U. W.

63263 NEU-ISENBURG

An den Deutschen Bundestag
- Ausschuss für Wahlprüfung, Immunität
und Geschäftsordnung -

Platz der Republik 1

11011 Berlin

Hiermit erhebe ich gemäß §2 WahlprG

Einspruch

gegen das Ergebnis der Wahlen zum 16. Deutschen Bundestag

in den Wahlkreisen

58 Oberhavel - Havelland II,
59 Märkisch-Oderland - Barnim II,
61 Potsdam - Potsdam-Mittelmark II - Teltow-Fläming II,
64 Cottbus - Spree-Neiße,
67 Elbe-Havel-Gebiet,
74 Burgenland,
92 Erftkreis I,
94 Köln I,
95 Köln II,
96 Köln III,
98 Rhein-Sieg-Kreis I,
99 Rhein-Sieg-Kreis II,
102 Leverkusen und Köln IV,
105 Mettmann I,
106 Mettmann II,
107 Düsseldorf I,
108 Düsseldorf II,
109 Neuss I,
122 Recklinghausen I,
123 Recklinghausen II,
132 Gütersloh,
134 Herford - Minden-Lübbecke II,
143 Dortmund I,
144 Dortmund II,
148 Hochsauerlandkreis,
150 Olpe - Märkischer Kreis I,
182 Main-Taunus,
186 Offenbach,
189 Bergstraße,
201 Koblenz

a) wegen Verstoßes gegen das in §10, Abs. 1 und §31 Satz 1 BWG[1] vorgeschriebene Öffentlichkeitsprinzip durch Verwendung von Wahlgeräten des Typs Nedap ESD1 oder ESD2 in allen oder einem erheblichen Teil der Wahlbezirke der jeweiligen Wahlkreise.

   Diese Geräte genügen in ihrer derzeitigen Hardware-Architektur, der Software und in ihren Funktionen nicht den Erfordernissen, die erfüllt sein müssen, um das verfassungsrechtlich und wahlrechtlich gebotene Öffentlichkeitsprinzip technisch, apparativ und funktional zu verwirklichen, und zwar nicht in der Weise, wie die Beachtung dieses Prinzips für die Öffentlichkeit des Wahlgangs (§31 BWG, Satz 1), für die öffentliche Kontrolle der Erfassung und Dokumentation der Stimmenabgabe durch Stimmzettel sowie für die öffentliche Kontrolle der Ermittlung und der Feststellung der

[1] Ein Abkürzungsverzeichnis befindet sich in Abschnitt 8

Ergebnisse sonst bei persönlicher Stimmenabgabe bzw. bei Briefwahl gesetzlich vorgeschrieben ist (§37 ff. BWG, §§67 ff., 74 ff. BWO).

Der Vorgang der Ergebnis-Feststellung mit diesen Geräten stellt sogar eine geheime Auszählung dar und ist deshalb von Anfang an gesetzeswidrig (BVerfG E Bd. 89, Seite 291, 302 ff.).

b) Die verwendeten Geräte entsprechen nicht den Richtlinien für die Bauart von Wahlgeräten (Anlage 1 zu §2 der BWahlGV) hinsichtlich

   1. der eindeutigen Identifizierbarkeit der eingesetzten Software (Teil B Abs. 1 Punkt 2),
   2. der Anforderung nach dem allgemeinen Stand der Technik (Teil B Abs. 2.2 Satz 1), insbesondere hinsichtlich dem Schutz vor Manipulation der eingesetzten Software,
   3. der Anforderung nach der Erkennbarkeit von Veränderungen der installierten Software (Teil B Abs. 2.2 Satz 2).

c) Bedingt durch die Bauart der Geräte lässt sich auch nachträglich nicht mehr feststellen, ob das Wahlergebnis in betroffenen Wahlbezirken rechtmäßig zustande gekommen ist. Damit wird die nach Art. 41 GG erforderliche Überprüfbarkeit des Wahlergebnisses unterlaufen.

d) Durch die hohe Zahl der eingesetzten Geräte (zwischen 1900 und 2200) ergibt sich eine Mandatsrelevanz sowohl für das Zweitstimmenergebnis als auch für das Erststimmenergebnis in den mindestens 13 Wahlkreisen, in denen die Geräte flächendeckend oder in erheblichen Umfang eingesetzt wurden.

Es wird beantragt,

a) zur Beweissicherung die Stimmbezirke zu ermitteln, in denen die Geräte zum Einsatz gekommen sind, sowie die genaue Anzahl der mit den Geräten abgegeben Stimmen,

b) die Wahl in den betroffenen Wahlbezirken zu wiederholen.

Es wird beantrag festzustellen, dass

c) die eingesetzten Geräte nicht den Anforderungen des BWG hinsichtlich der öffentlichen Kontrolle von Wahlen entsprechen,

d) die eingesetzten Geräte nicht den Richtlinien für die Bauart von Wahlgeräten (Anlage 1 zu §2 der BWahlGV) entsprechen,

e) sich nicht mehr zweifelsfrei ermitteln lässt, ob die eingesetzten Geräte zum Zeitpunkt der Wahl der zugelassenen Bauart entsprochen haben und die Benutzeroberfläche für die Erfassung der Stimmen in den jeweiligen Wahlkreisen fehlerfrei programmiert gewesen ist,

Ferner wird beantragt,

f) die im Rahmen des Zulassungsverfahrens der Geräte durch die Physikalisch-Technische Bundesanstalt erstellten Prüfberichte zu veröffentlichen oder hilfsweise dem Einsprechenden zu überlassen,

g) das Bundesamt für Sicherheit in der Informationstechnik als Gutachter für die Bewertung der Sicherheit und die Authentifizierbarkeit der eingesetzten Software beizuziehen,

h) den Staatsrechtler und Experten für elektronische Wahlen Prof. Dr. Ulrich Karpen, Universität Hamburg, als Gutachter für die Bewertung der wahlrechtlichen Problematik beizuziehen.

Der Bundestag wird aufgefordert,

a) Durch Konkretisierung von §35 BWG sicherzustellen, dass verfassungs- und wahlrechtliche Grundsätze einschließlich des Prinzips der öffentlichen Kontrolle auch bei Wahlen mit Wahlgeräten gewährleistet sind,

b) sicherzustellen, dass bei zukünftigen Wahlen mit softwaregesteuerten Wahlgeräten die zum Einsatz kommenden Geräte einschließlich ihrer Software in einem öffentlichen Zulassungsverfahren begutachtet werden, die gutachterlichen Prüfberichte der Öffentlichkeit zugänglich sind, die Authentizität der eingesetzte Software im Wahllokal bei jedem einzelnen Gerät unmittelbar vor dem Wahlgang öffentlich verifiziert wird und entweder

- die geräteunabhängige Verifizierbarkeit des Wahlergebnisses möglich ist, oder
- alle Prüfunterlagen aus dem Zulassungsverfahren einschließlich der Konstruktionsunterlagen, des Quellcodes der zum Einsatz kommenden Software der Öffentlichkeit zugänglich gemacht werden.

Dieser Einspruch ist in Zusammenarbeit mit meinem Vater, Prof. Dr. J.W., entstanden, von dem Sie bereits einen Wahleinsspruch in derselben Sache erhalten haben (WP 108/05). Die beiden Einsprüche sind in ihrer Begründung sowie der Schilderung des Sachverhalts im Wesentlichen inhaltsgleich, weichen aber in der Antragsstellung sowie des in Abschnitt 7 (Mandatsrelevanz) dargestellten Sachverhalts voneinander ab.

