bereits vier Wochen vor der Wahl das gültige Stimmzettel-Muster erhält, hat er genügend Zeit zur Vorbereitung. Da das Layout der verschiedenen Wahlzettel laut Wahlgesetz ebenfalls rechtzeitig vorher publiziert werden muß, ist selbst eine Fälschung mit dem Ziel, erst am Wahltag den Zettelaustausch vorzunehmen, problemlos durchführbar.

Die von der Firma Halbach bei der Anhörung behauptete Signalisierung eines gefälschten Musters durch den Wahlstift entspricht also nicht den Tatsachen. Der Stift signalisiert zwar in der Tat ein defektes oder

---

[2] Jürgen Dreesen, Veranstaltung der Patriotischen Gesellschaft „Wie sicher ist elektronisches Wählen?“ am 18. August 2007, http://www.send.de/07-09-18_Wahlstift_6_Diskussion.mp3 vom 14. November 2007.

ungültiges Muster mit dem demonstrierten Brummen. Herr Dreesen hat dort jedoch schlicht ein absichtlich defektes oder für den Stift nicht registriertes Muster zur Demonstration benutzt und so das Brummen ausgelöst.

Am eigentlichen Sachverhalt geht diese „Showeinlage“ jedoch vorsätzlich vorbei. Ein korrekt manipuliertes Wahlmuster, bei dem Teile des echten Musters umkopiert, ansonsten aber das Muster nicht beschädigt oder verändert wurde, kann der Stift – bedingt durch die zugrundeliegende Technologie – gar nicht als ungültig erkennen. Dies ist durch einfache Tests belegbar, die der CCC erfolgreich durchgeführt hat. Hierzu benötigt man lediglich einen echten Wahlzettel – etwa durch die Briefwahl – und wenige Tage Zeit für die technisch in einfacher Weise erstellbaren gefälschten Wahlzettel. Die benötigte Auflösung und Genauigkeit läßt sich mit einem geeigneten handelsüblichen Drucker mit kohlenstoffhaltiger Tinte erreichen.

Echtheitsmerkmale im Papier des Stimmzettels

Die seitens der Vertreter von Diagramm Halbach vorgebrachte Argumentation, daß der Wahlzettel durch aufwendige Echtheitsmerkmale vor einer Manipulation gesichert werden kann, weist mehrere offenkundige systematische Probleme auf:

1. Wie etwa die zahlreichen gefälschten Euro-Scheine belegen,[3] ist selbst bei Anwendung aufwendigster Sicherheitsmerkmale am Papier keine Fälschung auszuschließen. Effektive Sicherheitsmerkmale lassen sich ohnehin nur durch eine Individualisierung des Wahlzettels beispielsweise durch eine registrierte Seriennummer erzeugen, was aber mit dem Grundsatz der geheimen Wahl unvereinbar wäre.

2. Die Überprüfung von Echtheits- und Sicherheitsmerkmalen auf jedem einzelnen Wahlzettel stellt eine erhebliche Belastung für Wahlvorstand, Wahlhelfer und Wähler dar und würde in der Realität kaum konsequent durchführbar sein. Wasserzeichen, Hologramme, Silberfäden, UV-Tinte und ähnliche Merkmale können, wie wiederum das

---

[3] Siehe etwa Sabina Wolf „Vorsicht Falschgeld“ http://www.daserste.de/plusminus/beitrag_archiv.asp?aid=160 vom 14. November 2007.

Beispiel der Euro-Noten zeigt, auch bei nicht perfekter Fälschung vom Normalbürger nicht effektiv überprüft werden.[4] Neben der Einführung der komplexen Wahlstifttechnik ist es Wahlhelfern und Wählern zudem kaum zuzumuten, auch noch eine Schulung in der Interpretation von Echtheitsmerkmalen von Wahlzetteln zu durchlaufen.

3. Durch die Einführung von Echtheitsmerkmalen auf dem Wahlzettel entstehen erhebliche Zusatzkosten. Jedes einzelne Echtheitsmerkmal bedeutet pro Wahlzettel weitere finanzielle Aufwendungen in Höhe von mehreren Cent pro Wahlzettel, die sich durch die große Anzahl der Exemplare leicht zu sechsstelligen Eurobeträgen summieren. Diese Kosten fallen dann jeweils pro Wahl an. Mit einer Kostensteigerung ist zusätzlich dadurch zu rechnen, daß durch den Fortschritt bei Fälschungsmethoden jeweils neue, teurere Sicherheitsmerkmale für den nächsten Wahlgang einige Jahre später eingeführt werden müssen. Es muß spezielles Papier hergestellt werden, dessen drucktechnische Verarbeitung und Lagerung unter Sicherheitsbedingungen vorgenommen werden muß. Nicht alle auf dem Markt erhältlichen Echtheitsmerkmale sind jedoch überhaupt mit der Anoto-Technologie für den Wahlstift kombinierbar.

