Beschreibung und Auswertung der Untersuchungen an NEDAP-Wahlcomputern

Constanze Kurz, Frank Rieger,

Rop Gonggrijp

Berlin, 30. Mai 2007

1. Einleitung

Dieser Bericht dokumentiert und erläutert die vom Chaos Computer Club in Zusammenarbeit mit der niederländischen Stiftung „Wij vertrouwen stemcomputers niet“ durchgeführten technischen Untersuchungen zur Sicherheit und Manipulierbarkeit von NEDAP-Wahlcomputern. Durch Wahlbeobachtungen in mehreren deutschen Städten hat sich der Chaos Computer Club ein Bild über die tatsächliche Praxis bei der Benutzung der Wahlcomputer in den Gemeinden gemacht. Besonderes Augenmerk wurde daher auf die praktische Relevanz der Resultate der technischen Analyse gelegt.

Durch unsere Untersuchungen konnten umfangreiche neue Informationen und Erkenntnisse gewonnen werden, die einen detaillierten Einblick in die zuvor nicht öffentlich bekannte innere Funktionsweise der NEDAP-Wahlcomputer erlauben. Dadurch ist nun erstmals eine realistische Beurteilung der Eignung dieser Wahlcomputer hinsichtlich der in einer Demokratie geltenden Anforderungen an manipulationsfeste, nachvollziehbare und transparente Wahlen möglich.

Nach einer grundsätzlichen Darstellung der Funktionsweise der NEDAP-Wahlcomputer werden die Analyse- und Arbeitsschritte zum Erstellen einer manipulierten Wahlsoftware erläutert. Methoden zur Einbringung der manipulierten Software, Möglichkeiten zur Vermeidung der Entdeckung einer Manipulation und der dafür nötige Aufwand werden dokumentiert. Weitere Manipulationsmethoden, wie der Austausch von Hardwarekomponenten des Wahlcomputers, werden ebenfalls betrachtet. Besonderes Augenmerk wird der tatsächlichen Wirksamkeit der in der Vergangenheit und derzeit angewandten Maßnahmen zum Schutz gegen unbefugten Zugriff auf die Wahlcomputer gewidmet.

Unterschieden wird bei der Betrachtung der Manipulationsmöglichkeiten nach der Art der Angreifer. Dabei wird auch die vom Hersteller und den Behörden bisher vernachlässigte Bedrohung durch Innentäter erläutert.

Die Wirksamkeit der derzeitigen Zertifizierungs- und Zulassungsprozeduren zur Abwehr realistischer Angriffe wird anhand der neu gewonnenen Erkenntnisse analysiert und bewertet. Betrachtungen zu den grundlegenden Problemen von Wahlcomputern bei der Nachvollziehbarkeit und Transparenz des Wahlverfahrens für den Wähler, zu den Risiken neu entstehender Angriffe und zu Manipulationsverfahren, die keinen direkten Eingriff in den Wahlcomputer erfordern, bilden den Abschluß des Berichtes.

2. Analyse der Software

2.1 Funktionsweise der Software im Wahlcomputer

Funktionsbestimmendes Element des Wahlcomputers ist die im Basisgerät gespeicherte Software. Beim NEDAP-Wahlcomputer handelt es um einen eher „altertümlichen“ universalen Computer[1], der nur mittels dieser spezifischen Software zum Zählen von Stimmen programmiert ist. Die Stimmabgabe erfolgt durch Drücken einer Folientaste auf der Vorderseite des Gerätes. Die Tasten für die verschiedenen Wahloptionen sind mittels einer Papierauflage beschriftet, die über die Folientasten gelegt wird.
Die Software in den untersuchten Geräten ist so programmiert, daß sie nach der Inbetriebnahme und Freischaltung einen Tastendruck abspeichert. Die softwareseitige Zuordnung der Kandidaten und Parteien zu den Tasten erfolgt mit Hilfe einer Konfiguration, die in einem Speichermodul mit Hilfe der Programmiersoftware „Integriertes Wahl System“ (IWS) in einfach zu interpretierender Form abgelegt ist.[2]

Das Ablegen der Zuordnung von Kandidaten/Parteien zu Tasten im Speichermodul wird als „Vorbereitung“ bezeichnet. Ein Tastendruck auf dem Tastenfeld, gefolgt von der Bestätigungstaste, wird als Stimmabgabe gewertet und im selben Speichermodul, in dem auch die Konfigurationsdaten abgelegt sind, einzeln gespeichert. Es wird also im Speichermodul für jede abgegebene „Stimme“ ein separater Eintrag erzeugt. Auf dem Display des Wahlcomputers wird dem Wähler die Stimmabgabe entsprechend bestätigt. Am Ende der Wahl wird jede dieser Stimmen von der Software gezählt und zu einem Ergebnis zusammengefaßt. Die Ausgabe dieses Ergebnisses erfolgt über einen Drucker.

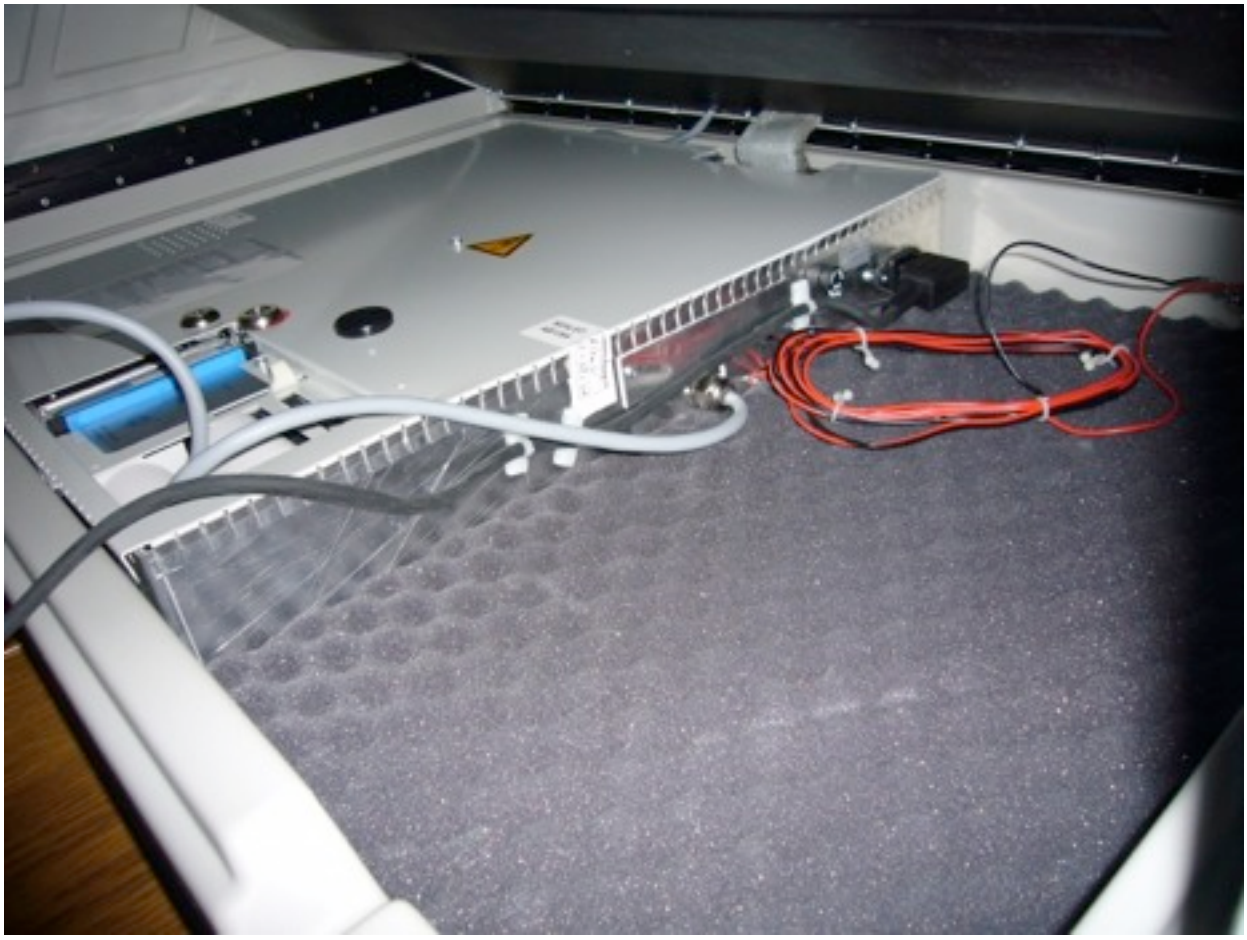
Die Auswertung der Wahlergebnisse im zentralen Wahlbüro erfolgt in der Regel durch das Auslesen der Speichermodule, auf denen die Stimmen gespeichert sind. Dies geschieht wiederum mit Hilfe der IWS-Software. Die IWS-Software wird dann verwendet, um das Gesamtergebnis mit Sitzverteilung etc. zu errechnen.[3]