1. Einspruchsgründe

a) Bei den Wahlen zum 16. Deutschen Bundestag wurden in den genannten Wahlkreisen Wahlgeräte des Typs Nedap ESD1 und ESD2 eingesetzt. Dabei handelt es sich um mikroprozessorgesteuerte Wahlcomputer, bei denen der Wähler seine Stimme auf einem dem amtlichen Wahlzettel nachempfundenen Bedienfeld per Tastendruck abgibt. Die Stimmen werden in einem elektronischen Speichermodul abgelegt. Nach Ende des Wahlgangs wird das Wahlergebnis automatisch ermittelt und über einen in das Gerät integrierten Drucker ausgegeben. Außerdem werden die Stimmenspeicher an das jeweilige Wahlamt weitergeleitet, wo sie erneut ausgewertet werden.

b) Die genannten Geräte sind gemäß BWahlGV durch das Bundesministerium des Inneren zur Verwendung bei den Wahlen zum Bundestag zugelassen. Die Zulassung erfolgt jeweils für eine bestimmte Bauart. Im Rahmen des Zulassungsverfahrens wird *ein* Gerät des entsprechenden Typs durch die Physikalisch Technische Bundesanstalt (PTB) getestet. Der Prüfbericht der PTB ist öffentlich nicht zugänglich.[2] Die Baugleichheit der zur Verwendung kommenden Geräte mit dem im Zulassungsverfahren geprüften Gerät wird gemäß §2 Abs. 6 BWahlGV vom Hersteller bestätigt, aber nicht von den mit der Durchführung der Wahl betrauten Organen verifiziert. Eine über einen einfachen Funktionstest hinausgehende Überprüfung der in den Wahllokalen eingesetzten Geräte erfolgt nicht.

c) Nach Ansicht des Beschwerdeführers widerspricht der Einsatz der genannten Wahlgeräte dem Öffentlichkeitsprinzip bei Wahlen, weil die Stimmabgabe mittelbar (über das

[2] Auf eine entsprechende Anfrage des Beschwerdeführers antwortete das Bundesministerium des Inneren am 15.09.2005, eine Veröffentlichung der PTB-Prüfberichte nehme das BMI zum Schutz des Firmen-Know-hows [des Herstellers] nicht vor.

Wahlgerät und die zum Einsatz kommende Software) erfolgt und nicht überprüft werden kann

- ob die abgegebene Stimme sofort und unverändert im Stimmenspeicher abgelegt wird,
- ob die Stimme nach der Ablage im Stimmenspeicher bis zur Ermittlung des Wahlergebnisses nicht mehr verändert wird.

d) Durch die fehlende Transparenz bei der Zulassung der Wahlgeräte sowie bei den - über die Geräte - nur mittelbar abgegebenen Stimmen wird eine wirksame Kontrolle der Wahlen durch die Öffentlichkeit verhindert. Dadurch ist eine ordnungsgemäße Durchführung nicht mehr gewährleistet.

   Die Verletzung des Öffentlichkeitsprinzips ist deshalb besonders schwerwiegend, weil die Geräte keine gleichwertigen Kontrollmöglichkeiten der ordnungsgemäßen Stimmenspeicherung und Stimmenzählung bieten und die Geräte keine ausreichenden Vorkehrungen bieten, über die eine eventuelle Manipulation der eingesetzten Software erkannt werden kann.

e) Der Beschwerdeführer bezweifelt außerdem, dass die eingesetzten Geräte hinsichtlich ihrer Manipulationssicherheit dem Stand der Technik entsprechen. Die Regierung der Republik Irland hat im Jahre 2004 eine Kommission zu elektronischen Wahlen eingesetzt (Commission on Electronic Voting, CEV), die die Sicherheit und Genauigkeit der Geräte der Firma Nedap bewerten sollte. Diese Kommission hat gegen erhebliche Sicherheitsbedenken gegen die irische Variante der Geräte geäußert und sich gegen eine Verwendung der Geräte in Irland ausgesprochen[3]. Im Rahmen der Kommissionsarbeit hat der Hersteller der Geräte geltend gemacht, die Geräte würden bereits in Deutschland eingesetzt und seien dort von der PTB geprüft worden. Deshalb ist davon auszugehen, dass die irischen und deutschen Ausprägungen der Nedap-Wahlgeräte im Wesentlichen technisch identisch sind.

f) Die Ergebnisse der Kommission stehen in eindeutigen Widerspruch zu den Anforderungen der BWahlGV.

g) Es ist mit dem Grundsatz der Amtlichkeit der Wahl nicht vereinbar, dass die Prüfung der Funktionstüchtigkeit der Wahlgeräte (§7 Abs. 1 BWahlGV) nicht zwingend durch die Gemeinde oder den Kreiswahlleiter erfolgt, sondern auch lediglich durch den Hersteller erfolgen kann.[4] Ebenfalls nicht Vereinbar mit der Amtlichkeit der Wahl ist die Tatsache, dass auf eine Überprüfung der Authentizität der eingesetzten Software ganz verzichtet wird.

2. Rechtliche Rahmenbedingungen

Die nachfolgenden Grundgesetz- und Wahlrechtsnormen sind – soweit erkennbar – in Rechtsprechung und herrschender Lehre nicht umstritten.

2.1. Das verfassungsrechtliche Fundament bildet das *Demokratie-Prinzip* (Art. 20 Absatz 1 GG, implicite auch Art. 23 NF Absatz 1, Satz 1, zweiter Halbsatz GG)

[3] First Report of the *Commission on Electronic Voting* on the Secrecy, Accuracy and Testing of the Chosen Electronic Voting System, Dublin, 15 December, 2004; zitiert nach www.cev.ie/htm/report/first_report.htm

[4] *Martin Leder*, Der Einsatz von Wahlgeräten und seine Auswirkungen auf die Amtlichkeit und Öffentlichkeit der Wahl, Die Öffentliche Verwaltung, August 2002, S. 648-654 (S.651)

Ihm entsprechen die *Grundsätze unmittelbarer, freier, gleicher und geheimer Wahlen* (Art. 38 Abs. 1, Satz 1 GG).

In diesem Zusammenhang verfassungsrechtlicher Grundentscheidungen stellen parlamentarische Wahlen Staatsakte des Souveräns dar – nämlich des Volkes, verkörpert in allen seinen wahlberechtigten Individuen.

2.2. Die *Verletzung* des Demokratie-Prinzips und aller daraus resultierenden Wahlrechtsnormen und -vorschriften stellt deshalb unmittelbar eine Verletzung der grundgesetzlich garantierten Rechte des einzelnen Wahlbürgers dar.

Alles Wahlrecht ist „...materielles Staatsrecht, konstituiert aus verfassungsrechtlichen und einfachgesetzlichen Normen. Von seinem Wesensgehalt her ist es Demokratie-Recht."[5] „Wahlen zum BT einschließlich Wahlprüfungsverfahren sind mithin *verfassungsrechtlicher Natur*"[6].

2.3. Somit sind Verletzungen der einfachgesetzlichen Normen auch Verletzungen der Verfassung und damit des Rechtsstaatsprinzips.

2.4. Wegen der wahlrechtlich beanstandeten Geräte-Abstimmungen, die das Gesamtwahlergebnis erheblich beeinflussen (s. nachfolgend Abschnitt 7 „Mandatsrelevanz") ist auch der Einsprechende in seinen staatsbürgerlichen Rechten verletzt. Er hat einen verfassungsrechtlichen Anspruch auf ein rechtlich „richtiges" Wahlergebnis.

2.5. Aus dem Demokratie-Prinzip wird das *Öffentlichkeitsprinzip* abgeleitet, das durch mannigfache Gesetzesvorschriften organisiert wird (§§ 10, Abs. 1, Satz 1 u. 17 , Abs. 1, Satz 2 u. 26, Abs. 3, u. 31, Satz 1 BWG sowie §§ 54 und 67 ff BWO).

„Die Öffentlichkeit übt gegenüber den Wahlorganen eine Kontrollfunktion aus. […] Geheime Auszählungen sind danach gesetzwidrig".[7] So hat jedermann auch Zutritt zu den Sitzungen der Wahlausschüsse und Wahlvorstände[8], d.h.: Jeder kann Wahlhandlungen sowie die Ermittlung und Feststellung von Wahlergebnissen beobachten.

„Der Ausschluss von Beobachtern […] ist grundsätzlich ausgeschlossen und stellt einen Wahlfehler dar. Das gilt auch für Stimmenauszählungsverfahren."[9]

Diese höchstrichterliche Rechtsprechung und Rechtsmeinung ist grundlegend für diese Beschwerde, da beim Einsatz von Wahlgeräten der Vorgang eines Teiles der Wahlhandlung (nämlich die Erzeugung der Stimme, vergleichbar mit der Kennzeichnung des Stimmzettels, der Speicherung der abgegebenen Stimmen im Gerät, vergleichbar der Ablage der Stimmen beim Urneneinwurf)[10] sowie die Ermittlung und Feststellung der Ergebnisse *im Inneren des Gerätes* stattfinden und deswegen nicht beobachtet werden können.