Sicherung der Stimmzettel

Entgegen der in der Anhörung von der Wahlbehörde gemachten Aussagen werden die Stimmzettel nicht gesichert verarbeitet und gelagert. Aus dem Grobkonzept von Fujitsu Siemens Computers[5] geht hervor, daß die Stimmzettel zusammen mit den nicht als sicherheitskritisch angesehenen Teilen des Wahlsystems, der sogenannten „P-Urne“, gehandhabt und gelagert werden. Nur die elektronischen Teile des DWS werden hingegen als „T- & B-Urne“ bezeichnet und unter gewissen Sicherheitsanforderungen gelagert. „Die P-Urne besteht aus den Stimmzetteln, der Wahlkabine (Pappversion) und dem Behälter für die Abgabe und sicheren

---

[4] Bei Euro-Noten ist das Problem mittlerweile so gravierend, daß größere Bargeldbestände von Banken nur noch unter dem Vorbehalt der Prüfung durch die Landeszentralbank angenommen werden.

[5] Grobkonzept für die Digitalen Wahlen 2008 in der Freien und Hansestadt Hamburg, Fujitsu Siemens Computers GmbH, Version: V 1.0 vom 9. Oktober 2007, S. 12.

Aufbewahrung der Stimmzettel. Alle Komponenten werden von unterschiedlichen Lieferanten geliefert. Für dieses Material wird eine Fläche von ca. 2.500 m² benötigt. FSC ist aufgefordert, hierfür beim Logistiker eine geeignete Lagerfläche bereitzustellen, da weder in der BfI noch in den Bezirksämtern ausreichende Logistikflächen bereit gestellt werden kann (sic). An die Fläche wird keine große Sicherheitsanforderungen wie bei der T- & B-Urne gestellt."[6] Weiter heißt es: „Die Stimmzettel werden vom Lieferanten in Chargen an das Lager geliefert, weil hier keine ausreichende Fläche für die gesamte Menge vorhanden ist. Die Lieferungen der Stimmzettel sind nach Wahlbezirken sortiert und geben damit bereits die Kommissionierung vor."[7]

Es wird deutlich, daß die Stimmzettel nicht als sicherheitskritisches Element des Wahlsystems angesehen werden. Die Möglichkeit der vom CCC dargelegten Manipulation an den Stimmzetteln wurde also bei der Planung des Gesamtsystems nicht berücksichtigt. Die Nachplanung und Nachrüstung von Sicherheitsmaßnahmen, die zudem nur begrenzte Erfolgsaussichten haben, erfordert erhebliche Zusatzinvestitionen und verteuert die Gesamtkosten des DWS nochmals drastisch.

Fälschung des Wahlstift-Prüfbogens

Die komplexen Risiken, die durch den Einsatz eines von Wähler und Wahlleiter nicht überprüfbaren Verfahrens zur Stimmerfassung entstehen, setzen sich an weiteren Stellen fort. Ein sehr einfacher Weg, die Wahl zu manipulieren, ist der Austausch des im Wahllokal verwendeten Prüfbogens, mit dem vor jeder Wahlhandlung sichergestellt werden soll, daß der Stift einwandfrei funktioniert. Wenn ein gefälschter Prüfbogen vom Wahlfälscher zum Teil mit einem positionsbestimmenden Muster des Wahlzettels bedruckt wird, lassen sich auf diese Art und Weise durch einen einzelnen Wahlhelfer mit einem einzigen Blatt Papier hunderte Stimmen mindestens ungültig machen oder – je nach Verfahrensweise – sogar verfälschen. Das Entdeckungsrisiko ist gering, da der Wahlfälscher an dieser Stelle problemlos den Prüfbogen wieder gegen das Original austauschen kann und die Markierbewegung des Stiftes auf dem

---

[6] Grobkonzept für die Digitalen Wahlen 2008 in der Freien und Hansestadt Hamburg, Fujitsu Siemens Computers GmbH, Version: V 1.0 vom 9. Oktober 2007, S. 12.

[7] Ebd.

gefälschten Prüfbogen unter seiner Kontrolle bleibt. Er kann somit auch verhindern, daß bei der Durchsicht der ungültigen Stimmen auffällt, daß diese eine uniforme Abweichung aufweisen.

Dieses Beispiel zeigt auf, daß durch das Hinzufügen von weiteren Maßnahmen zu einem ohnehin schon komplexen System zwar möglicherweise ein Risiko (hier die Manipulation von Kamera und Stiftaufsetzkontakt) vermindert werden kann, gleichzeitig aber neue Angriffswege eröffnet werden, deren Schwere über der des Ursprungsrisikos liegt. In der Informatik gilt der Grundsatz, daß komplexe Systeme komplexe Fehler erzeugen. Dies ist auch hier zutreffend.