---

[1] Die Hardware der NEDAP-Wahlcomputer entspricht dem Stand der Technik für industrielle Computersysteme von etwa Ende der 80er Jahre.

[2] Die Resultate der Analyse an den niederländischen NEDAP-Wahlcomputern ES3B sind eins zu eins auf die in Deutschland zugelassenen Geräte übertragbar. Siehe dazu auch den Bericht der niederländischen Zertifizierungsbehörde TNO (Nederlandse Organisatie voor toegepast-natuerwetenschappelijk onderzoek) zur Baugleichheit und der Verwendbarkeit von in Deutschland verwendeten NEDAP-Bautypen bei Wahlen in den Niederlanden in Anlage 1.

[3] Siehe die allgemeine Beschreibung des NEDAP-Wahlsystems vom deutschen Importeur. http://hsg-wahlsysteme.de/IWS/System.htm



Blick auf das Computermodul hinter der Abdeckplatte

2.2 Arbeitsschritte zum Erstellen einer manipulierten Software

Im Zuge der Untersuchung wurden verschiedene manipulierte Software-Versionen für die NEDAP-Wahlcomputer erzeugt. Dazu wurde die Software aus dem Festspeicher eines NEDAP-Wahlcomputers ausgelesen und die genaue Funktionsweise analysiert. Mit Hilfe der neugewonnenen Erkenntnisse wurde Software programmiert, welche die gewünschten Manipulationsfunktionen ergänzend zu der vorhandenen Wahlcomputer-Funktionalität realisiert. Diese manipulierte Software wurde dann auf identische Speicherbausteine übertragen, die in den Wahlcomputer eingesteckt wurden, sodaß die manipulierte Software zur Ausführung gebracht werden konnte.

Auslesen der NEDAP-Originalsoftware aus einem EPROM (Erasable Programmable Read Only Memory)

2.3 Analyse der Original-Software

NEDAP, Groenendaal B.V. (Bureau voor Verkiezingsuitslagen), HSG Wahlsysteme GmbH (HSG) und die Physikalisch-Technische Bundesanstalt (PTB) haben bisher mit Verweis auf die angeblich zu schützenden „Geschäftsgeheimnisse“ der beteiligten Firmen und die Sicherheit des Systems die Freigabe des Quellcodes und sonstiger Detaildokumentation der NEDAP-Wahlcomputer verweigert.

Um einen detaillierten Einblick in die Funktionsweise zu erhalten und die tatsächlichen Möglichkeiten zur elektronischen Wahlfälschung zu prüfen, war es daher notwendig, aus dem aus dem Festspeicher des NEDAP-Wahlcomputers ausgelesenen ausführbaren Code (sog. „Binary“) wieder von Menschen les- und verstehbaren Code zu machen. Dazu wurde ein Prozeß namens Dekompilieren (Disassembly) verwendet. Dieses semiautomatische Verfahren kehrt den Prozeß des Kompilierens[4] um.

Das für diesen Analyse-Schritt verwendete Werkzeug war die kommerziell verfügbare Software „IDA Pro“ der Firma DataRescue. In einem interaktiven Prozeß wurden damit die Markierungen für die einzelnen Funktionen und Variablen rekonstruiert sowie Programm- und Datenflußdiagramme erstellt, die ein Verständnis der Funktionsweise der Software ermöglichten. Der Gesamtaufwand dafür war gering. Im Ergebnis entstand eine

[4] Beim Kompilieren wird ein in einer dem Menschen verständlichen Programmiersprache geschriebenes Programm in auf dem Prozessor des Computers ausführbaren Code übersetzt.

hinreichend detaillierte Rekonstruktion eines lesbaren Quellcodes[5] für die Software der NEDAP-Wahlcomputer, welche die Grundlage für alle folgenden Untersuchungsschritte und die Erstellung einer Manipulationssoftware bildete.

Mit diesem Schritt wurde gezeigt, daß das Geheimhalten des Quellcodes keinen nennenswerten Sicherheitsgewinn bringt. Ein Angreifer kann mit überschaubarem Aufwand, auch ohne Kenntnis des Original-Quellcodes, in den Besitz aller notwendigen Informationen für eine erfolgreiche elektronische Wahlfälschung kommen. Das Geheimhalten des Quellcodes erschwert somit ausschließlich eine unabhängige Überprüfung der Funktionsweise eines Wahlcomputers. Die Geheimhaltung des Quellcodes stellt für einen Wahlfälscher keine nennenswerte Hürde dar.

Dieser Nachweis deckt sich mit international gewonnenen Erkenntnissen bei der Analyse von Wahlcomputern anderer Hersteller. Auch dort versuchten die Hersteller erfolglos, unter allen Umständen eine Analyse ihrer Produkte durch die interessierte Öffentlichkeit zu vermeiden.

2.4 Innovation und Erfindungshöhe der Software

Ein wesentliches Ergebnis dieses ersten Analyseschrittes war die Erkenntnis, daß die Software der NEDAP-Wahlcomputer außerordentlich simpel strukturiert ist und ohne besondere Innovationen arbeitet. Im Kern wird eine „elektronische Strichliste“ für jeden erfaßten Tastendruck geführt. Das Argument, der Quellcode könne zum Schutz von Betriebsgeheimnissen nicht offengelegt werden, entbehrt jeglicher sachlicher Grundlage. Die in der Software verwendeten Verfahren und Programmiermethoden sind trivial und lediglich Stand der Technik von Anfang der 90er Jahre.

Jan Groenendaal, der Hersteller der Software der NEDAP-Wahlcomputer, beschreibt die Funktionsweise korrekterweise so: „Die Maschine ist keine Zauberkiste. Die Koordinaten eines Tastendrucks werden in einem Speicher festgelegt [...]. Beim Abschließen werden alle übereinstimmenden Festlegungen 'mit Strichen gezählt'. Das ist alles.“[6]

Aus Sicht eines Programmierers oder Informatikers stellt die softwaretechnische Abbildung eines streng kodifizierten Ablaufes, wie etwa einer Wahlhandlung, ohnehin eine schlichte Aufgabe dar, die ohne Notwendigkeit zur Innovation „herunterprogrammiert“ werden kann. Genau das hat der Hersteller auch getan.

---

[5] Der durch das Dekompilieren gewonnene Quellcode ist unter http://www.wijvertrouwenstemcomputersniet.nl/ES3B_V02_12_disassembly einsehbar.

[6] „Wahlnachrichten“ der HSG Wahlysteme GmbH, Statement von Jan Groenendaal, August 2006. http://www.wahlsysteme.de/Wahlnachrichten/2006_WIRVERTRAUENWAHLMASCHINENNICHT.pdf

Zusammenfassung:
Auch ohne Kenntnis des Quellcodes war es mit überschaubarem Aufwand möglich, die zur Erstellung einer manipulierten Software notwendige Analyse der detaillierten Funktionsweise der NEDAP-Soft- und Hardware durchzuführen. Im Ergebnis der Analyse wurde festgestellt, daß die Software einfacher Natur ist und keine Innovationen enthält, die eine Geheimhaltung des Quellcodes als „Betriebsgeheimnis“ rechtfertigen würden.