---

[5] *Wolfgang Schreiber*, Handbuch des Wahlrechts zum Deutschen Bundestag. Kommentar zum Bundeswahlgesetz, 7. Auflage, Köln 2002, S. 30, Rdnr. 2

[6] ebenda, S. 33, Rdnr. 9

[7] ebenda, S. 249 f, Rdnr. 1 mit Verweis auf BverfGE Bd. 89, S. 291, 302 f – FN 1

[8] ebenda

[9] ebenda, S.250

[10] Zur Begrifflichkeit Stimmerzeugung, Stimmabgabe und Stimmzählung (vote generation, casting, recording and counting) siehe auch: *California Institute of Technology and The Massachusetts Institute of Technology* (Hrsg.): Report of the Caltech/MIT Voting Technology Project: Voting - What Is, What Could Be (2001), S. 58 ff

2.6. Die Kontrollfunktion der Öffentlichkeit soll gewährleisten, dass die Wahlen rechtmäßig durchgeführt werden und somit das Parlament richtig zusammengesetzt ist.[11] Der „Grundsatz der Öffentlichkeit und die Transparenz des gesamten Wahlgeschäfts (vgl. §§ 10 Abs. 1, 31)“ sind Ausdruck „der in einer Demokratie unverzichtbaren Möglichkeit öffentlicher Kontrolle der Vorbereitung und Durchführung der Wahl“.[12]

Die „allgemeine Sicherung des Vertrauens in die Tätigkeit der Wahlbehörden“ und die „optimale normative Ausgestaltung des Grundsatzes der Öffentlichkeit der Wahl“[13] gehören zusammen.

2.7. Somit unterliegen sowohl die Wahlhandlung (§ 31, Satz 1 BWG) als auch die Ermittlung und die Feststellung (§§ 37-41 u. 42 BWG, §§ 67-70 u. 72 BWO – letztere beide sind das so genannte „Wahlgeschäft“ – derart genannt in § 76, Abs. 1, Satz 4 BWO) dem Grundsatz der Öffentlichkeit.

3.1. „Die Verletzung des Öffentlichkeitsgrundsatzes ist ein grundlegender Verfahrensmangel, der eine Anfechtung der Wahl rechtfertigt. Er hat die Ungültigkeit der Wahl im betreffenden Wahlbezirk (-lokal) zur Folge, wenn nach den Umständen des Einzelfalles mit an Sicherheit grenzender Wahrscheinlichkeit feststeht, „dass die Unregelmäßigkeit auf das Wahlergebnis von Einfluss gewesen ist oder sein kann“.[14]

3.2. Eben diese Ungültigkeit der Wahl in allen Stimmbezirken mit Wahlgeräten wird von dem Einsprechenden behauptet und in den nachfolgenden Abschnitten 3 bis 6 begründet. Im darauf folgenden Abschnitt 7 der Begründung wird auch eine erhebliche Mandatsrelevanz ausgewiesen.

3.3. Den Rechtsgrund hierfür liegt in der verletzten Öffentlichkeit. „In einem freiheitlich-demokratischen Rechtsstaat finden Wahlen vor den Augen der Öffentlichkeit statt.“ Das Öffentlichkeitsprinzip „… gehört zu den wichtigen Sicherungen freiheitlicher demokratischer Wahlen; es ist schlechthin die Grundvoraussetzung für eine demokratische Willensbildung“.[15]

3.4. Alle vorgetragenen Rechtsgrundsätze haben auch für die Wahlhandlung mittels Wahlgeräten sowie für die Ermittlung und die Feststellung der aus diesem Geräteeinsatz resultierenden Wahlergebnisse zu gelten.

4.1. Die Stimmabgabe mit Wahlgeräten erlaubt und regelt § 35 BWG. Dort wird zwar die Beachtung des Grundsatzes der Geheimhaltung gefordert (Absatz, 1. Halbsatz), nicht jedoch der Grundsatz *freier* Wahlen, aus dem das Öffentlichkeitsprinzip zwingend hervorgeht – und auch nicht der Grundsatz der Wahl*gleichheit.*

4.2. § 35 BWG ist somit in der Wiederholung grundgesetzlicher Prinzipien defizitär. Gleichwohl greifen die verfassungsrechtlichen Normen.

Aus der Nichterwähnung des Öffentlichkeitsprinzips als unveräußerlicher Grundlage aller demokratischen Kontrollen jedoch darf nicht geschlossen werden, es dürfe bei Wahlhandlung und Wahlgeschäft darauf verzichtet werden.

4.3. Außerdem wird dort als „öffentlich“ gefordert die Erprobung eines Geräts *vor* seiner Verwendung (§ 35, Absatz 3, Nr. 4 BWG). Diese Art von Öffentlichkeit betrifft jedoch nicht die Wahl selbst.

---

[11] *Wolfgang Schreiber*, a.a.O., S. 250, Rdnr. 1
[12] ebenda, S. 335, Rdnr. 5
[13] ebenda, S. 336, Rdnr. 7
[14] ebenda, S. 489, Rdnr. 4
[15] ebenda, S. 487, Rdnr. 2

5.1. § 34 BWG organisiert das individuelle Wahlgeheimnis mit Stimmzetteln, macht zugleich aber den äußeren Ablauf transparent: „Der Wähler faltet daraufhin den Stimmzettel in der Weise, dass seine Stimmabgabe nicht erkennbar ist *und wirft ihn in die Wahlurne*." (Kursivsetzung vom Verfasser). Der Stimmzettel-Einwurf in die Urne ist also ein öffentlich zu beobachtender Teil der Wahlhandlung, dessen Öffentlichkeit nicht das Erfordernis des Wahlgeheimnisses beeinträchtigt. Die eingesetzten Nedap-Geräte aber organisieren dieses Erfordernis der Öffentlichkeit, nämlich der beobachtbaren Stimmen-Ablage (vergleichbar mit dem Einwurf in die Urne) einer zuvor vom Wähler verifizierbar erzeugten Stimme (vergleichbar mit der Kennzeichnung des Wahlzettels) – eben nicht und entsprechen deshalb nicht dem Öffentlichkeitsgebot.

§ 37 BWG impliziert die unbestrittene Öffentlichkeit der Stimmenauszählung.

5.2. § 54 BWO schreibt explizit die Öffentlichkeit für die Wahlhandlung sowie für die Ermittlung und Feststellung des Wahlergebnisses vor (§§ 67 ff BWO). Diese Vorschriften organisieren höchst detailliert und penibel die öffentliche Ordnung und Kontrolle bei den drei Wahlstufen:

- Die Abgabe der geheimen Stimmen muss öffentlich erkennbar sein (s. zuvor),
- das Entnehmen der Zettel aus der Urne, das Auffalten und Zählen – eigentlich lauter Selbstverständlichkeiten – werden detailliert verbalisiert,
- es müssen Stimmenzettel-Stapel nach Erst- und Zweitstimmen, nach Landeslisten und Stapel mit ungekennzeichneten Zetteln gebildet werden,
- bei der Zählung der Stimmen muss jeder Stimmzettel *laut* vorgelesen werden,
- die Stapel müssen von zwei Beisitzern (also mit Gegenkontrolle) gezählt werden (§ 69, BWO),
- etc. etc. (§§ 67 – 70 BWO).

5.3. Alle solchen öffentlichen Ermittlungshandlungen fehlen bei den eingesetzten Wahlgeräten, bzw. es wird bei diesen nicht erkennbar, dass die Dokumentation und Feststellung innerhalb der Geräte manipulationsfrei vor sich geht.

Vielmehr besteht – wie in der nachfolgenden Begründung vorgetragen werden wird – eine hohe Manipulations-*Gefahr*.