Bluetooth

Wie aus dem Kurzbericht zu kompromittierenden Abstrahlungen von Markus Kuhn klar hervorgeht, enthält der ihm zur Untersuchung vorliegende Digitale Wahlstift entgegen den bisherigen öffentlichen Angaben des Herstellers einen eingebauten Bluetooth-Sender: „Ich habe im Rahmen dieser Untersuchung ebenfalls nicht den im Stift enthaltenen Bluetooth-Sender untersucht, da mir versichert wurde, daß dieser durch eine Firmwareänderung durch den Hersteller zuverlässig und dauerhaft ausgeschaltet wird.“[8]

Diese Anmerkung im Bericht legt nahe, daß entweder alle Wahlstifte einen Bluetooth-Sender enthalten oder die Behörde für Inneres (BfI) einen Wahlstift zur Prüfung vorgelegt hat, dessen Bauart abweicht. Der Bluetooth-Sender stellt ein erhebliches Sicherheitsrisiko dar und kann von Angreifern aktiviert werden, um unbemerkt das Wahlgeheimnis zu brechen oder die Software auf dem Stift anzugreifen. Enthält der in Hamburg eingesetzte Wahlstift keinen Bluetooth-Sender, ist das Abstrahlungsgutachten wertlos, da nicht die tatsächlich verwendete Hardware geprüft wurde. Eine Hardware zur Prüfung einzureichen, die nicht ein exaktes Baumuster des eingesetzten Modells ist, verfälscht insbesondere die Aussagen zur komprimittierenden Abstrahlung, bei denen es auf jedes noch so kleine Detail der Elektronik ankommt, und ist mindestens als fahrlässig zu bezeichnen.

---

[8] Markus Kuhn, Bericht über eine Kurzuntersuchung zur Einschätzung des Risikos kompromittierender RF-Abstrahlungen eines digitalen Wahlstifts, University of Cambridge, 4. November 2007, S. 2.

Sollten die eingesetzten Stifte jedoch tatsächlich ein Bluetooth-Modul enthalten, liegt eine schwerwiegende Gefahr für das Wahlgeheimnis vor, die auch einen Einsatz als Zählhilfe ausschließt. Über den Bluetooth-Datenfunk können sowohl Daten aus dem Stift ausgelesen als auch Manipulationen am Speicher des Stiftes vorgenommen werden. Zudem kann sogar eine Möglichkeit zur Veränderung der Firmware des Wahlstiftes nicht ausgeschlossen werden. Bluetooth nur softwareseitig zu deaktivieren, ist definitiv keine ausreichende Sicherheitsmaßnahme, da diese Abschaltung auch per Software wieder rückgängig gemacht werden kann. Ob die Abschaltung des Bluetooth-Moduls nun erfolgt ist oder nicht, ist von Wähler ohnehin nicht nachzuprüfen. Allein das Vorhandensein einer drahtlosen Ausspähschnittstelle im Wahlstift ist inakzeptabel. Dem Wähler ist nicht zuzumuten, seine Wahl mit einem Wahlstift durchzuführen, der eine Funkschnittstelle enthält, die technisch in der Lage ist, seine Wahlentscheidung live über fünfzig Meter zu übertragen.

Das Vorhandensein des Bluetooth-Senders bedarf einer umgehenden Aufklärung. In beiden Varianten liegt hier ein schwerwiegender Bruch der grundlegenden Regeln vor, der nicht stillschweigend übergangen werden kann.

Firmware-Update

Da sich der Wahlstift in den Händen des Wählers in einer nicht einsehbaren Wahlkabine befindet, stehen einem wählenden Angreifer verschiedene Methoden der Manipulation offen. Das Schutzprofil fordert Maßnahmen gegen solche Manipulationen, jedoch sind diese ohne Vorlage des Evaluationsberichtes zum Schutzprofil bisher nicht überprüfbar.

Die wenigen beobachtbaren und bekanntgewordenen Details, etwa daß ein für Firmware-Updates notwendiger Reset-Knopf vorhanden ist, der nur durch eine mit einer einfachen Nadel überwindbare Siegelbanderole geschützt ist, lassen vermuten, daß hier notdürftig „herumgebastelt“ wurde, um die nach und nach entdeckten Sicherheitsprobleme irgendwie zu vermindern.

Eine abschließende Beurteilung der Möglichkeiten, die Firmware auf dem Stift in der Wahlkabine zu manipulieren, ist aufgrund der vollständig fehlenden technischen Dokumentation der vorgenommenen Änderungen gegenüber dem Standard-Digitalstift derzeit nicht möglich. Es ist jedoch davon auszugehen, daß Restrisiken verbleiben, die bauartbedingt nicht durch das Schutzprofil abgedeckt werden können.