2.5 Erstellen eines Testprogramms – NEDAP Schach

Der Hersteller der Software der NEDAP-Wahlcomputer, Jan Groenendaal, hatte in einer Pressepublikation, die auch vom deutschen Importeur HSG auf dessen Webseite verbreitet wurde, folgende Behauptung aufgestellt:

„Den Beweis für die Aussage, daß man mit unserer Wahlmaschine auch Schachspielen kann, würde ich gerne vorgeführt bekommen [...] Unsere Wahlmaschine ist dagegen eine sog. Dedicated Special Purpose Machine, d. h. eine Maschine, die ausschließlich für den Zweck einer Wahl und sonst nichts anderes hergestellt wurde.“[7]

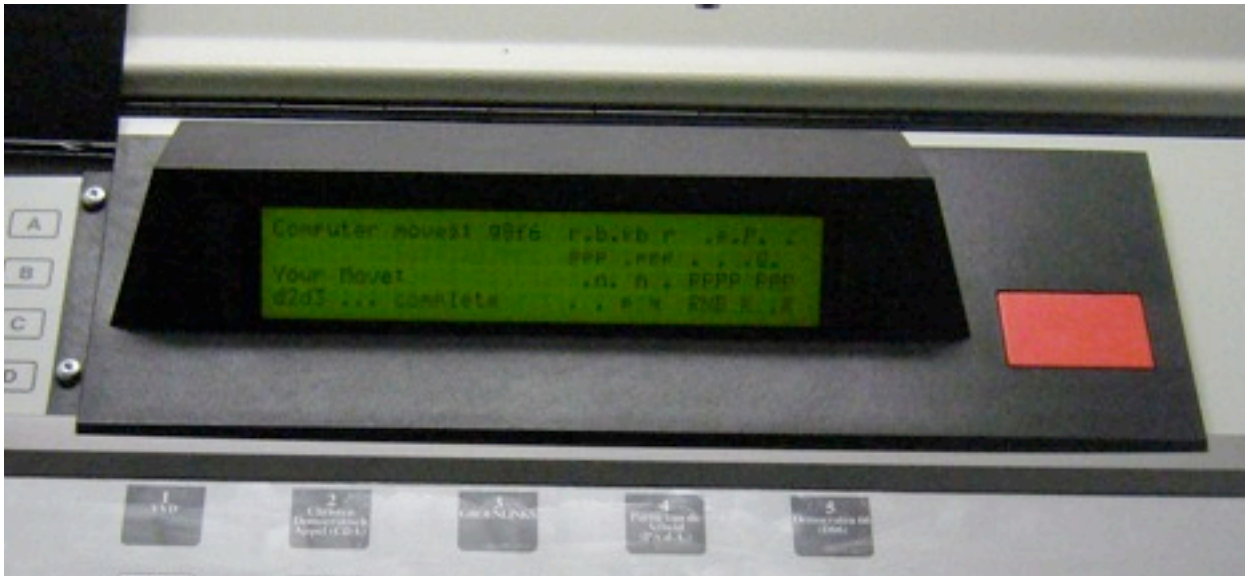
Der Begriff der „Dedicated Special Purpose Machine“ beschreibt einen Mechanismus, der ausschließlich und unabänderbar für einen eng begrenzten Zweck gebaut ist. Jan Groenendaal versucht also hier den Eindruck zu erwecken, NEDAP-Wahlcomputer könnten in keinem Fall andere als die vorgesehenen Funkionen ausführen.

Um die Legende von der „Dedicated Special Purpose Machine“ ein für alle mal auszuräumen sowie zur Validierung unserer Erkenntnisse aus der Analyse des Systems, wurde das Schach-Programm „Tom Kerrigan's Simple Chess Program“ für den NEDAP-Wahlcomputer übersetzt.[8] Aufgrund des relativ knappen Speichers mußte leider die komplexere Endspiel-Bibliothek im Wahlcomputer weggelassen werden. Bis auf diese Einschränkung gelang es, auf dem NEDAP-Wahlcomputer ein voll funktionsfähiges Schachprogramm laufen zu lassen. Um die Bedienung zu erleichtern, wurde auf die eigentlich für die Stimmabgabe verwendeten Tasten ein Schachbrett mit magnetischen Feldern aufgelegt. Die eigenen Spielzüge werden dem Computer durch Niederdrücken der Spielfigur auf dem Schachfeld und dadurch erfolgendes Drücken der darunterliegenden Folientaste mitgeteilt. Die Spielzüge des Computers werden im Display des Wahlcomputers angezeigt.

---

[7] „Wahlnachrichten“ der HSG Wahlysteme GmbH, Statement von Jan Groenendaal, August 2006. http://www.wahlsysteme.de/Wahlnachrichten/2006_WIRVERTRAUENWAHLMASCHINENNICHT.pdf
[8] http://home.comcast.net/~tckerrigan/

NEDAP-Wahlcomputer mit Schachprogramm



Anzeige der Schachzüge im Display

Zusammenfassung:
NEDAP-Wahlcomputer sind frei programmierbare universelle Computer. Die vorgenommene Analyse der Software ist insofern vollständig, als ein vollkommen neues Programm für den Wahlcomputer erstellt werden konnte, das alle Systemfunktionen verwendet. Dies belegt, daß beliebig manipulierte Wahlsoftware einsetzbar ist.

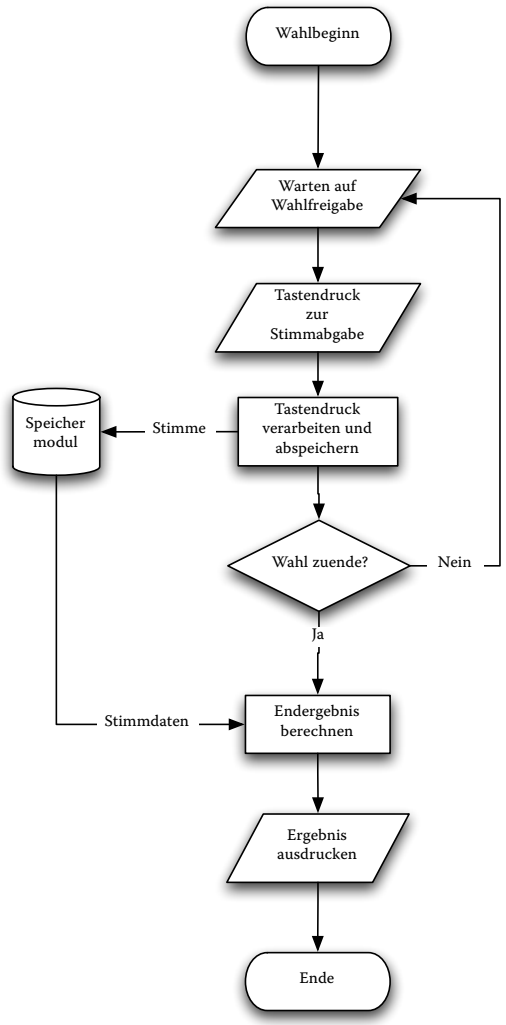
3. Methoden zur Manipulation der Software