Insgesamt gilt: Alle diese Vorschriften haben auch für die Verwendung von Wahlgeräten zu gelten. „Es würde deshalb dem Sinn der Verordnungsermächtigung in §35 BWG widersprechen, wenn es durch den Einsatz von Wahlgeräten zu einer Einschränkung oder auch nur einer inhaltlichen Aushöhlung der im Bundeswahlgesetz niedergelegten und in der Bundeswahlordnung für die Urnenwahl mit Stimmzetteln konkretisierten Verfahrensgrundsätze zum Schutz der freien, geheimen und gleichen Wahl kommen würde."[16]

6.1. Die Bundeswahlgeräte-Verordnung fordert und organisiert jedoch diese verfassungs-grundsätzlichen und wahlgesetzlichen Anforderungen nicht explicite im Einzelnen, obwohl § 5 BWahlG für die Verwendung von Wahlgeräten die Geltung der BWO und der Europa-Wahlordnung vorschreibt.

6.2. In dieser ihrer Disparatheit der BWahlGV zwischen detaillierten apparatetechnischen Anweisungen einerseits und ihrer nur allgemeinen Forderung nach Geltung der BWO

[16] *Martin Leder*, a.a.O., S. 653

andererseits – und damit sinngemäß des BWG – liegt wohl der Grund für die Tatsache, daß die Prüf- und Zulassungsverfahren sich vornehmlich oder sogar ausschließlich auf die technischen Vorschriften konzentrieren.

Die verfassungsgrundsätzlichen und wahlrechtlichen Kategorien, Prinzipien, Normen u.a. werden von der BWahlGV vernachlässigt und in der Folge davon offensichtlich auch von der Praxis in Prüfung und Einsatz ausgeklammert.

7. Gegenstand dieses Einspruches ist es, die Verfassungs- und Wahlrechtswidrigkeiten derartiger Zusammenhänge im einzelnen herauszuarbeiten und – jenseits des eigentlichen Einspruchs – auch eine *Korrektur de lege ferenda* einzufordern.

8. Die Verletzung der Verfassungs- und Wahlrechtsnormen stellt insgesamt eine Verletzung des Rechtsstaatsprinzips dar.

3. Fehlenden Kontrollmöglichkeit

a) Nach allem vorstehend Vorgetragenen ist die durch das BWG für Wahlgang und Wahlgeschäft vorgeschriebene Öffentlichkeit ein Kontrollmechanismus, der die ordnungsgemäße Durchführung der Wahlen gewährleistet. Diese Kontrolle durch die Öffentlichkeit ist Voraussetzung für echte demokratische Wahlen und wesentliches Unterscheidungsmerkmal zu Scheinwahlen in totalitären Staaten. Wird der Kontrollmechanismus „Öffentlichkeit“ im Wahlgeschäft oder Wahlgang teilweise eingeschränkt, so muss er durch entsprechend wirksame Kontrollmechanismen ersetzt werden. Diese äquivalenten Kontrollmechanismen müssen transparent und öffentlich verifizierbar sein, wenn sie wirksam die Manipulation von Wahlen verhindern sollen.

b) Bei den Nedap-Wahlgeräten handelt es sich um Wahlcomputer, auf denen ein komplexes Softwareprogramm installiert ist. Der Wähler gibt seine Stimme mittelbar über das Wahlgerät ab, und die Stimme wird von der Software in einen Stimmenspeicher geschrieben. Am Ende der Wahl werden die Stimmenspeicher von der Software ausgelesen, und das Wahlergebnis über ein in das Gerät integrierten Drucker ausgegeben. Da die Stimmabgabe geheim erfolgt und die Funktionsweise der Software nicht transparent, also vom Wähler nicht unmittelbar einsehbar ist, ist es prinzipiell nicht möglich, die ordnungsgemäße Speicherung und Zählung der Stimmen zu kontrollieren. Denkbar wäre z.B., dass eine fehlerhafte Software einen bestimmten Anteil der abgegebenen Stimmen unabhängig von der Wahl des jeweiligen Wählers einer bestimmten Partei zuweist, oder dass eine manipulierte Software lediglich die abgegebenen Stimmen zählt und nach einem vorgegebenen Verhältnis auf die zur Wahl stehenden Parteien verteilt.

c) „Weder der Wähler noch der Wahlvorstand können wissen, ob nicht irgend jemand den Chip ausgetauscht hat. Also auch nicht, was mit der Stimme passiert. Technisch gibt es keine Garantie für richtige Speicherung, wenn der gewählte Kandidatenname auf dem Display angezeigt wird.“[17]

d) Diese Problematik ergibt sich ausschließlich aus der Mittelbarkeit der Stimmabgabe und dem Verzicht auf eine alternativen Kontrollmöglichkeit. Bei konventionellen (etwa mechanischen) Wahlgeräten tritt sie in dieser Form nicht auf, da das Funktionsprinzip unmittelbar transparent ist, und bei reinen Stimmzählgeräten ist in der Regel eine manuelle Verifikation des Ergebnisses möglich. Daher ist es erforderlich, die

[17] *Jakob Klein*, Bitte keine Kreuze machen! Frankfurter Allgemeine Sonntagszeitung, 21.08.2005, Nr. 33, S. 58

ordnungsgemäße Wahldurchführung durch einen alternativen Kontrollmechanismus sicherzustellen. Dieser Kontrollmechanismus muss öffentlich verifizierbar sein.

e) Die BWahlGV bestimmt zwar in §15 Abs. 3 und §16 Abs. 2 die Versiegelung sichere Aufbewahrung der Stimmenspeicher. „Der Stimmenspeicher gibt aber über die Art und Weise, in der die Abgabe und die Zählung der Stimmen erfolgten, keine Auskunft. Deshalb lassen sich Vorwürfe wie diese, das Gerät habe nicht mit der zugelassenen Bauart übereingestimmt oder die Angaben auf der Benutzeroberfläche seien unvollständig gewesen oder die Benutzeroberfläche sei für die Abgabe der Stimme nicht richtig programmiert worden, nicht mit hinreichender Sicherheit aufklären.“[18]

3.1. Gefährdungspotential

a) Bei Wahlen mit softwaregesteuerten Wahlgeräten geht eine besondere Gefahr von dem Umstand aus, dass der Gerätehersteller einen zentralen Angriffspunkt darstellt und sich Wahlen über eine Manipulation der Software noch beim Gerätehersteller wesentlich wirkungsvoller als Urnenwahlen manipulieren lassen. Eine solche Manipulation könnte etwa durch einen durch Drohungen, politisch oder finanziell motivierten Insider beim Hersteller erfolgen. Ein Angriff auf den Hersteller ist auch von außen denkbar, etwa über Viren oder Trojaner, die Dritten einen Zugang auf die Rechner des Herstellers ermöglichen. Wegen der Komplexität der eingesetzten Software mit über zweihunderttausend Zeilen Quellcode kann eine solche Manipulation auch bei sorgfältiger Qualitätskontrolle des Herstellers unentdeckt bleiben.

b) Die von solchen Manipulationen ausgehende Gefahr ist umso größer, je höher der Anteil der Wähler ist, die mit dem Wahlgerät eines bestimmten Typs abstimmen. Die Firma Nedap ist derzeit der einzige Anbieter von softwaregesteuerten Wahlgeräten mit Bauartzulassung gemäß BWahlGV, und die Zahl der eingesetzten Nedap-Geräte hat sich seit der Bundestagswahl 2002 verdoppelt. Es ist daher nur eine Frage der Zeit, bis sich über die Manipulation der Nedap-Software die Mehrheitsverhältnisse im Deutschen Bundestag kontrollieren lassen.

c) Der Wähler als Souverän hat einen Anspruch darauf, dass von den mit der Durchführung der Wahl beauftragten Organen wirksame Mittel ergriffen werden, um solche Manipulationen auszuschließen. Das Öffentlichkeitsprinzip des BWG erfordert außerdem, dass der Öffentlichkeit wirksame Kontrollmechanismen zur Verfügung stehen, um eine Manipulation der Software, auch durch die mit der Durchführung der Wahl beauftragten Organe, erkennen und verhindern zu können. Solche Kontrollmöglichkeiten hat die Öffentlichkeit derzeit nicht, sie ist im Gegenteil von der Kontrolle der eingesetzten Software völlig ausgeschlossen.