Zur Verwendung von Siegeln

Die Verwendung von Siegeln am Stift selbst stellt keine ausreichende Sicherheitsmaßnahme dar, da auch holographische Siegel heute problemlos nachgemacht werden können. Die Erfahrungen der Hersteller von Software und Computerchips, die versucht haben, Fälschungen ihrer Produkte durch Verwendung verschiedenster Siegeltechnologien einzudämmen, sprechen hier eine deutliche Sprache. Anerkannter Stand der internationalen Sicherheitsforschung ist es, daß es praktisch keine Siegel gibt, die nicht innerhalb weniger Minuten mit geringem Aufwand überwunden werden können.

In der umfangreichsten Studie zu diesem Thema wurden 244 am Markt verfügbare Siegel für Sicherheitsanwendungen untersucht.[9] Es wurde festgestellt, daß alle untersuchten Siegel innerhalb weniger Minuten mit geringem Materialeinsatz überwunden oder gefälscht werden konnten. Die Ergebnisse der Untersuchung belegen, daß Siegel nicht dazu geeignet sind, ein inhärent unsicheres System sicher zu machen. Siegel können lediglich bei äußerst disziplinierter Anwendung mit penibel geführten Kontrollaufzeichnungen durch regelmäßig geschulte, aufmerksame Anwender einen Angriff auf ein ansonsten gut gesichertes System erschweren – mehr aber nicht.

Sonstige Angriffe

Da der Wahlstift für alle an der Wahl Beteiligten eine Black Box ist, die keinen Einblick erlaubt, steht es einem Angreifer frei, den Stift als Angriffswerkzeug gegen den Wahllaptop zu verwenden. Er kann sich dabei entweder einer modifizierten Firmware im Wahlstift oder einer umgebauten Elektronik im Gehäuse eines Wahlstifts bedienen. Die auf dem Wahllaptop offengelegten USB-Schnittstellen, an denen der Wahlstift angeschlossen wird, bieten ein reichhaltiges Betätigungsfeld für einen Angreifer. Der Hersteller des Windows-XP-Betriebssystems, das auf dem Wahllaptop läuft, betrachtet die USB-Schnittstelle nicht als gegen alle lokalen Angriffe schützbar und deshalb nicht als Bestandteil der abzudeckenden Bedrohungsszenarien.

---

[9] Roger G. Johnston, Jon S. Warner: Anti-Evidence Seals, 2006. http://pearl1.lanl.gov/external/c-adi/seals/images/AE_seals.pdf vom 14. November 2007.

Eine detaillierte Betrachtung der hier entstehenden Risiken wird wiederum erst nach Vorliegen der technischen Dokumentation und des Evaluierungsberichtes zum Schutzprofil möglich sein. Angesichts der Komplexität der Software und des zugrundeliegenden Betriebssystems ist jedoch davon auszugehen, daß es eine große Anzahl von angreifbaren Schwachstellen gibt.

Nichteignung der Zertifizierung

Der für das DWS eingeschlagene Weg, die Sicherheit des Systems durch die Durchführung einer Common-Criteria-Evaluierung auf dem Niveau EAL3+ zu gewährleisten, ist zwar akademisch möglicherweise interessant, löst jedoch die grundlegenden Probleme eines computerisierten Wahlsystems nicht. Zunächst ist für das Common-Criteria-Konzept noch kein Standard allgemein anerkannter Kriterien für ein Wahlsystem definiert worden, nach denen ein Evaluationsobjekt geprüft werden könnte. Damit scheidet eine Common-Criteria-Evaluierung für die Zertifizierung des DWS schon aus formalen Gründen aus. Das vorliegende Schutzprofil ist aus den allgemeinen Sicherheitsanforderungen für IT-Systeme hergeleitet und weist dadurch zwangsläufig große Lücken auf. Das weitaus gravierendere Problem ist aber, daß auch eine Common-Criteria-Evaluierung in keiner Weise das oben erläuterte Dilemma der durch Technologieeinsatz entstehenden mangelnden Transparenz und Nachvollziehbarkeit für den Wähler löst.

Das vorliegende Schutzprofil weist zudem verschiedene handwerkliche Fehler auf. Selbst wenn man der fragwürdigen Grundannahme, daß ein computerisiertes Wahlsystem durch eine Common-Criteria-Evaluierung hinreichend zu sichern ist, folgen würde, ist nicht einzusehen, daß Komponenten des DWS, die für die Sicherheit des Systems wesentlich sind, nicht Bestandteil des Schutzprofils wurden. So sind weder der Aufdruck der Rasterung auf dem Papierstimmzettel noch der Papierstimmzettel selbst Bestandteil der Prüfung. Auch der Drucker, das transportable Speichermedium, die Software in der Wahlzentrale sowie die statistische Datenerfassung unterliegen nicht einer Evaluierung. Eine Sicherheitsprüfung ist für alle diese Komponenten auch nicht vorgesehen, lediglich ein Funktionsfähigkeitstest durch die PTB soll erfolgen.