3.1 Erstellung einer manipulierten Wahlsoftware

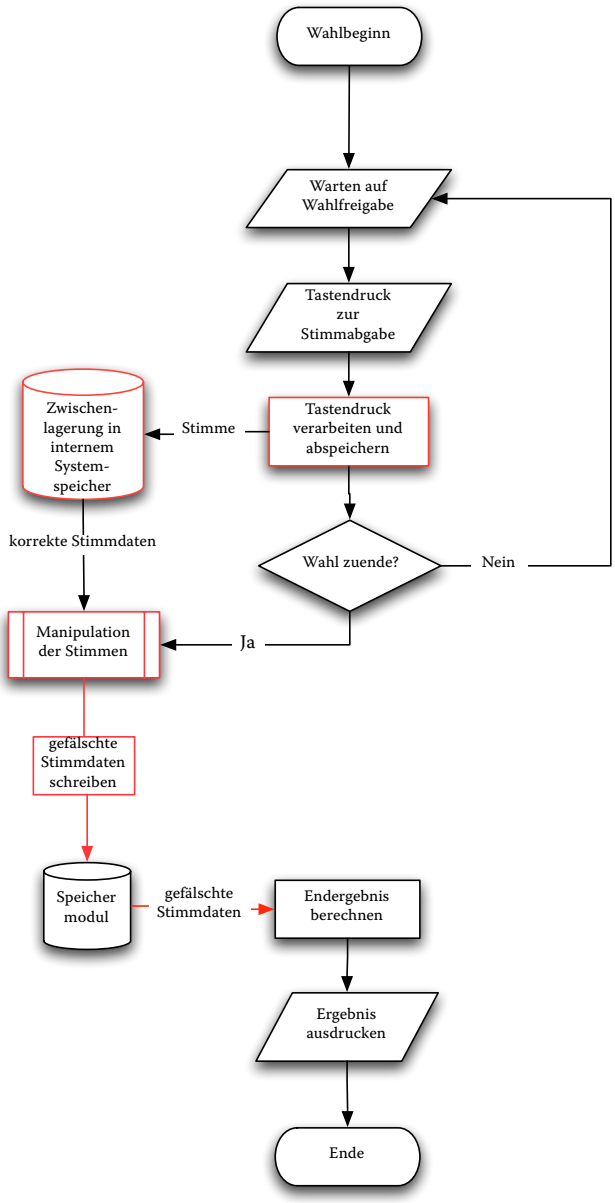
Auf der Basis der durch die Analyse gewonnenen Erkenntnisse wurden in den Programmablauf der Original-Software gesonderte Funktionen eingefügt und vorhandene Funktionen modifiziert. Dazu wurde in der Regel die Struktur der Original-Software nicht wesentlich verändert. Es wurden lediglich an kritischen Stellen (z. B. Auslösen der „Auszählung“, Darstellung der Prüfsumme für die Software etc.) Sprungbefehle zu neu in den Festspeicher programmierten Funktionen eingebaut, welche die Manipulationshandlungen ausführen.[9]

[9] Sprungbefehle bezeichnen Anweisungen in einem Computerprogramm, bei denen der ansonsten lineare Ablauf des Programms (ein Befehl wird nach dem anderen ausgeführt) durch einen Sprung an eine andere Stelle des Programmcodes verändert wird. Sprunganweisungen sind häufig bedingt, d. h. sie werden nur ausgeführt, wenn eine bestimmte Bedingung zutrifft.

Stark vereinfachter Programmablaufplan für NEDAP-Wahlcomputer



Stark vereinfachter Programmablaufplan für manipulierten NEDAP-Wahlcomputer



Unveränderter (links) und manipulierter (rechts) Programmablaufplan, stark vereinfacht und ohne Darstellung der Testwahlerkennung

Mit dieser Methode ist es einfach, die Software des Wahlcomputers derart zu verändern, daß von außen keine Möglichkeit besteht, eine Manipulation zu erkennen. Durch die

Benutzung der in der Original-Software vorhandenen Aus- und Eingabefunktionen reduziert sich der Aufwand zur Erstellung der manipulierten Software auf wenige Tage.

3.2 Funktionsweise der manipulierten Software

Im einfachsten Manipulationsfall wurden in den Teil der Software, der die „Auszählung" der gespeicherten Tastenbetätigungen am Ende der Wahl übernimmt, einige Zusatzfunktionen integriert.

Diese Zusatzfunktionen erhalten als voreingestellten Parameter einen Partei- oder Kandidatennamen, der zu begünstigen ist. Kenntnisse über den Listenplatz der Partei oder des Kandidaten sind dafür nicht notwendig, da diese Information aus der Wahlkonfiguration des Stimmspeichermoduls ausgelesen werden kann. Die Manipulationsfunktion verändert dann die abgegebenen Stimmen entsprechend, bevor sie gespeichert werden. So wird z. B. eine für Partei A abgegebene Stimme so manipuliert, daß sie als Stimme für Partei B auf das Stimmspeichermodul geschrieben wird. Der Wähler erlangt von diesem verdeckten Vorgang keine Kenntnis, für ihn sieht die Anzeige des Wahlcomputers so aus, als wäre seine Stimme für die vom ihm präferierte Partei A gezählt worden.
Da die sonstigen Begleitinformationen nicht verändert werden, ist auch durch eine Analyse des Stimmspeichermoduls bei der Auswertung eine Manipulation in keiner Weise feststellbar.

In einer erweiterten Variante der Manipulation wurden die für die Verfälschung vorgesehenen Stimmen zuerst zwischengespeichert, bis der Wahlvorgang abgeschlossen war. Dadurch kann man die Manipulation so gestalten, daß voreingestellte Prozentwerte für das Endergebnis erreicht werden. Beispielsweise begünstigt die Software eine Partei A derart, daß bereits vor Beginn der Wahl deren prozentuales Wahlergebnis feststeht.
Die Speicherung der „echten" Stimmen in einem internen Speicher des Wahlcomputers ermöglicht es, im Falle einer bloßen Testwahl (siehe nachfolgendes Kapitel) das korrekte Stimmergebnis auf dem Stimmspeichermodul abzulegen und auszudrucken und so eine Entdeckung der Manipulation zu vermeiden.
Sobald eine echte Wahl erfolgt ist, wird das manipulierte Ergebnis auf das Speichermodul geschrieben und auf dem Drucker ausgegeben. Wenn eine Testwahl vermutet wird, werden die tatsächlich gewählten Stimmen unverändert auf das Speichermodul geschrieben und ausgedruckt.

3.3 Erkennen von Testwahlversuchen

Der Hersteller schlägt zur Erhöhung der Sicherheit und zur Funktionsüberprüfung eine Testwahl jeweils vor der eigentlichen Wahl vor. Um das Entdeckungsrisiko für die Manipulation der Software weiter zu verringern, wurde eine Erkennungslogik erstellt, die bestimmte Eingabemuster, wie sie z. B. bei einem Test des Wahlcomputers auftreten würden, erkennen kann. Eine Testwahl wird z. B. durch den Wahlleiter durchgeführt, um die korrekte Ausgabe der gewählten Stimmen vor einer tatsächlichen Wahl zu verifizieren.