3.2. Fehlen eines verifizierbaren Protokolls

a) Einen wirksamen Kontrollmechanismus kann z.B. ein verifizierbares, vom Wähler einsehbares Papierprotokoll der abgegebenen Stimmen darstellen, das die Möglichkeit einer Überprüfung des Wahlergebnisses bietet. Im angelsächsischen Raum wird diese Möglichkeit als Voter-Verifiable Audit-Trail bezeichnet. Damit ist ein System gemeint, bei dem ein in das Wahlgerät integrierter Drucker die Wahlentscheidung des Wählers protokolliert. Dieses Protokoll ist vom Wähler hinter Glas einsehbar. Um das

[18] *Martin Leder*, a.a.O., S. 652

Wahlgeheimnis sicherzustellen, fallen diese Quittungen einzeln in eine Wahlurne und stehen nach Ende der Wahl für eine manuelle Kontrollzählung zur Verfügung. Ein solches System stellt sicher, dass das Wahlergebnis unabhängig von der Vertrauenswürdigkeit der eingesetzten Software verifizierbar bleibt.[19]

b) Die Nedap-Geräte verfügen hingegen über keinerlei Kontrollmöglichkeit und sind deshalb per se anfällig für Manipulationen. Die irische CEV bemängelt das Fehlen eines überprüfbaren Protokolls und kommt zu dem Schluss, dass es nicht möglich ist zu prüfen, ob die im Stimmenspeicher hinterlegten Stimmen tatsächlich mit den durch den Wähler in den Wahlcomputer eingegebenen Stimmen übereinstimmen.[20]

c) Im Rahmen ihrer Arbeit hat die CEV die irische Öffentlichkeit aufgerufen, sich zur Sicherheit und Zuverlässigkeit der Wahlgeräte zu äußern. Die meisten Äußerungen bemängelten dabei das Fehlen eines vom Wähler überprüfbaren Papierprotokolls. Die Notwendigkeit eines solchen Protokolls ergäbe sich

   1. zur Sicherstellung der Zuverlässigkeit der Software aus der Komplexität der Software,
   2. aus der Notwendigkeit, Manipulationen an Wahlgerät und Software auszuschließen,
   3. aus dem öffentlichen Interesse daran, die Zuverlässigkeit der Wahlgeräte belegen zu können.[21]

d) Die Bedeutung der fehlenden Kontrollmöglichkeit wird unmittelbar verständlich an einem Beispiel aus der Finanzwelt: Einer Bank, die ihren Kontoinhabern zwar monatlich die Zahl der Umsätze auf deren Girokonten und die neuen Kontosalden mitteilt, ihren Kunden aber Kontoauszüge mit verifizierbaren Umsatzinformationen vorenthält, würde man ohne Not nicht vertrauen wollen. Eben dieses Vertrauen wird vom Wähler beim Einsatz der Nedap-Geräte verlangt.

3.3. Vertrauenswürdigkeit der Software

a) Aus dem Verzicht auf eine alternative Kontrollmöglichkeit der Stimmenspeicherung folgt unmittelbar, dass an die Vertrauenswürdigkeit der Software besonders hohe Maßstäbe anzulegen sind. Dabei kann es keinesfalls ausreichend sein, dass die eingesetzte Software dem BMI als oberster Wahlbehörde vertrauenswürdig erscheint. Das Öffentlichkeitsprinzip und die implizierte Kontrollfunktion der Öffentlichkeit erfordern, dass die Vertrauenswürdigkeit der Software allgemein verifizierbar ist. Eine solche Verifizierbarkeit ist derzeit nicht gegeben:

   - Das Zulassungsverfahren für die Geräte einschließlich der Prüfung durch die PTB ist nichtöffentlich und schon deshalb nicht verifizierbar,

---

[19] Auch andere Konzepte der physischen Verifizierbarkeit sind denkbar So hat etwa das Caltech/MIT Voting Technology Project vorgeschlagen, die Stimmabgabe die Stimmerzeugung und Stimmzählung in getrennten Geräten vorzunehmen. Die (z.B. auf Chipkarten) abgelegten Stimmen werden vom Wähler mit dem ersten Gerät erzeugt. Die Stimme wird anschließend in ein zweites Gerät eingebracht, dass dem Wähler seine Wahl nochmals anzeigt, und das Speichermedium mit der Stimme anschließend als physikalischen, verifizierbaren Beleg einbehält. (*California Institute of Technology and The Massachusetts Institute of Technology* (Hrsg.), a.a.O., S.58 ff)

[20] "…while it is possible to independently verify that the votes recorded on ballot modules are those uploaded onto the PC at the count centre, there is no method of validating that the votes stored on ballot modules are those which were originally entered by the voters using the voting machine at the polling centre." (*Commission on Electronic Voting*, a.a.O., Part 2, S. 39)

[21] *Commission on Electronic Voting*, a.a.O., Part 3, S. 44f

- die Nedap-Geräte einschließlich der eingesetzten Software stehen der interessierten Öffentlichkeit nicht für eine unabhängige Überprüfung zur Verfügung,
- die Software der Nedap-Geräte ist nicht quelloffen („Open Source"), obwohl die Verfügbarkeit des Quellcodes für eine Einschätzung der Vertrauenswürdigkeit unabdingbar ist. Die irische CEV hat ausdrücklich festgestellt, dass die Zuverlässigkeit der Software ohne einen vollen Einblick in den Quellcode der Software nicht beurteilt werden kann.[22] Diese Einschätzung findet sich auch in der Anlage 1 zu §2 der BWahlGV wieder, die einer Vorlage des Quellcodes im Rahmen des Zulassungsverfahrens erfordert.
- Die eingesetzt Software ist im Wahllokal nicht authentifizierbar, d.h. es ist nicht überprüfbar, ob die im Wahllokal zum Einsatz kommende Software tatsächlich der zugelassenen Software entspricht und diese frei von Manipulationen ist.

b) Aus diesem Grunde ist in Wahllokalen, in denen die Nedap-Geräte zum Einsatz kommen, das Prinzip der öffentlichen Kontrolle der Wahlen ausgehebelt. Dies steht im klaren Widerspruch zu den Anforderungen des BWG.

c) Ganz unabhängig davon stellt sich die Frage, ob es dem Wähler als Souverän zuzumuten ist, bei der Beurteilung der ordnungsgemäßen Durchführung von Wahlen auf eine Experten-Öffentlichkeit angewiesen zu sein, oder ob nicht die Wahl als grundlegender Akt der staatlichen Legitimation für jedermann transparent nachvollziehbar und kontrollierbar bleiben muss.

4. Authentizität der Software

a) Ein prinzipielles Problem bei der Vertrauenswürdigkeit von Software ist die Frage, ob die vom Anwender eingesetzte Kopie der Software mit einer ursprünglich geprüften Software identisch und damit frei von Manipulationen ist. Zur Authentifizierung von Software gibt es verschiedene etablierte Verfahren. Oft wird dabei eine Zeichenkette, ein so genannter Hash-Wert, berechnet, die mit einer ebenso berechneten Zeichenkette der Original-Software verglichen wird. Es ist praktisch nicht möglich, die Software so zu verändern, dass die vom Algorithmus gelieferte Zeichenkette unverändert bleibt.[23]

b) Wesentlich bei solchen Prüfverfahren ist, dass der Prüfalgorithmus und die zu prüfende Kopie der Software nicht aus derselben Quelle stammen, da sonst die Vertrauenswürdigkeit des Prüfalgorithmus mitgeprüft werden muss. Ein Angreifer könnte ohne weiteres den Prüfalgorithmus so verändern, dass er auch für die manipulierte Software wieder die erwartete Zeichenkette liefert. Genau diese Anforderung erfüllen die Nedap-Geräte nicht: Die beim Gerätestart angezeigten und auch ausgedruckten Prüfsummen werden von der eingesetzten Software selbst berechnet und sind deshalb nicht geeignet, eine Manipulation der Software zu verhindern. Sie können allenfalls dazu dienen, den versehentlichen Einsatz einer falschen oder unvollständigen Softwareversion zu erkennen.

---

[22] "…as the system is self auditing and does not provide a facility for independent audit of the process for the recording of votes, the requirement for a full source code review is heightened significantly on account of the need to establish that no unexpected behaviour of the system will occur that cannot be identified by means of 'black box' testing." (*Commission on Electronic Voting*, a.a.O., Part 2, S. 31).