Der seitens der Wahlbehörde in der Öffentlichkeit erweckte Eindruck, mit der Zertifizierung und Evaluierung des Schutzprofils würde das Bundesamt für die Sicherheit in der Informationstechnik (BSI) prak-

tisch eine Garantie für die Sicherheit des Systems übernehmen, ist irreführend und falsch. Das BSI macht dies in seinem Zertifikat deutlich: „Mit diesem Zertifikat ist weder eine generelle Empfehlung des Schutzprofils noch eine Garantie des Bundesamtes für Sicherheit in der Informationstechnik oder einer anderen Organisation, die dieses Zertifikat anerkennt oder darauf Einfluß hatte, verbunden.“[10]

Komplexität des Rollout-Projektes

Anhand des vorliegenden Grobkonzeptes und eigener Erfahrungen mit dem Rollout von sicherheitskritischen Infrastrukturen ist festzustellen, daß das allgemeine Fehlerrisiko und die entstehenden Sicherheitslücken beim Rollout am Wahltag nicht vollständig berücksichtigt wurden. Der Planungsstand ist zum derzeitigen Zeitpunkt wohl noch vorläufig und wird diverse Revisionen erfahren. Das ändert allerdings nichts an der in der Informatik bekannten Tatsache, das IT-Projekte dieser Größenordnung, noch dazu mit einem neuen und praktisch ungetesteten System eine hohe Fehlschlagswahrscheinlichkeit aufweisen. Die Liste von vergleichbaren Großprojekten, die aus sehr unterschiedlichen Gründen nicht erfolgreich waren, ist lang. Typischerweise wird ein erfolgreicher Wirkbetrieb erst mit mehrmonatiger oder gar mehrjähriger Verzögerung erreicht, meist nur unter Einschränkung der ursprünglich geplanten Funktionalität und oft unter Vernachlässigung ursprünglich gesetzter Sicherheitsziele. Dies wäre jedoch für das DWS, das an einem genau definierten Tag perfekt und sicher funktionieren muß, nicht akzeptabel.

Die dem DWS eigene Systemkomplexität durch viele verschiedene Einzelteile, die alle fehlerfrei funktionieren müssen und einer komplexen Logistik bedürfen, macht das Projekt insgesamt anfällig für Fehler, die sich wiederum schnell zu Sicherheitslücken ausweiten können.

Abhängigkeit vom Technologielieferanten

Die Abhängigkeit von einem Technologielieferanten bei einer demokratischen Wahl stellt einen weiteren kritischen Unsicherheitsfaktor dar. Auch wenn der Lieferant eine betriebswirtschaftlich solide Firma ist,

---

[10] BSI-PP-0031-2007 zu Schutzprofil Digitales Wahlstift-System, Version 1.0.1 entwickelt im Auftrag der Freien und Hansestadt Hamburg, S. 3.

können sich leicht prekäre Situationen ergeben, z. B. weil die Firma ihrerseits kritische Komponenten des DWS von Einzelpersonen oder weiteren Auftragnehmern erstellen läßt oder das Interesse am Geschäftsfeld Wahltechnologie verliert. Diese Problematik konnte international bereits beobachtet werden.

Als Beispiel seien hier wiederum die Niederlande angeführt. Die Hardware der Wahlcomputer selbst wird dort von der hochangesehenen, vormals im Staatsbesitz befindlichen Firma NEDAP hergestellt. NEDAP existiert seit 1929 und machte im Jahre 2006 138,5 Millionen Euro Umsatz. Die Software für die Wahlcomputer wurde jedoch über Jahrzehnte von der kleinen Firma Groenendaal B.V. erstellt und gepflegt. Aufgrund dieser Monopolstellung des Softwareherstellers konnte die prekäre Situation entstehen, daß der Firmeninhaber Jan Groenendaal in einer E-Mail an das niederländische Innenministerium vom 10. November 2006 mit der sofortigen Einstellung aller Arbeiten an der Wahlsoftware drohte, falls der Staat nicht seine Firma aufkaufe.[11] Der niederländische Staat machte so unwissentlich das Funktionieren seiner Demokratie von einem kleinen Unternehmen und dessen Besitzer abhängig, ohne dessen Kooperation er keine Wahlen durchführen konnte.

Das Beispiel illustriert exemplarisch die Risiken, die durch die Einführung einer komplexen Technologie wie dem DWS für Wahlen entstehen. Es liegt in der Natur von Technologieentwicklung, daß sich ein vollständiges und detailliertes Verständnis, das für das reibungslose Funktionieren eines komplexen Systems notwendig ist, in den Köpfen einer nur geringen Anzahl von Personen konzentriert. Das Funktionieren der Demokratie hängt beim Einsatz computergestützter Wahlverfahren damit zwangsläufig von diesen wenigen Personen ab. Interessenskonflikte werden unvermeidlich, wie sich schon jetzt exemplarisch an Roland Vogt vom Deutschen Forschungszentrum für Künstliche Intelligenz zeigt. Als Mitautor des Wahlstift-Schutzprofils sollte er eigentlich die Position des unabhängigen Experten wahren. Mittlerweile ist er jedoch für den Hersteller des DWS beratend tätig.[12]

---

[11] Hervorgegangen aus amtlichen Dokumenten, die durch das niederländische Informationsfreiheitsgesetz erlangt wurden.
http://www.wijvertrouwenstemcomputersniet.nl/English/Groenendaal vom 14. November 2007.