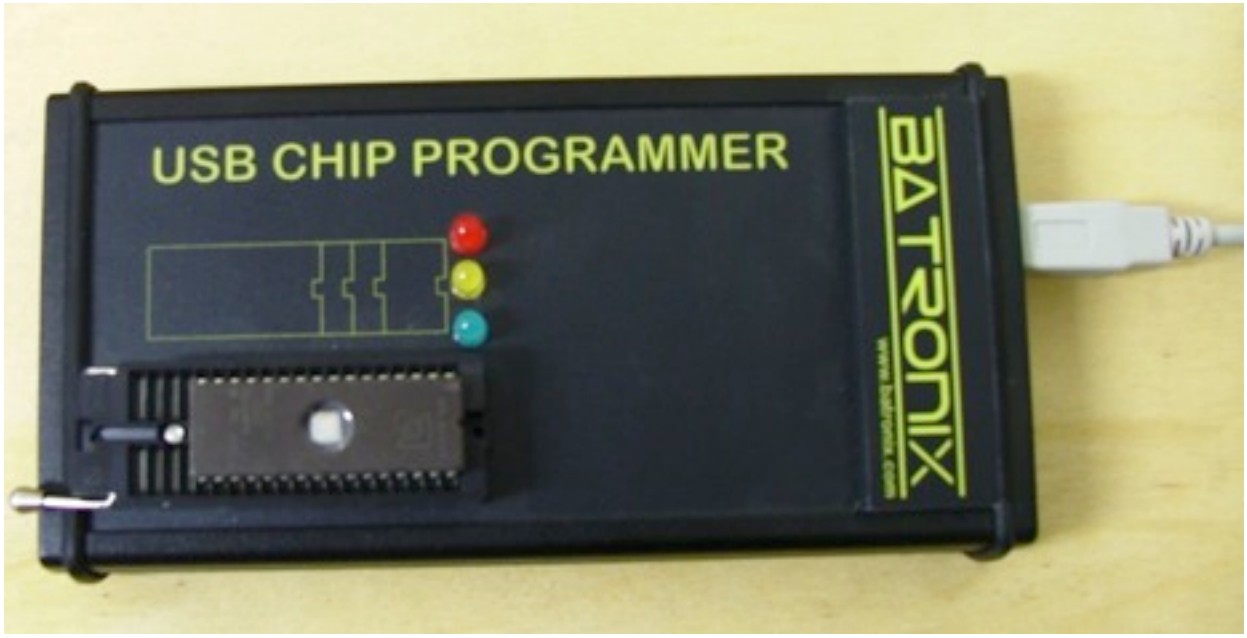
Wenn typische Muster einer Testwahl, wie etwa die Abgabe von vielen Stimmen in kurzer Zeit oder eine Abfolge von Inbetriebnahme, Abschaltung und Wiederinbetriebnahme des Wahlcomputers, erkannt werden, wird die Manipulationsfunktion zum Ende der Wahl nicht ausgeführt. Das korrekte Ergebnis wird ausgegeben und auf dem Speichermodul abgelegt, ohne daß der Prüfer erkennen kann, ob der getestete Wahlcomputer manipuliert ist oder nicht. Diese Methode mit der Erkennungslogik ermöglicht es dem manipulierten Wahlcomputer problemlos, eine Testwahl ohne Entdeckung zu überstehen. Für den Tester des Wahlcomputers verhält sich das Gerät vollkommen normal.

Testwahlen auf einer zufälligen Stichprobe von Wahlcomputern waren vom Hersteller vorgeschlagen worden, um manipulierte Wahlcomputer zu erkennen. Die gezeigte „clevere“ Manipulationssoftware mit Erkennungslogik verdeutlicht, daß eine solche Stichproben-Testwahl relativ simpel umgangen werden kann, ohne daß die Manipulation entdeckt wird. Die von der Manipulationssoftware zu erkennenden Muster, die auf das Stattfinden eines Tests hinweisen, können beliebig an die zu erwartenden Testverfahren angepaßt werden.

Zusammenfassung:
Es gelang mit geringem Aufwand, eine praxistaugliche manipulierte Wahlsoftware zu erstellen, die keinerlei äußere, erkennbare Merkmale der Manipulation aufweist. Die Software ist in der Lage, Testwahlen zu erkennen und hierfür nicht manipulierte Ergebnisse auszugeben, um so eine Entdeckung der Manipulation zu vermeiden.

3.4 Austausch der Software im Wahlcomputer in der Praxis

Ein Austausch bzw. eine Modifikation der Software erlaubt also eine erhebliche, vollkommen verdeckte Änderung der Funktionsweise des Gerätes. Ein konsequenter Schritt für eine Wahlmanipulation ist nun der Austausch der Software in den Wahlcomputern in der Praxis.
Die Software befindet sich in in einem lösch- und neuprogrammierbaren Festspeicher, einem sog. EPROM (Erasable Programmable Read Only Memory). Dieser Speicher kann mittels einfacher, handelsüblicher Werkzeuge aus dem Wahlcomputer entnommen, ausgelesen, gelöscht und neu beschrieben werden.



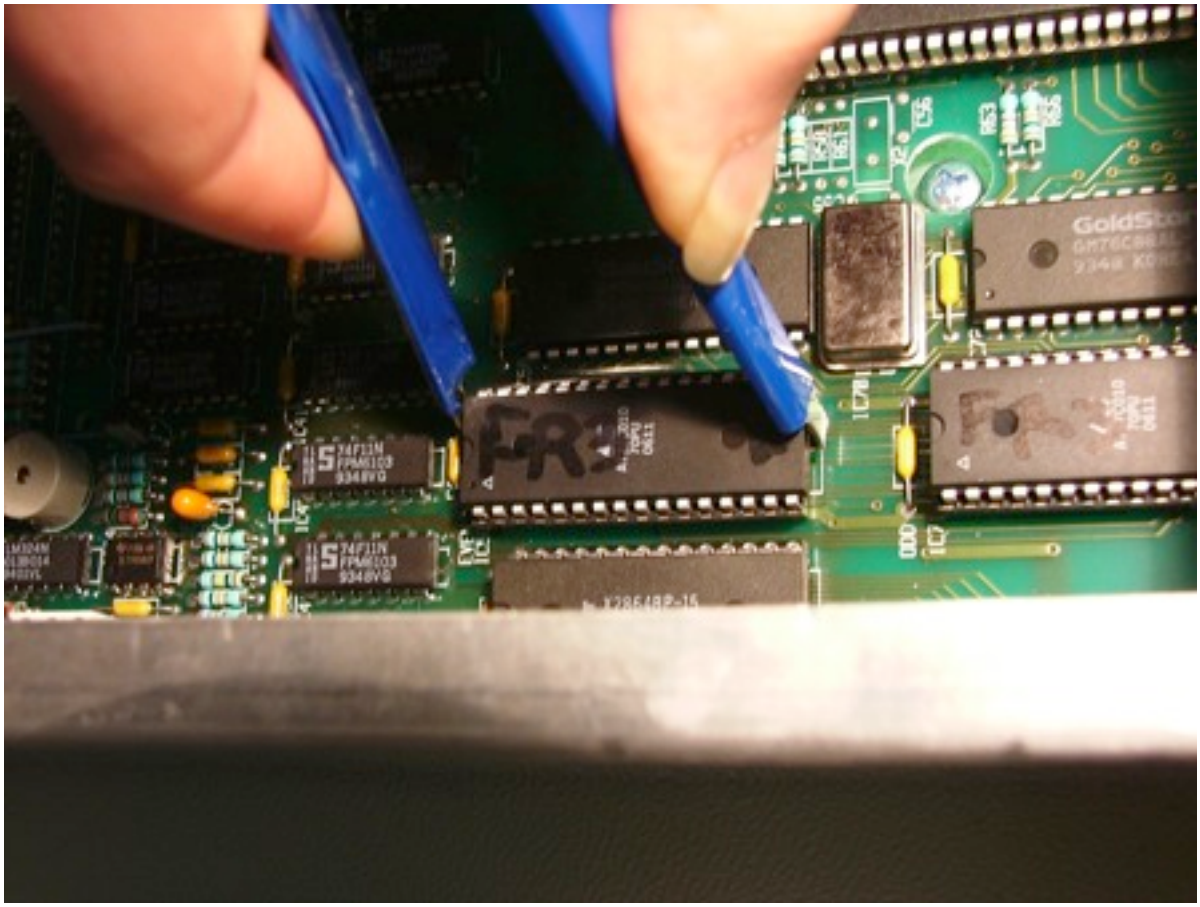
Programmieren der Manipulationssoftware in einen neuen EPROM

In den NEDAP-Wahlcomputern befinden sich zwei EPROMs mit jeweils 128 Kilobyte Speicherkapazität. Bedingt durch die Konstruktion des Computers ist die funktionsbestimmende Software in einer Weise in diesen EPROMs programmiert, bei der die geradzahligen und die ungeradzahligen Speicheradressen in jeweils einem EPROM gespeichert sind. Die EPROMs bilden also zwangsläufig immer ein Paar und müssen gemeinsam behandelt werden.