[23] Weit verbreitet sind zum Beispiel Algorithmen wie MD5 und SHA-1 (siehe z.B. http://de.wikipedia.org/wiki/Hash-Funktion)

c) Zu diesem Schluss kommen auch Mc Donnell und Cunningham vom Department of Computer Science des Trinity College Dublin in einem Gutachten für die Irische Kommission für elektronische Wahlen. Sie stellen fest, dass Personen, die Zugang zum Quellcode der eingesetzten Software haben, diese Software einschließlich der internen Prüfsummenberechnung so verändern könnten, dass das Wahlergebnis in ihrem Sinne verändert wird, obwohl das Wahlgerät weiterhin beim Anschalten die erwarteten Prüfsummen anzeigt.[24] Dies steht im eindeutigen Widerspruch zu den Richtlinien für die Bauart von Wahlgeräten, die vorschreiben, „dass eine Veränderung auch der installierten Software durch unbefugte Dritte nicht unbemerkt bleibt“[25]

4.1. Authentizität des vorgelegten Quellcodes

a) Für die Einschätzung der Vertrauenswürdigkeit einer komplexen Software ist in der Regel ein Einblick in den Quellcode der Software erforderlich. Diese Einschätzung findet sich in den Abschnitt B.1 der Richtlinien für die Bauart von Wahlgeräten (Anlage 1 zu §2 BWahlGV) wieder, der neben der Vorlage des lauffähigen Programms (Objektcode) auch die Vorlage des kommentierten Quellcodes verlangt.

b) Um die Vertrauenswürdigkeit des lauffähigen Programms zu gewährleisten, ist aber die gleichzeitige Vorlage von Objekt- und Quellcode nicht ausreichend, es muss auch geprüft werden, ob sich das lauffähige Programm tatsächlich aus dem vorgelegten Quellcode erzeugen lässt. Eine solche Überprüfung erfordert das Übersetzen (Compilieren) des Quellcodes unter definierten Bedingungen und einen anschließenden Vergleich der Hash-Werte für den vorgelegten und erzeugten Objektcode.

c) Soweit sich der Prüfansatz der PTB aus den irischen Publikationen und der BWahlGV erschließen lässt, erfolgt eine solche Überprüfung nicht. Daher ist nicht sichergestellt, dass der PTB nicht bereits ein manipulierter Objektcode vorgelegt wird, in dem sich etwa eine Hintertür oder ein so genannter Trojaner befindet, über die später eine weitere Manipulation der Software möglich ist oder die später im Wahllokal zu einem Verhalten der Software führen, die vom Verhalten im Test erheblich abweicht.

d) Ebenso wenig erfolgt durch die PTB eine geräteunabhängige Ermittlung eines Hash-Wertes für die geprüfte Software, der später zur Authentifizierung der in den Wahllokalen eingesetzten Software verwendet werden könnte. Damit bleibt auch die Anforderung der Richtlinien für die Bauart von Wahlgeräten nach einer „eindeutigen Identifikation der installierten Software“[26] unerfüllt.

[24] “Might it be possible to tamper with a voting machine’s software? The answer is that this is theoretically possible. Someone with access to Nedap’s source code (written in C) could alter the program while also ensuring that it returned the expected checksum at start-up. One possible alteration, for example, would be to enable a voter to press buttons in a specific sequence during polling that would cause the machine to alter preferences in favour of a particular candidate from that point on. The danger that machine software can be altered is explicitly highlighted by PTB [ref. 11, p.11]: ‘an exchange of the ROM chips including fraudulent presentation of the correct checksums cannot be avoided by software but by means of sealing only’. […] There are no tests that would detect fraudulent exchange of voting machine software; this may be avoided by secure storage of voting machines between elections.” (*Neil McDonnell, Pádraig Cunningham*, in: Commission on Electronic Voting, a.a.O., Appendix 2A – Part 1, S. 96)

[25] Anlage 1 zu §2 BWahlGV, Teil B, Abs. 2.1 Satz 2

[26] Anlage 1 zu §2 BWahlGV, Teil B, Abs. 1 Punkt 2

4.2. Authentizität der eingesetzten Software

a) Die BWahlGV verlangt vom Hersteller der Wahlgeräte die Abgabe einer Baugleichheitserklärung (§2 Abs. 6) für jedes in den Verkehr gebrachte Gerät. Eine über das Vorliegen dieser Baugleichheiterklärung hinausgehende Prüfung der ausgelieferten Wahlgeräte erfolgt nicht. Insbesondere erfolgt keine Authentifizierung der eingesetzten Software, so dass sich die mit der Durchführung der Wahl befassten Organe auf eine wirksame Qualitätssicherung beim Hersteller verlassen müssen sowie darauf, dass die Software nach der Herstellerüberprüfung nicht mehr manipuliert wird. Dies ist mit der Amtlichkeit der Wahl unvereinbar. Die Wahlbehörden haben jederzeit die tatsächliche Sachherrschaft über den Geschehensablauf zu wahren.[27]

b) Die Authentifizierung der eingesetzten Software ausschließlich dem Hersteller zu überlassen ist ebenso grotesk wie der Gedanke, die Auszählung der Stimmen bei einer Urnenwahl nichtöffentlich durch einen Dienstleister ausführen zu lassen, nur weil dieser schriftlich bestätigt, die Zählung ordnungsgemäß durchzuführen.

5. Technische und konstruktive Mängel

5.1. Sicherheit und Vertrauenswürdigkeit des Systems

a) Die irische CEV kommt zu dem Schluss, dass die Sicherheitsmerkmale des Systems vom Hersteller definiert sind, anstatt sich an international anerkannten Sicherheitskriterien zu orientieren. Solchen allgemein anerkannten Sicherheitskriterien würde das System überwiegend nicht entsprechen.[28]

b) Ein Gutachten der Dublin City University kommt sogar zu dem Schluss, dass das System sicherheitstechnisch dem Stand der 1980er Jahre entspreche, als Sicherheitsmängel solcher Systeme noch nicht ausreichend verstanden wurden. Entsprechend fehlten inzwischen verfügbare effektive Sicherheitsmaßnahmen. Die Sicherheit des Systems sei inadäquat und erlaube es einem Insider mit kurzfristigem Zugang zum Wahlgerät, den Stimmenspeichern oder dem Auswertecomputer, die gespeicherten Stimmen zu verändern. Das Sicherheitskonzept des Systems beruhe überwiegend auf dem aus heutiger Sicht unakzeptablen Konzept „Security by Obscurity“, also auf dem Ansatz, Sicherheit in erster Linie durch fehlende Transparenz herzustellen.[29]

c) Es ist völlig unakzeptabel, dass ein Wahlsystem, das auf eine systemunabhängige Verifizierbarkeit des Wahlergebnisses verzichtet, in seinem Sicherheitsansatz nicht

---

[27] *Martin Leder*, a.a.O., S. 654

[28] “It is concluded that security features of the system … are self-defining instead of being measured against internationally recognised criteria and that such criteria appear to be absent from the original specification for the system.” (*Commission on Electronic Voting*, a.a.O., Part 2, S. 35)

[29] “1. The voting system is 1980’s technology. In the 1980’s the threats to this kind of technology were not as well understood as they are today; furthermore many effective defensive counter-measures have been perfected in the meantime (such as the use of cryptography) which are not deployed here.
2. Security is inadequate. A determined individual insider with short-term access to a voting machine, ballot modules or the count-centre computer could significantly affect the recorded votes. With the possible exception of the voting machine such tampering could be done in an undetectable fashion.
3. Security, such as it is, relies largely on the long discredited concept of ‘Security Through Obscurity’. It is a well-established principle in the world of electronic and computer security, that this is inadequate.”
(*Charlie Daly*, *David Gray*, *Michael Scott*, *Renaat Verbruggen*: Review of Hardware, Software Security and Testing, Appendix 2B to *Commission on Electronic Voting*, a.a.O., S. 129)

allgemein anerkannten Konzepten folgt. Die Feststellungen der irischen CEV und der beteiligten Gutachter stehen im klaren Widerspruch zu den Richtlinien für die Bauart von Wahlgeräten, die ausdrücklich verlangen, dass das Wahlgerät in seiner Konstruktion dem „allgemeinen Stand der Technik“ entspricht und „unter Beachtung der für Systeme mit schwerwiegenden Schadensfolgen bei Fehlverhalten (hohe Kritikalität) anerkannten Regeln der Technik aufgebaut“ ist[30]. Der Einsatz der Nedap-Geräte und die dabei zustande gekommenen Wahlergebnisse sind allein schon deshalb rechtswidrig.

