

Wahlnachrichten

der HSG Wahlsysteme GmbH

Oktober 2006

Statement

von Herbert Schulze Geiping

Geschäftsführer der HSG Wahlsysteme GmbH

Zu der Nachricht

„Bürgerinitiative in den Niederlanden hackt Nedap Wahlmaschine“

Die niederländische Aktivistengruppe „Wij vertrouwen stemcomputers niet“ um Rop Gonggrijp hat es mit Unterstützung einer „Mannschaft“ vom Computer Chaos Club aus Berlin ‚geschafft‘:

Sie haben sich in den Niederlanden drei Wahlgeräte besorgt und diese dahingehend verändert, dass einem Kandidaten oder einer Partei bevorzugt Stimmen zugeordnet werden.

Ich habe das in dieser Art und Weise erwartet und bin eigentlich nur etwas erstaunt darüber, dass es so lange gedauert hat! Jetzt resümiert die selbsternannte Gruppe von Computer- und Wahlspezialisten, dass alle Wahlgeräte von Nedap unsicher seien und verschwinden müssten. Das also scheint ihre Zielsetzung zu sein. Dabei wird jedoch übersehen, dass es immer um das richtige Zusammenspiel von Mensch und Technik geht, dass ein Sicherheitssystem also niemals allein in der Technik angelegt sein kann.

In Deutschland gibt es für den Einsatz von Wahlgeräten umfangreiche Gesetze und Verordnungen, Prüfungsvorschriften und Zulassungsregelungen. Zudem wird in den diversen Wahlvorschriften die Bedeutung der Wahlvorstände hervorgehoben. Das Vorhandensein solcher Vorschriften und Regelungen sowie deren Umfang und Inhalt hebt sich deutlich von den Vorgaben in anderen Ländern und insbesondere von den Vorgaben in den Vereinigten Staaten ab. Dies sei erwähnt, weil immer wieder Vergleiche mit anderen Ländern herangezogen werden.

Die Wahlgeräte ESD1 und ESD2 entsprechen in Deutschland den geltenden Vorschriften und verfügen über entsprechende Zulassungen auf Bundes- und Landesebene. Diese Zulassungen wurden nach umfangreichen und langjährigen Tests erteilt. Die Geräte erfüllen genau das, was gefordert wird und dass dies so ist, bestätigen nicht nur die Prüfzertifikate sondern auch alle Anwender mit großer Zufriedenheit. Es ist in Deutschland schon mehr als 15 Millionen Mal an den Geräten gewählt worden, ohne ein einziges Problem!

Nun wird man aber an keiner Stelle in Prozessen technische Geräte einbauen können, die von sich aus gegen rechtswidrige und verbrecherische Handlungen immun sind. Dies zu glauben ist naiv.

Genau aus diesem Grunde sind für den Einsatz von Wahlgeräten eine Kette von Sicherheitsmaßnahmen vorgeschrieben, die zum Teil von Menschen und zum Teil von der Technik abgedeckt werden. Im Folgenden ist einmal diese Kette von Sicherheitsmaßnahmen ohne Detailerläuterung und nur in den Überschriften aufgeführt:

- Prüfung nach den Gesetzen und Verordnungen.
- Erteilung einer Bauartzulassung (generell).
- Erteilung einer Verwendungsgenehmigung (pro Wahl).
- Qualitätssicherung und deren Kontrolle beim Hersteller.
- Baugleichheitserklärungen bei jedem Gerät.
- Gesicherte Aufbewahrung (von Geräten und Zubehör) in der Kommune.
- Prüfung der Unversehrtheit des Gerätes vor jedem Einsatz durch die Kommune.
- Identifizierung der richtigen Hard- und Software vor jedem Einsatz durch die Kommune.
- Prüfung und Dokumentation der richtigen Vorbereitung vor jeder Wahl durch die Kommune.
- Versiegelung des Gerätes nach den Tests der richtigen Vorbereitung durch die Kommune.
- Gesicherte Aufbewahrung und gesicherter Transport sowie Übergabe an den Wahlvorstand.
- Prüfung der Unversehrtheit und der richtigen Vorbereitung durch den Wahlvorstand.

- Überwachung des Gerätes und der Wahlhandlung durch den Wahlvorstand (mindestens sechs Augen!) während des Wahltages.
- Nach dem Ergebnisausdruck erfolgt ein Vergleich der abgegebenen Stimmen mit der Anzahl der Abgabevermerke im Wählerverzeichnis durch den Wahlvorstand.
- Kontrolle der richtigen Summenbildung der Stimmen pro Partei/Bewerber.
- Erstellung einer Niederschrift über das Ergebnis im Wahlbezirk.