Original eines NEDAP-EPROMs

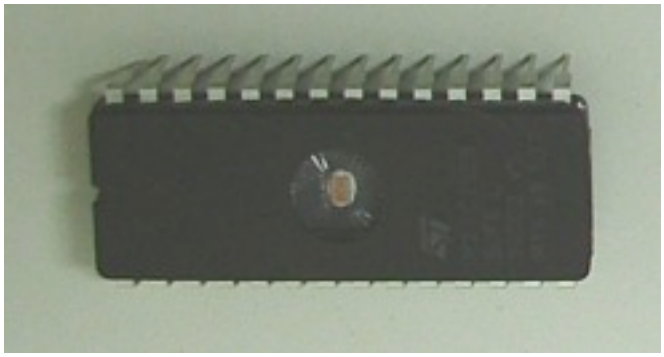
Werkzeuge zum Entnehmen, Auslesen, Löschen und Programmieren von EPROMs wurden für weniger als 500 Euro im normalen Handel erworben. Neue EPROMs wurden für etwa 10 Euro pro Paar bezogen. Der Austausch der Original-EPROMs gegen vorprogrammierte, manipulierte EPROMs erfordert lediglich eine grundlegende Kenntnis des nun öffentlich bekannten mechanischen Aufbaus des Gerätes und ein wenig Fingerspitzengefühl. Auch eine technisch wenig versierte Person kann nach kurzem Training einen

EPROM-Austausch[10] innerhalb von weniger als fünf Minuten durchführen. Geübte Angreifer haben gezeigt, daß der Austausch des EPROMs in etwa einer Minute vollzogen werden kann.



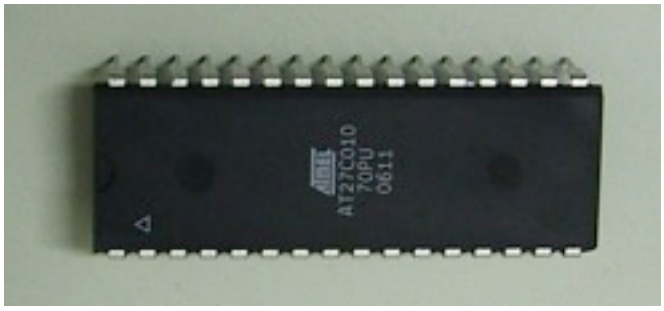
Entnehmen eines Speicherbausteins mit Hilfe eines einfachen Zangenwerkzeugs

[10] Siehe Anlage 2, DVD-Videosequenz Nr. 1, EPROM-Austausch.


EPROM mit manipulierter Software

Für die Programmierung der EPROM-Festspeicher mit einer manipulierten Softwareversion sind keine über das Niveau eines normalen Computerbastlers hinausgehende Fähigkeiten erforderlich.

NEDAP hat in letzter Zeit die Verwendung nur einmal beschreibbarer Speicherbausteine, sog. PROMs (Programmable Read Only Memory), für die Speicherung der Software eingeführt. Damit soll das Überschreiben der Original-Speicherbausteine mit einer manipulierten Software verhindert werden. Ein Angreifer würde jedoch in der Praxis nicht versuchen, die Original-Bausteine zu reprogrammieren. Das Löschen und Neubeschreiben dauert etwa 15 Minuten. Ein direkter Austausch gegen vorbereitete Bausteine mit der manipulierten Software läßt sich demgegenüber in weniger als fünf Minuten durchführen und weist weniger Risiken auf, da nicht mit Computern und Programmiergeräten hantiert werden muß. Die von NEDAP verwendeten PROM-Bausteine sind ebenfalls problemlos wie EPROMs im freien Handel erhältlich und können mit den gleichen Werkzeugen beschrieben werden.

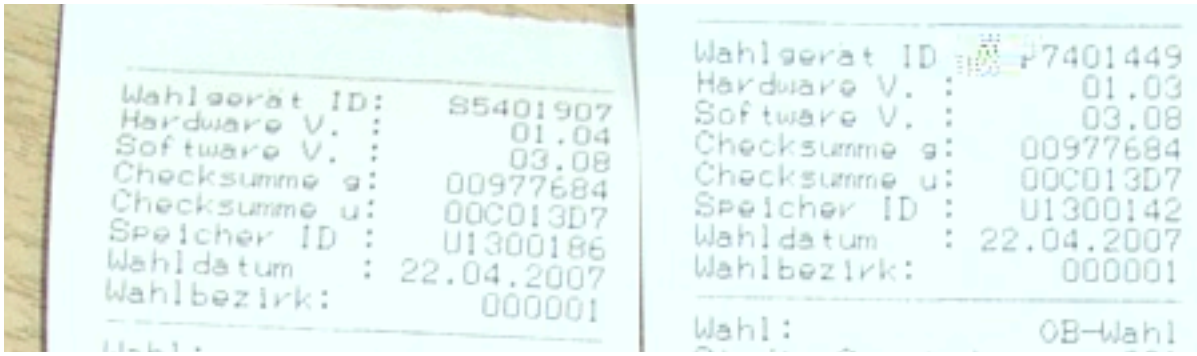


PROM mit manipulierter Software

Anhand dieses Beispiels offenbart sich zum wiederholten Male die Realitätsferne der Sicherheitsmaßnahmen von NEDAP. Es wurde eine „Verbesserung“ eingeführt, die für den technisch wenig versierten Kunden gut klingt, aber keinen effektiven Sicherheitsgewinn gegen reale Angriffsmethoden bringt.

3.5 Prüfsummen

EPROMs weisen gelegentlich Speicherfehler auf, die zu einer Fehlfunktion bei der Ausführung der darauf gespeicherten Software führen können. Die Speicherfehler äußern sich in der Regel als sog. „Kippen“ von einzelnen Speicherstellen, d. h. dort, wo zuvor eine 0 gespeichert war, steht nach dem Fehler eine 1, oder umgekehrt. Diese Fehler entstehen z. B. durch Umwelteinwirkungen oder Materialfehler im Baustein. Um ein Versagen der Software durch solche Fehler zu verhindern, führen die NEDAP-Wahlcomputer bei der Inbetriebnahme eine sog. Prüfsummenberechnung durch. Dabei werden alle Speicherstellen durch einen speziellen Programmteil in einem genormten Verfahren zu einer Prüfsumme zusammengerechnet, die auf dem Bildschirm angezeigt wird. Dem Wahlcomputer liegt nach der „Vorbereitung“ ein Ausdruck bei, auf dem die korrekten Prüfsummen für die entsprechende Softwareversion vermerkt ist. Weiterhin sind die Prüfsummen auf den Wahlergebnis-Ausdrucken verzeichnet.



Prüfsummen auf Wahlergebnis-Ausdrucken, „Checksumme g“ und „Checksumme u“ für beide EPROMs mit den geraden und ungeraden Speicherstellen

Im Wahllokal soll nun der Wahlleiter bei Inbetriebnahme des Gerätes die Prüfsummen auf dem Bildschirm und auf dem Ausdruck vergleichen, um sicherzustellen, daß kein Speicherfehler während Lagerung und Transport aufgetreten ist.[11]
Bei den vom Chaos Computer Club durchgeführten Wahlbeobachtungen u. a. in Cottbus, Zerbst, Zeitz, Roßlau und Neuss wurde aber in keinem einzigen Fall dieser Prüfsummen-Vergleich im Wahllokal durchgeführt. Die Wahlvorstände verließen sich darauf, daß dies bei der Vorbereitung der Wahlcomputer in der zentralen Wahlbehörde geschehen sei. Die dazu befragten Wahlvorstände hatten keinerlei Kenntnis von der Bedeutung der Prüfsumme. Eine Überprüfung fand also in der Praxis nicht statt.