[12] Vgl. Richard Sietmann „Für den Wahlstift ‚ist die Zeit nicht reif'“, http://www.heise.de/newsticker/result.xhtml?url=/newsticker/meldung/98764 vom 14. November 2007.

Die vorgesehene Überprüfung von Angestellten und Mitarbeitern der beteiligten Unternehmen durch ein polizeiliches Führungszeugnis bietet hier nur einen geringen Schutz, da damit nur eine offenkundig kriminelle Vergangenheit ausgeschlossen werden kann. Über Interessenskonflikte oder zukünftige Intentionen kann eine solche Überprüfung naturgemäß keine Auskunft geben.

Weitere entstehende Risiken sind z. B. ein Aufkauf der Herstellerfirma oder des entsprechenden Geschäftsbereichs für Wahltechnologie, der durchaus auch durch einen ausländischen Interessenten erfolgen kann. Insbesondere Hersteller aus den USA haben öffentlich Interesse am Zukauf europäischer Technologie im Wahlbereich geäußert. Im besten Fall wäre die Stadt Hamburg für die Durchführung ihrer Wahlen dann von einem zweifelhaften ausländischen Unternehmen abhängig. Die Folgen für das Wählervertrauen bedürfen keiner weiteren Erläuterung.

Nachprüfbarkeit der Wahl durch den Wähler

Das Bedürfnis, in Hamburg Computer bei Wahlen einzusetzen, resultiert aus dem neuen, deutlich komplexeren Wahlverfahren. Hinzu kommt der Wunsch nach einem schnellen Ergebnis bei Verringerung des Aufwands für die Durchführung der Wahl. Schnelligkeit kann jedoch nicht vor Gründlichkeit und Sicherheit gehen. Die Behauptung, daß mit dem neuen Wahlverfahren ein vorläufiges Endergebnis erst nach Tagen erzielbar wäre, kann zudem nicht als realistisch angesehen werden. Das prozentuale Ergebnis der Erststimme ist auch unter den neuen Gegebenheiten selbstverständlich am Wahlabend ermittelbar.

Um die angestrebten Ziele mit den Anforderungen an eine demokratische Wahl zu vereinbaren, ist es unabdingbar, daß das Wahlverfahren vom Wähler direkt im Wahllokal nachprüfbar bleibt. Jede durch den Einsatz des DWS erzeugte Notwendigkeit zur Delegation der tatsächlichen Überprüfbarkeit an Dienstleister und Prüfbehörden bedeutet unausweichlich, daß Möglichkeiten zur nur schwer oder gar nicht mehr nachweisbaren Manipulation entstehen. Es erscheint daher als einzig sinnvoller Weg, daß die Stimme auf Papier weiterhin endgültiger Ausdruck des Wählerwillens bleibt. Elektronische Wahlverfahren sind als Hilfsmittel zur Erzielung eines schnellen vorläufigen Ergebnisses nur dann vertretbar, wenn zweifelsfrei geregelt ist, daß eine Auszählung des Papierergebnisses in jedem Falle erfolgt.

Im Gegensatz zum bewährten Wahlverfahren mit Papier und Stift ist eine computergestützte Wahl ohnehin nicht mehr vom Wähler nachvollziehbar und überprüfbar. Durch die von der BfI praktizierte Delegierung der Überprüfung an Firmen und Behörden wird dem Wähler das Recht genommen, sich selbst von der Korrektheit der Wahl zu überzeugen.

Die BfI vertritt die Position, daß – wie in vielen anderen Bereichen der Gesellschaft – die Bürger ihre Kontrollmöglichkeiten an Experten und Behörden abtreten sollen. Dies erscheint angesichts der grundsätzlichen Bedeutung von demokratischen Wahlen unangemessen und höchst problematisch. Die für die Einführung des DWS vorgelegten Gründe haben keineswegs das gleiche Gewicht wie das Recht auf transparente und verifizierbare Wahlen. Nur aufgrund eines neuen Wahlverfahrens dürfen nicht die bewährten Regel der Demokratie außer Kraft gesetzt werden. Auch andere Bundesländer führen schließlich mit vergleichbar komplexen Wahlverfahren eine Wahl mit Papier und Stift erfolgreich und zeitlich effizient durch. Der Einsatz des DWS verkennt, daß es neben der heutigen „Schönwetter-Demokratie“ auch extremistische Kräfte in einer Gesellschaft geben kann, die sich demokratischen Spielregeln nicht unterwerfen wollen. Ein Wahlverfahren muß aber so beschaffen sein, daß es unter allen, also auch unter widrigen Umständen funktioniert und nachprüfbar bleibt.

