Irische Kommission für elektronische Wahlen.

Der im Dezember 2004 vorgelegte erste Bericht der Commission on Electronic Voting (CEV-2004, abrufbar im Internet unter der URL http://www.cev.ie/htm/report/first_report.htm) bemängelt die folgenden Sicherheitsaspekte:

- Die Nedap-Geräte verfügen über keinerlei unabhängige Kontrollmöglichkeit und sind deshalb per se anfällig für Manipulationen. Es sei nicht möglich zu prüfen, ob die im Stimmenspeicher hinterlegten Stimmen tatsächlich mit den durch den Wähler in den Wahlcomputer eingegebenen Stimmen übereinstimmen (S. 39).
- Die vom Gerät angezeigten Prüfsummen der Software seien als Schutz gegen Manipulationen wirkungslos (S. 96).
- Die Sicherheitsmerkmale des Wahlcomputers orientierten sich nicht an international üblichen Sicherheitskriterien. Solchen allgemein anerkannten Sicherheitskriterien würde das System überwiegend nicht entsprechen (S. 35).
- Das Sicherheitskonzept des Wahlcomputers beruhe überwiegend auf dem aus heutiger Sicht unakzeptablen Konzept „Security by Obscurity“, also auf dem Ansatz, Sicherheit in erster Linie durch fehlende Transparenz herstellen zu wollen (S. 129).
- Ein Austausch der Gerätesoftware sei innerhalb von 2 Minuten möglich und könne unbemerkt bleiben (S. 139).
- Die Schlüssel, mit denen die Geräte vor unautorisierter Bedienung geschützt werden, seinen bei allen Geräten in Irland identisch (S. 35).

Ihren zweiten und abschließenden Bericht hat die CEV im Juli 2006 vorgelegt (CEV-2006, abrufbar im Internet unter der URL http://www.cev.ie/htm/report/download_second.htm). Dieser zweite Bericht bestätigt die Befunde des ersten Berichts vom Dezember 2004. Er ergänzt die Befunde des ersten Berichts um eine vergleichende Risikobewertung einer Wahl mit Stimmzetteln und einer Wahl mit den

Nedap-Computern. Außerdem erfolgt eine detaillierte Bewertung der in Irland auch sicherheitsrelevanten Auswerte-Software IES, deren Quellcode für den ersten Bericht noch nicht untersucht werden konnte. Die Kritik der CEV an der IES-Software (*„...has not been developed in accordance with any recognisable standard process and is thus unlikely to be capable of meeting the high standards of software engineering that would be required in a mission critical system"*, S. 189) ist zwar für Deutschland aufgrund der dezentralen Auszählung nicht unmittelbar relevant, ermöglicht aber eine Bewertung der Sensibilität und Kompetenz des Herstellers im Hinblick auf sicherheitskritische Anwendungen.

Zum geprüften Wahlcomputer befindet die Kommission, die Hardware sei von guter Qualität und gutem Design. Die Software der Wahlcomputer sei offensichtlich aus einem strukturierten Design- und Entwicklungsprozess hervorgegangen und von ordentlicher (*„adequate"*) Qualität, entspreche aber nicht den Anforderungen sicherheitskritischer Anwendungen *(„mission critical",* S. 188).

Zur Sicherheit der Wahlcomputer stellt die Kommission fest, die getroffenen Maßnahmen,

- um eine unbefugte Bedienung („*access to its services*") zu verhindern,
- um Wahlvorstand und Beobachtern die Verifizierung der Software- und Hardwareversionen zu ermöglichen,
- um die Geräte vor unbefugtem Zugriff und der Veränderung der Gerätesoftware wie auch der abgegebenen Stimmen zu schützen

seinen insgesamt nicht ausreichend *(„less rigorous than appropriate")* für ein System, für das die Eignung für hohe Kritikalität gefordert sei (S. 189). Die Kommission zieht daraus den Schluss, es entstehe eine sehr hohe Abhängigkeit von der Zuverlässigkeit und Integrität der administrativen Prozesse und der sichern Handhabung *(„secure deployment")* der Geräte.