5.2. Mangelhafte Gerätesicherheit

a) Nach der Auslieferung der Geräte hängt die Vertrauenswürdigkeit der Geräte wesentlich davon ab, ob unbefugter Zugang zu den Geräten wirksam verhindert wird und ob Manipulationen an den Geräten erkennbar sind.

b) Nach Einschätzung von Mitarbeitern der Dublin City University lässt sich der Speicherbaustein, auf dem die Wahlsoftware gespeichert ist, innerhalb von zwei Minuten auswechseln.[31] Deshalb ist es unerlässlich, dass die Geräteelektronik vor Manipulation gesichert ist. Die Elektronik befindet sich auf der Rückseite des Gerätes unter einer verschraubten Abdeckung und ist durch zwei vom Hersteller angebrachte – also nichtamtliche – Siegel gesichert. Diese Siegel können offenbar ohne große Schwierigkeit entfernt werden.[32] Somit besteht kein ausreichender Schutz gegen eine Manipulation des Wahlgerätes. Das gilt auch deshalb, weil die Geräte während der Wahlvorbereitung nicht ständig versiegelt sind (und auch nicht sein können) und auch keine Regelungen zur sicheren Verwahrung der Wahlgeräte bestehen.

c) Wie inkonsistent und lückenhaft das Sicherheitskonzept des Herstellers ist, zeigt sich an folgendem Beispiel: Vor und nach dem Wahlgang werden die Geräte über zwei farbig markierte Schlüssel in einen anderen Betriebszustand versetzt, der die Konfiguration und das Auslesen der Stimmenspeicher ermöglicht. Diese Schlüssel sind, mindestens in Irland, bei allen Geräten identisch, wodurch der unautorisierte Zugang zu solchen Schlüsseln erheblich erleichtert wird.[33]

5.3. Mangelhaft gesicherte Stimmenspeicher

a) Die Stimmen werden in den Stimmenspeichern unverschlüsselt abgelegt. Bei den Stimmenspeichern handelt es sich um einfachste Bauelemente aus Standardkomponenten,

---

[30] Anlage 1 zu §2 BWahlGV, Teil B, Abs. 2.1 Satz 1

[31] “In practice it took a technician about 40 seconds to open the machine from the back. We observed that the controlling program chips are actually socketed for ease of access. Therefore there is little to prevent removal and substitution of the program […]. We estimate that 2 minutes of unauthorised access would be sufficient to switch programs.” (*Charie Daly et. al.*: Review of Hardware, Software Security and Testing, Appendix 2B to *Commission on Electronic Voting*, a.a.O., S.139)

[32] “The seals on the voting machine peeled back equally easily. Four Philips head screws had to be removed. The voting machine uses the same circuit board as the Programming/Reading Unit, only with different peripherals plugged into the numerous (11!) connectors.” (*Richard Sinnott, Ted Selker, Bil Lewis Brendan, Whelan James, Williams James, McBride*: Evaluation of Voting Machine, Peripherals and Software, in: Appendix 2C to *Commission on Electronic Voting*, a.a.O., S.189)

[33] *Commission on Electronic Voting*, a.a.O., Part 2, S. 35

deren Spezifikation öffentlich verfügbar ist.[34] Die Bausteine sind ohne weitere Beschädigung zu öffnen und wieder zu schließen.[35]

b) Da die Stimmen in den Stimmenspeichern unverschlüsselt abgelegt werden, besteht die einzige Sicherungsmaßnahme gegen ein bösartiges Manipulieren der Speicher in den Nedap-spezifischen Steckverbindungen, über die die Speicher mit den Wahlgeräten bzw. Lesegeräten verbunden werden.

5.4. Sicherheitsmängel der Auswertecomputer

a) Die Wahlgeräte werden über besonders gesicherte Personalcomputer für die Wahlen konfiguriert. Diese gesicherten PCs werden auch für die Auswertung der Stimmenspeicher im Wahlamt eingesetzt.

b) Die irische CEV hat bei diesen gesicherten Computern erhebliche Sicherheitsmängel festgestellt, die das Aushebeln der Sicherheitsmaßnahmen ermöglichen.[36] Die nötigen Schritte für das Aushebeln dieser Sicherheitsmaßnahmen sind in einem Gutachten der City University Dublin im Detail dokumentiert.[37]

c) Außerdem seien mehrere Versionen der auf den PCs installierten Software im Umlauf, der Einsatz der aktuellen Version aber nicht sichergestellt. Auch das gleichzeitige Installieren mehrerer Versionen auf einem PC sei möglich. Im Übrigen seien keine Sicherheitsmaßnahmen implementiert, die verhindern, dass essentielle Schritte der Wahlvor- und -nachbereitung auf völlig ungesicherten Personalcomputern durchgeführt würden.[38]

6. Organisatorische Mängel

6.1. Fachliche Zuständigkeit

a) Es ist offensichtlich, dass die BWahlGV und die Richtlinien für die Bauart von Wahlgeräten unter Mitwirkung der PTB entstanden sind. Das lässt sich aus dem Fokus der Anforderungen auf den apparatetechnischen Bereich (Belastbarkeit, Haltbarkeit,

---

[34] *Charie Daly et. al.*: Review of Hardware, Software Security and Testing, Appendix 2B to *Commission on Electronic Voting*, a.a.O., S.141f

[35] "The memory module snapped open and exposed readily available, labelled parts with no security provisions. Putting it back together without noticeable damage was simple." (*Richard Sinnott, Ted Selker, Bil Lewis Brendan, Whelan James, Williams James, McBride*: Evaluation of Voting Machine, Peripherals and Software, in: Appendix 2C to *Commission on Electronic Voting*, a.a.O., S.189)

[36] "In the case of the hardened PC on which elections are configured before the poll and on which the votes are counted afterwards, it was found that the 'hardening' measures were easily bypassed so as to allow the PC's suppressed functions to be re-enabled, possibly for purposes which might interfere with the functioning of the software or the conduct of the election. " (*Commission on Electronic Voting*, a.a.O., Part 3, S. 56)

[37] *Charie Daly et. al.*: Review of Hardware, Software Security and Testing, Appendix 2B to *Commission on Electronic Voting*, a.a.O., S. 151

[38] "Multiple versions of the application software are in circulation and, although guidelines and training are given, there is no express control over which version is used in any particular case. It is possible to load and run older versions of the software onto the hardened PC in parallel with newer versions while any version can be overwritten, quite possibly inadvertently, by another. In addition, it appears that there is nothing in the overall deployment procedures that would force key aspects of running the election to be carried out on the hardened PC rather than on any other PC." (*Commission on Electronic Voting*, a.a.O., Part 3, S. 56)

Rückwirkungsfreiheit, Energieversorgung) sowie funktionale Anforderungen erschließen, die sich im Kompetenzbereich der PTB befinden.

b) Bei den Nedap-Geräten handelt es sich jedoch um Computer mit einer komplexen Software, die auf über zweihunderttausend Zeilen Quellcode beruht. Ein Fokus der Zulassungsprüfung auf apparatetechnische Kriterien ist daher völlig unangemessen. Es ist ganz offensichtlich, dass der Kompetenzträger des Bundes für Software-Sicherheit, das Bundesamt für Sicherheit in der Informationstechnik, weder bei der Gestaltung der BWahlGV einbezogen wurde noch im Rahmen des Zulassungsverfahrens von Wahlgeräten einbezogen wird. Die fehlende Definition von konkreten Anforderungen an die Softwaresicherheit bei der Zulassung eines solchen Wahlcomputers stellt einen erheblichen Verstoß gegen die Sorgfaltspflicht dar und ist als grob fahrlässig zu werten.