Schon die jüngste Vergangenheit liefert ein Beispiel für die Notwendigkeit nachvollziehbarer Auszählungen nach Wahlen. Denn selbst unter den Bedingungen der DDR war der Nachweis von strukturellen Wahlfälschungen durch das Beobachten der Auszählung in den Wahllokalen, das Zusammentragen der Ergebnisse aus den einzelnen Wahllokalen und den Vergleich mit den offiziellen Zahlen erfolgreich. Mutige Bürger haben es so geschafft, den systematischen Wahlbetrug aufzudecken. Mit computerisierten Wahlen wäre dies nicht möglich gewesen, die Ergebnisse hätten bereits unsichtbar in den Computern manipuliert werden können. Ein demokratisches Gemeinwesen sollte gerade aufgrund der Erfahrungen aus der Vergangenheit keinem Wahlfälscher entgegenarbeiten und ihm die Mittel zur nicht nachweisbaren Manipulation an die Hand geben.

Bildschirmdarstellung im Wahllokal

Auf dem für den Wähler einsehbaren Bildschirm des DWS wird zwar die Stimmenübertragung visualisiert, welche Stimme er abgegeben hat, kann dabei jedoch aufgrund des zu schützenden Wahlgeheimnisses nicht direkt nach dem Auslesen aus dem Wahlstift vom ihm überprüft werden. Auch die bei der „Auszählung“ erfolgende Visualisierung der elektronisch erfaßten Stimmen auf dem Bildschirm des Notebooks ermöglicht keine effektive Transparenz, da zum einen nicht alle Stimmen nochmals angezeigt werden und zum anderen die Visualisierung nur eine Darstellung dessen ist, was das System als Wählerstimme zu erkennen glaubt. Ist das Papier zuvor manipuliert worden, kann dies bei der „Auszählung“ nicht erkannt werden.

Zudem ist auch die Visualisierungssoftware des DWS potentiell angreifbar und könnte so umgebaut werden, daß eine Manipulation nicht entdeckt werden kann. Ein gefälschter Stimmzettel oder ein Betrug mit Hilfe eines Wahl-Musters auf dem Testbogen, der vor jeder Stiftbenutzung abgehakt wird, läßt sich daher mit dieser Visualisierung ebensowenig erkennen wie eine manipulierte Software auf dem Wahllaptop oder ein manipulierter Wahlstift. Die Stimmvisualisierung hat somit nur kosmetischen Charakter und stellt keinen Ersatz für die öffentliche Auszählung von Papierstimmzetteln dar.

Praktische Relevanz der Manipulationsmöglichkeiten

In der Computersicherheitsforschung wird in der Regel für eine Sicherheitsbeurteilung ein Angreifer mit bestimmten Fähigkeiten und Zugangsrechten modelliert, um die tatsächliche Wirksamkeit von Sicherheitsmaßnahmen zu beurteilen. Für die Untersuchung werden schwerpunktmäßig Angriffsmethoden beurteilt, die tatsächlich für einen Angreifer realisierbar sind.

Aus den Erfahrungen der vergangenen Wahlmanipulationen ergibt sich, daß die potentiellen Hauptinteressenten einer Wahlfälschung Kandidaten oder Parteien, die zur Wahl stehen bzw. mit ihnen verbundene Interessengruppen, sind.

Die Wahlergebnisse in den letzten Jahren haben oftmals knappe Ausgänge der Wahlen gezeigt. Das bedeutet, daß selbst eine kleine

Menge gefälschter Stimmen mandatsrelevant sein kann. Es ist also wahrscheinlich, daß schon die Manipulation einiger weniger Wahllokale die Zusammensetzung der Mandatsträger im Senat ändern kann. Je knapper das zu erwartende Ergebnis, desto weniger muß für eine erfolgreiche Wahlfälschung manipuliert werden. Eine geringere Anzahl von manipulierten Systemen verringert so den vom Angreifer zu betreibenden organisatorischen Aufwand und senkt das Entdeckungsrisiko.

Knappe Wahlausgänge bedeuten weiterhin, daß eine Manipulation, die nur wenige Stimmen fälscht, nicht aufgrund eines wenig wahrscheinlichen Wahlausgangs erkannt werden kann. Die Ergebnisse der Meinungsforschungsinstitute vor Wahlen ermöglichen ebenfalls keinen sinnvollen Rückschluß auf eventuelle Manipulationen, da die Abweichung zwischen Umfragewerten und Wahlergebnis in den letzten Jahren durchaus erheblich war. Als Referenz sei hier auf die Ausführungen von Matthias Moehl in der Anhörung verwiesen, der mit Zahlen der letzten Wahlen belegt hat, wie wenige Stimmen mandatsrelevant sein können.