Die PTB hat in der Vergangenheit argumentiert, durch den Vergleich der Prüfsumme könnte eine manipulierte Software in den Wahlcomputern erkannt werden. Dabei blieb unbeachtet, daß die Prüfsumme auch nur durch eine Software berechnet wird, die ebenso austauschbar ist wie der Teil der Software, der die Stimmen zählt. Eine manipulierte

[11] Siehe Anlage 3: NEDAP-Kurzanleitung für den Wahlvorstand, Seite 1.

Software-Version würde also so programmiert werden, daß sie die Prüfsumme nicht berechnet, sondern einfach das „korrekte“ Ergebnis anzeigt, das auf dem mitgelieferten Ausdruck vermerkt ist. Auch diese Manipulation des Programmteils, der die Prüfsumme berechnet, bliebe unbemerkt.

Zusammenfassung:
Die Erstellung einer das Stimmergebnis manipulierenden Software für die NEDAP-Wahlcomputer war ohne jegliche Kenntnis des Quellcodes mit geringem Aufwand möglich. Die Software kann so gestaltet werden, daß eine Erkennung der Manipulation von außen nicht möglich ist. Das Einsetzen der manipulierten Software in den Wahlcomputer kann auch von technisch wenig versierten Personen in wenigen Minuten vorgenommen werden. Die vorhandene Prüfsummenverifikation ist nicht geeignet, eine manipulierte Software auf dem Wahlcomputer zu erkennen. In der Praxis wird die Prüfsumme ohnehin nicht oder nur unzureichend abgeglichen.

3.6 Angriff auf das Integrierte Wahl System (IWS)

Die Konfiguration der Speichermodule vor der Wahl sowie das Auslesen der aus den Wahllokalen eingesammelten Stimmspeicher am Ende der Wahl und die Berechnung des Endergebnisses erfolgen mit Hilfe der von NEDAP und Groenendaal B.V. mit den Wahlcomputern ausgelieferten Software „Integriertes Wahl System“ (IWS). Die IWS-Software war nicht Bestandteil der Prüfung durch die PTB. Das bedeutet, daß diese Software, mit der am Ende der Wahl die Sitzverteilung ermittelt wird, nicht einmal einer einfachen Untersuchung unterzogen wurde. Die Verwendungsgenehmigung für die Wahlcomputer durch das Bundesinnenministerium (BMI) gemäß § 35 Abs. 2 Satz 4 und 5 Bundeswahlgesetz für die Bundestagswahl 2005 führt das IWS lediglich als Initialisierungs-Software mit dem Namen „iws.exe“ auf, obwohl es sich um einen zentralen Bestandteil des Wahlcomputersystems handelt.
Wie der Chaos Computer Club bei den Wahlbeobachtungen vor Ort feststellte, läuft diese Software auf einem normalen PC, der sonst für andere Aufgaben in der Gemeinde verwendet wird.
Angeschlossen ist ein Programmier- und Auslesegerät, bei dem es sich im wesentlichen um die Computerplatine eines NEDAP-Wahlcomputers ohne Tastatur und Display handelt. Das Speichermodul wird in dieses Gerät gesteckt und dort ausgelesen bzw. gelöscht und programmiert.

Ein erfolgreicher Angriff auf die IWS-Software ermöglicht es dem Angreifer, die Wahlkonfiguration auf den Speichermodulen für einen ganzen Wahlbezirk zu manipulieren. Weiterhin kann er die „Auszählung“ und das für die meisten Menschen nicht mehr per Hand nachvollziehbare Berechnen von Sitzverteilungen (Kumulieren, Panaschieren etc.) nach Belieben manipulieren. Theoretisch wäre ein Erkennen einiger, jedoch nicht aller Manipulationsvarianten möglich, wenn die Konfigurations- und Ergebnisausdrucke in den Wahllokalen tatsächlich systematisch mit den Ergebnissen aus den Speichermodulen

verglichen würden. In der Praxis wurde nach unseren Wahlbeobachtungen dieser Vergleich nur sporadisch oder gar nicht vorgenommen.

Da nur eine niederländische IWS-Version für eine Analyse zur Verfügung stand und die zuvor untersuchten Angriffe gegen die NEDAP-Wahlcomputer schon gravierende Manipulationsmöglichkeiten ergeben hatten, wurde auf die Implementierung praktischer Angriffsdemonstrationen gegen das IWS bislang verzichtet. Die grundlegende Struktur der Software wurde jedoch analysiert. Dabei wurden keine nennenswerten Sicherheitsmechanismen gefunden, die eine Manipulation der Software zur Laufzeit verhindern würden. Mechanismen, die einen Austausch der Software auf dem Computer gegen eine manipulierte Version effektiv erkennen oder verhindern könnten, waren ebenfalls nicht vorhanden.

In der Praxis gut vorstellbare Angriffswege gegen die IWS-Software sind der Austausch der Software gegen eine manipulierte Version auf dem Lieferweg (CD-ROM oder Download) oder auf dem Computer vor Ort.

Auf dem Computer kann entweder manuell durch einen Innentäter eine manipulierte Version installiert werden, oder der Computer kann von außen auf „klassischem“ Wege über das Internet angegriffen werden. Bei den vom Chaos Computer Club durchgeführten Wahlbeobachtungen wurde teils durch Befragung, teils durch direkte Beobachtung deutlich, daß die Computer, auf denen das IWS betrieben wird, mit dem Internet verbunden waren. Als Betriebssystem wurde in der Regel Microsoft Windows 2000 verwendet, das unter Sicherheitsgesichtspunkten mittlerweile als vollkommen inakzeptabel angesehen wird. Dieses Betriebssystem weist nur geringen Widerstand gegen lokale oder über das Internet durchgeführte Angriffe auf. Weiterhin wurde beobachtet, daß Wahlergebnisse per unverschlüsselter, nicht elektronisch unterschriebener E-Mail an die Landeswahlbehörden verschickt wurden.

Für die Verwendung von Computern mit sensitiven Daten im Behördenbereich gibt es eindeutige und bewährte Regeln, die im IT-Grundschutzhandbuch des Bundesamt für Sicherheit in der Informationstechnik (BSI)[12] niedergelegt sind. Diese Regeln schreiben Schutzmaßnahmen und Zugangsbeschränkungen für sensitive Computersysteme vor. Angesichts der offenkundigen Unkenntnis der Wahlbehörden auch nur der elementarsten Grundsätze der Computersicherheit wurde hier auf eine systematische Berücksichtigung der Sicherheitskriterien nach dem IT-Grundschutzhandbuch verzichtet.

---

[12] BSI: IT-Grundschutz-Kataloge 2006.
http://www.bsi.bund.de/gshb/deutsch/download/it-grundschutz-kataloge_2006_de.pdf

Zusammenfassung:
Mit einem erfolgreichen Angriff gegen die Programmier- und Auswertesoftware IWS kann das Ergebnis eines ganzen Wahlbezirks oder Wahlkreises mit geringstem Aufwand bei leicht erhöhtem Entdeckungsrisiko manipuliert werden. Die Software läuft in der Regel auf vollkommen ungesicherten, angreifbaren PCs mit Internet-Anbindung und weist keine ernstzunehmenden Sicherheitsfunktionen auf.

4. Möglichkeiten der Hardware-Manipulation

4.1 Austausch von Original-Chips gegen manipulierte Chips

Moderne Microchips sind äußerlich nur durch die aufgedruckte Beschriftung identifizierbar. Das bedeutet in der Praxis, daß ein Angreifer einen oder mehrere der in den NEDAP-Wahlcomputern verbauten Chips gegen manipulierte Chips austauschen kann. Die zentralen Chips im NEDAP-Wahlcomputer sind auf sog. Chipsockeln aufgesteckt. Diese Sockel ermöglichen ein einfaches Entfernen und Austauschen der Chips zu Wartungszwecken. Für den Angreifer ist ein solcher Austausch ebenso leicht möglich.