6.2. Sicherheitsmängel in der Organisation des Wahlgeschäfts

a) Aufgrund der erheblichen Probleme, die durch unautorisierten Zugang zu den Geräten, Zubehör und Software entstehen können, sieht die irische Kommission für elektronisches Wählen die dringende Notwendigkeit, unautorisierten Zugang zu den Geräten auch zwischen verschiedenen Wahlen durch geeignete Sicherheitsmaßnahmen zu verhindern.[39] Eine solche Kontrolle findet in Deutschland nicht statt, und es sind auch keine angemessenen Regelungen in Kraft, die eine solche Zugangskontrolle sicherstellen könnten.

b) Es ist deshalb davon auszugehen, dass die Geräte als Ganzes in der Regel ausschließlich am Wahltag versiegelt werden.[40] Dies ist wegen der beschriebenen Sicherheitsmängel nicht ausreichend: Eine Manipulation an den Geräten ist durch wirksame amtliche Versiegelung und angemessene, sichere Verwahrung dauerhaft zu gewährleisten.

7. Mandatsrelevanz

7.1. Erststimmenergebnis

Der Bundeswahlleiter hat dem Einsprechenden auf Anfrage eine Kundenliste des Geräteherstellers überlassen, dass die zum Einsatz vorgesehenen Wahlgeräte nach Wahlkreisen und Gemeinden aufschlüsselt.[41] Eine Liste der Wahlbezirke, in denen die Nedap-Geräte tatsächlich eingesetzt wurden, existiert nach Auskunft des Statistischen Bundesamtes nicht.

In den Wahlkreisen

- 64 Cottbus - Spree-Neiße,
- 94 Köln I,

[39] "In view of the significant issues which can arise through unauthorised access to voting machines and other equipment and software used for electronic voting, it is of vital importance that there are correspondingly substantial procedures and controls in place to minimise the likelihood of such access, both at election time and between elections. This requirement is accentuated by the fact that voting equipment is stored at numerous different locations around the country." (*Commission on Electronic Voting*, a.a.O., Part 2, S. 36).

[40] *Jakob Klein*, a.a.O.

[41] Kundenliste zur Bundestagswahl 2005, 12.08.2005; durch das Statistische Bundesamt per E-mail dem Einsprechenden am 04.10.2005 mitgeteilt.

- 95 Köln II,
- 96 Köln III,
- 98 Rhein-Sieg-Kreis I,
- 99 Rhein-Sieg-Kreis II,
- 102 Leverkusen und Köln IV,
- 106 Mettmann II
- 109 Neuss I,
- 123 Recklinghausen II,
- 143 Dortmund I,
- 144 Dortmund II,
- 201 Koblenz

wurde demnach in Wahllokalen ausschließlich oder überwiegend mit den Nedap-Geräten gewählt. Die beanstandeten Mängel bei der Wahldurchführung sind hier offensichtlich mandatsrelevant, weil nicht überprüft werden kann, ob das Erstimmenergebnis in diesen Wahlkreisen rechtmäßig zustande gekommen ist.

7.2. Zweitstimmenergebnis

Nach der vom Bundeswahlleiter überlassenen Liste war der Einsatz von 1921 Geräten geplant. Da dem Einsprechenden keine Liste der tatsächlich eingesetzten Geräte vorliegt, kann die Zahl der tatsächlich mit Wahlgeräten abgegebenen Stimmen nur abgeschätzt werden. In Presseberichten ist von 2150[42] und 2200[43] Geräten die Rede. Deshalb dürfte die Zahl der mit Nedap-Geräten abgegebenen Stimmen deutlich über 2 Millionen betragen. Vor den Wahlen war von ca. 2,5 Millionen Wahlberechtigten zu lesen, die ihre Stimme mit den Nedap-Geräten abgeben sollten.[44] Dies entspricht etwa 5% der abgegebenen Stimmen und damit etwa 15 der 300 Listenmandate. Somit sind die beanstandeten Mängel offensichtlich mandatsrelevant hinsichtlich des Zweitstimmenergebnisses.

7.3. Aufstellung der betroffenen Wahlkreise

Die nachfolgende Aufstellung der angeschafften und vermutlich bei den Bundestagswahlen eingesetzten Nedap-Wahlgeräte beruht auf den Angaben der vom Bundeswahlleiter überlassenen Kundenliste des Herstellers.

Land	Wahlkreis	Ort	Anzahl	Summe
Brandenburg	58	16761 Hennigsdorf	27	27
	59	15366 Hoppegarten	15	
		15366 Neuenhagen bei Berlin	12	
		15370 Fredersdorf/Vogeldorf	10	37
	61	14513 Teltow	15	15
	62	14959 Trebbin	4	4
	64	03050 Cottbus	74	74
Summe Brandenburg: 157 Geräte				

[42] *Volker ter Haseborg:* Die ungeheure Demokratiemaschine, Spiegel Online, 12.09.2005, 16:52, URL: http://www.spiegel.de/politik/deutschland/0,1518,374301,00.html
[43] *Jakob Klein*, a.a.O.
[44] *Richard Sietmann*: Dreimal drücken – fertig? C't - Magazin für Computertechnik, 19/2005, 02.09.2005

Land	Wahlkreis	Ort	Anzahl	Summe45
Hessen	170	34266 Niestetal	7	7
	174	35683 Dillenburg	3	3
	182	65760 Eschborn	24	
		65812 Bad Soden am Taunus	15	39
	186	63179 Obertshausen	11	
		63225 Langen	21	32
	187	64665 Alsbach-Hähnlein	6	6
	189	68519 Viernheim	15	
		68623 Lampertheim	25	40
Summe Hessen: 127 Geräte				
Nordrhein-Westfalen	92	50181 Bedburg	22	22
	94	50765 Köln		
	95	50765 Köln		
	96	50765 Köln	570	570
	97	53111 Bonn	1	1
	98	53721 Siegburg	26	
		53840 Troisdorf	44	70
	99	53332 Bornheim	30	
		53639 Königswinter	22	
		53757 Sankt Augustin	29	81
	102	50765 Köln		
		51373 Leverkusen	10	10
	105	40721 Hilden	26	26
	106	40878 Ratingen	60	60
	107	40225 Düsseldorf	30	30
	108	40225 Düsseldorf		
	109	41460 Neuss	98	98
	122	45657 Recklinghausen	33	33
	123	45711 Datteln	4	
		45739 Oer-Erkenschwick	21	
		45768 Marl	52	77
	131	59320 Ennigerloh	1	1
	132	33803 Steinhagen	18	18
	134	32052 Herford	30	30
	143	44122 Dortmund		
	144	44122 Dortmund	300	300
	148	59759 Arnsberg	47	47
	150	57462 Olpe	9	9
Summe Nordrhein-Westfalen: 1483 Geräte				
Rheinland Pfalz	201	56073 Koblenz	82	82
	206	56203 Höhr-Grenzhausen	4	4
	208	55232 Alzey	2	
		55276 Oppenheim	2	4
Summe Rheinland Pfalz: 90 Geräte				
Sachsen-Anhalt	67	06862 Roßlau	7	
		39167 Irxleben	20	
		39261 Zerbst	11	
		39340 Haldensleben	3	41
	74	06231 Bad Dürrenberg	12	
		06242 Braunsbedra	10	22
		06108 Halle (Saale)	1	1
Summe Sachsen-Anhalt: 64 Geräte				
Gesamt				1921

[45] Dem Beschwerdeführer ist nicht bekannt, wie sich die 570 Geräte der Stadt Köln auf die Wahlkreise 94-96 und 102 bzw. die 300 Geräte der Stadt Dortmund auf die Wahlkreise 143 und 144 verteilen.

8. Abkürzungen

BWahlGV	Bundeswahlgeräteverordnung
BMI	Bundesministerium des Innern
BSI	Bundesamt für Sicherheit in der Informationstechnik
BWG	Bundeswahlgesetz
BWO	Bundeswahlordnung
CEV	Commission on Electronic Voting (Regierungskommission der Republik Irland zum Elektronischen Wählen)
ESD1, ESD2	Gerätebezeichnung der deutschen Wahlgeräte des Herstellers Nedap
ESI2	Gerätebezeichnung der irischen Wahlgeräte des Herstellers Nedap
GG	Grundgesetz
Nedap	N.V. Nederlandsche Apparatenfabriek
PTB	Physikalisch-Technische Bundesanstalt
WahlprG	Wahlprüfungsgesetz

Neu-Isenburg, den 06.11.2005