Für einen motivierten Wahlfälscher ist es ohne Schwierigkeiten möglich, das technische Personal für die Durchführung der Manipulationsmittel zu finden. Das Manipulationssystem kann so gestaltet werden, daß es auch von technisch nicht versierten Tätern vor Ort angewandt werden kann. Die von der BfI und dem Hersteller angenommene Bedrohung durch den einsamen Außentäter, der versucht, eine Manipulation durchzuführen, entspricht nicht den tatsächlichen Bedrohungen. Die Behauptung, ein Innentäter-Angriffsszenario sei extrem unwahrscheinlich, läßt sich nicht aufrechterhalten. Alle bekannt gewordenen Wahlmanipulationen sind von Innentätern mit Zugang zu den Wahlmitteln begangen oder wesentlich unterstützt worden.

Auch in der Kriminalität sind vergleichbare komplexe Betrugshandlungen vorwiegend Innentäterdelikte. Finanzinstitute gehen z. B. aus Erfahrung davon aus, daß erhebliche Betrugsversuche überwiegend von Innentätern begangen werden und richten ihre Sicherheitsprozeduren entsprechend aus. Das Innentäter-Angriffszenario muß daher als die wichtigste praxisrelevante Bedrohung angenommen werden, gegen welche die Sicherheitsmaßnahmen eines Wahlsystems wirksam sein müssen.

Es soll betont werden, daß der Chaos Computer Club durch die Betrachtung des Innentäterrisikos selbstverständlich keine pauschale Verdächtigung von Wahlhelfern und Mitarbeitern der Wahlbehörde beabsichtigt. Gerade die ehrenamtlichen Helfer sind das Rückgrat einer funk-

tionierenden Demokratie. Es muß jedoch im Rahmen einer nüchternen Sicherheitsanalyse festgestellt werden, daß der Kreis der potentiellen Innentäter groß ist und auch die Wahlvorstände und Wahlhelfer umfaßt. Ein spezifisches Risiko computergestützter Wahlen ist es, daß eine kleine Gruppe oder auch Einzeltäter Manipulationen mit sehr großer Wirkung durchführen können, wenn sie denn an der richtigen Stelle wirken. Insofern ist eine nüchterne Betrachtung des Innentäterrisikos zwingend erforderlich und sollte nicht pauschal als „Generalverdacht“ diffamiert werden.

Um die Wichtigkeit der ehrenamtlichen Wahlhelfer zu unterstreichen und die eventuell entstehende Mehrarbeit durch den Wegfall computerisierter Wahlsysteme aufzufangen, hat der Chaos Computer Club seine Mitglieder und Freunde aufgerufen, Wahlhelfer in ihren Gemeinden zu werden.

Fazit

Die dem DWS zugrundeliegenden Technologien weisen gravierende Mängel auf, die auch mit dem eingeschlagenen Pfad der Zertifizierung und Evaluierung nicht behoben werden können. Nicht einmal die zugesagten Zertifizierungs- und Evaluierungsberichte sowie die für eine seriöse Beurteilung der Detailrisiken notwendige technische Dokumentation liegen zum Zeitpunkt der angestrebten politischen Entscheidung vor. Weder der Gesetzgeber noch die bestellten Experten sind somit in der Lage, eine angemessene Prüfung des DWS vorzunehmen.

Angesichts der schon mit dem jetztigen, noch unvollständigen Informationsstand absehbaren systemimmanenten Angriffsmöglichkeiten wie der Manipulation des Anoto-Musters, ist eine den Anforderungen an eine demokratische Wahl in Deutschland entsprechende technische Sicherung des Systems nicht realisierbar.

Das gravierendste Problem des DWS ist es jedoch, daß dem Wähler durch den Einsatz komplexer Technologie die Möglichkeit der unabhängigen Überprüfung der Wahl genommen wird, die sein verfassungsmäßig verbrieftes Recht ist. Dieses Manko läßt sich auch nicht durch noch mehr Technikeinsatz beheben, die Intransparenz und Komplexität wird dadurch nur noch vergrößert.

Der Chaos Computer Club rät daher nachdrücklich von der Verwendung des DWS als Wahlsystem ab. Angesichts der systembedingten Mängel ist auch ein Einsatz als Zählhilfe nur dann vertretbar, wenn die

Papierstimmme dauerhaft und unverrückbar als Ausdruck des Wählerwillens festgeschrieben und in jedem Falle vollständig ausgezählt wird. Das System ist auch nicht nachträglich bis zur Wahlreife reparierbar. Die gravierenden Manipulationsrisiken, der Verlust der Überprüfbarkeit durch den Wähler und der damit einhergehende Verlust an Legitimität würden nur in die Zukunft verschoben. Der einzig vertretbare Weg, um beim Wähler das Vertrauen in die Demokratie zu erhalten, ist und bleibt die dauerhafte Festschreibung der Papierstimme als Ausdruck des Wählerwillens.