Die Wahlgeräte werden immer in einer ‚geschützten Umgebung‘ gelagert, vorbereitet und betrieben. Wenn man sie nun aus dieser geschützten Umgebung herauslöst und versucht sie zu manipulieren, ist die Wahrscheinlichkeit groß, dass dieses gelingen wird. Würde man das manipulierte Gerät jedoch wieder in diesen Prozess stellen, ist die Wahrscheinlichkeit ebenfalls groß, dass dieses entdeckt wird! Genauso kann ich mir das Auto meines ungeliebten Nachbarn zugänglich machen und den CD Player durch einen Toaster ersetzen.

Eine Manipulation der Geräte, gleich an welcher Stelle im Prozess, ist gesetzeswidrig und wird strafrechtlich verfolgt! Einen umfassenden Schutz davor, dass manipulierte Geräte zum Einsatz kommen, kann nur das Zusammenwirken von menschlichen Kontrollen, organisatorischen und technischen Maßnahmen bringen.

Das erklärt auch die Aussage des Innenministeriums: „Die Wahlgeräte sind (*Zwischenbemerkung: in der Kette von Sicherungsmaßnahmen und der geschützten Umgebung*) hinreichend manipulationssicher“.

Es wird nie ein Wahlgerät geben können, das für sich allein manipulationssicher ist. Heute ist eine Sicherungsmethode ‚state of the Art‘, morgen ist sie gehackt. Hier bringt die Kette von menschlicher Kontrolle, strenger Organisation und Technik das hohe Maß an Sicherheit. Ein weiteres Sicherheitskriterium liegt darin, dass alle Geräte „stand-alone-Geräte“, also nicht vernetzt sind. Dies schließt ein externes „Einhacken“ per se aus.

Man muss natürlich ständig darüber wachen, ob die Sicherungsmaßnahmen ausreichend oder verbesserungswürdig sind. Dies tun auch alle Verantwortlichen in der Konstruktion, in der Prüfung und Zulassung, in der Kommune bei der zentralen Vorbereitung und in den Wahlvorständen.

Zu den Schlüsseln des Wahlgerätes:

Dass viele Dinge bei diesem Thema nicht verstanden werden, zeigt auch dieser Punkt. Die selbst ernannten Spezialisten bemängeln u. a. die Einfachheit der Schließmechanismen an unseren Wahlgeräten. Der Einsatz von (zwei) Schlüsseln ist nicht Teil des Sicherheitssystems im vorgenannten Sinne. Diese Schlüssel sollen lediglich verhindern, dass im Wahllokal beabsichtigt oder unbeabsichtigt ohne Wissen des Wahlvorstandes besondere Funktionen ausgelöst werden können. Insofern besteht allenfalls eine Unterfunktion im Sicherungskonzept.

Käme nun jemand, der sich für einen Euro zwei dieser Schlüssel besorgt hat ins Wahllokal und würde versuchen, an der Bedieneinheit das Gerät in einen anderen Zustand zu versetzen oder auf der Rückseite des Gerätes das Speichermodul herauszunehmen, würde das mit großer Wahrscheinlichkeit nicht unbemerkt bleiben. Das Umliegen eines Schalters oder das ungesicherte Herausziehen des Speichermoduls hingegen könnte einfacher und vielleicht unbemerkt vonstatten gehen.

Fazit

Manipulationsversuche können bei technischen Geräten nie ausgeschlossen werden, isoliert betrachtet mögen sie sogar Erfolg haben. Die Durchführung einer Wahl besteht jedoch aus mehr als einigen isoliert zu betrachtenden technischen Modulen, sodass weitere Sicherheitsmaßnahmen wirken. Wer jedoch unterstellt, dass systematisch Manipulationen erfolgen könnten, irrt sich im Gesamtsystem der Wahlorganisation. Er irrt auch in den Möglichkeiten, auch im derzeit vorherrschenden System der Zettelwahl Manipulationen vorzunehmen. Nur, diese Möglichkeiten sind in gleicher Weise strafwürdig, wie Manipulationen an technischen Geräten. Und auch hier garantiert der Mensch für die letzte Sicherheitsstufe.

nedap

HSG Wahlsysteme

HSG Wahlsysteme GmbH - Bockumer Straße 16a - 59368 Werne - Tel.: 02389 51623 - Hsg001@t-online.de