Hauptprozessor und PROMs auf Chipsockeln

Um einen Chip im Wahlcomputer auszutauschen, würde ein Angreifer einen vorhandenen Chip äußerlich nachahmen, jedoch Zusatzfunktionen zur Manipulation einbauen. Dies geschieht am einfachsten mit Hilfe eines sog. Mikrocontrollers. Bei diesen Mikrocontrollern handelt es sich um sehr kleine Computerprozessoren, wie sie etwa in Mobiltelefonen zum Einsatz kommen. Der Funktionsumfang eines modernen Mobiltelefons, das von so einen Mikrocontroller gesteuert wird, ist um ein Vielfaches umfangreicher als

der eines NEDAP-Wahlcomputers. Diese Mikrocontroller sind mittlerweile so leistungsfähig, daß sie z. B. die Funktion des gesamten Wahlcomputers problemlos steuern und manipulieren können.

Moderne Mikrocontroller sind sehr klein, die im Wahlcomputer verwendeten Chips aufgrund ihres Alters jedoch vergleichsweise sehr groß. Ein Angreifer kann einen solchen von ihm programmierten Mikrocontroller in das Gehäuse eines Originalchips, wie er im Wahlcomputer verbaut wurde, einkleben. Ebenfalls einfach möglich ist eine Nachbildung des Originalgehäuses des zu fälschenden Chips.

Größenvergleich Hauptprozessor des NEDAP-Wahlcomputers mit einem aktuellen Mobiltelefon

Einem Chip, wie z. B. Hauptprozessor oder EPROM im Wahlcomputer, ist von außen nicht anzusehen, welche Funktionen er tatsächlich ausführt. Ein Manipulationschip wird selbst beim elektrischen Test und Auslesen zu Prüfzwecken alle Merkmale eines normalen Hauptprozessors oder eines normalen EPROM mit der korrekten Software aufweisen können. Beim Einsatz im Wahlcomputer wird er jedoch ein beliebig komplexes Manipulationsprogramm ablaufen lassen. Ausgelöst würde die Manipulationsfunktion durch eine spezifische Tastendrucksequenz, die nur dem Wahlfälscher bekannt ist.

Chip in geschlossenem Gehäuse

Chip mit sichtbarem Chipkern

Erst ein Aufschleifen des Chips im Reinraum könnte Hinweise auf einen Austausch geben. Dabei wird der Chip mikrometerweise mit Spezialwerkzeugen Schicht für Schicht abgetragen. Dann wird von jeder Schicht eine Mikroskopaufnahme gefertigt, aus der mit aufwendigen Computerverfahren Rückschlüsse auf die Funktion des Chips gezogen werden können. Der Aufwand für einen einzigen Manipulationsnachweis durch Aufschleifen liegt bei mehreren tausend Euro und kann nur in sehr wenigen spezialisierten Labors durchgeführt werden.

Eine vorgeschlagene Methode, einen Chip-Austausch zu erschweren, ist das Aufbringen von äußerlichen Sicherheitsmerkmalen, wie etwa Hologrammen. Es wird angenommen, daß ein Angreifer Probleme hätte, diese Merkmale nachzuahmen. In der Praxis würde dies jedoch keinen wesentlichen Sicherheitsgewinn bringen. Die seit Jahrzehnten andauernden massiven Probleme der großen Chiphersteller (Intel und AMD) mit gefälschten Hauptprozessor-Chips, bei denen derartige Sicherheitsmerkmale von kommerziellen Fälschern nachgemacht werden, zeigen, daß diese nicht wirklich greifen.

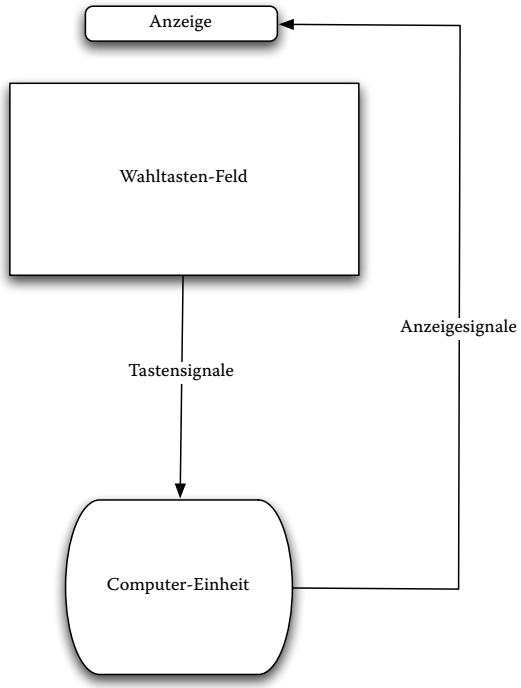
Die technische Machbarkeit dieser Manipulationsmethode wurde geprüft und durchgeplant. Der technische Entwicklungsaufwand für den Angreifer liegt bei etwa 6 Personenmonaten und einigen zehntausend Euro für Material und Miete von Maschinen. Dafür erhält er eine Manipulationsmethode, die de facto keinerlei Entdeckungsrisiko aufweist und problemlos großflächig anzuwenden ist.

Zusammenfassung:
Nach unserem Erkenntnisstand kann der Austausch von Chips gegen manipulierte Chips als Manipulationsverfahren für keine der bisher mit NEDAP-Wahlcomputern durchgeführten Wahlen zweifelsfrei ausgeschlossen werden. Mit keinem der vom Hersteller oder der PTB angewandten oder vorgeschlagenen Prüfverfahren wäre eine solche Manipulation zu erkennen.

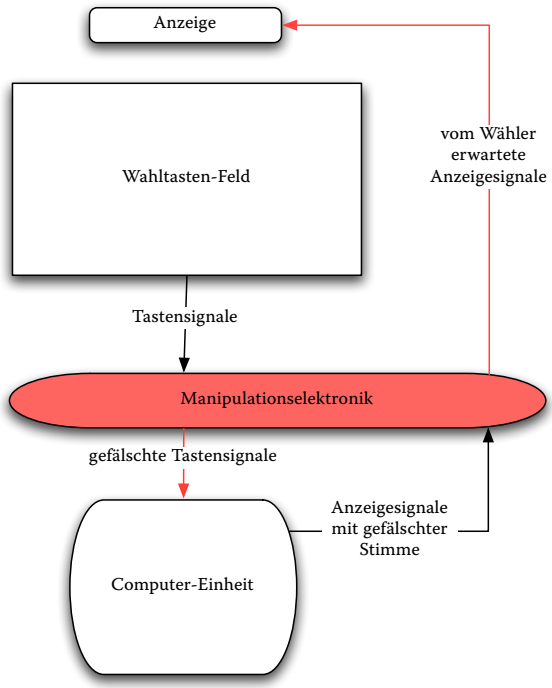
4.2 Manipulation der Ein- und Ausgabegeräte

Eine weitere geprüfte Möglichkeit zur Manipulation, die ohne Austausch der Software des Wahlcomputers auskommt, ist der Einbau einer Zusatzelektronik, die zwischen die Computerplatine des Wahlcomputers und das Tastenfeld und die Anzeige geschaltet wird. Mit einer kleinen Elektronik-Platine, die in den Signalweg zwischen Tastenfeld bzw. Display und eigentlichem Wahlcomputer eingebracht wird, läßt sich ein anderer als der eigentlich vom Wähler vollzogene Tastendruck simulieren. Die Anzeige wird dann entsprechend gesteuert, um dem Wähler ein korrektes Verhalten des Computers zu suggerieren.

Schematischer Aufbau des NEDAP-Wahlcomputers
(stark vereinfacht)



Schematischer Aufbau des NEDAP-Wahlcomputers mit eingefügter Manipulationselektronik
(stark vereinfacht)



Schematische Darstellung der Funktion der eingefügten Manipulationselektronik

Für den Wähler ist der Wahlcomputer eine „Black Box“. Der einzige Anhaltspunkt, den er für eine korrekte oder nicht-korrekte Funktion des Wahlcomputers hat, ist die Anzeige im Display. Eine effektive Kontrolle der korrekten Erfassung seines Wählerwillens ist ihm faktisch nicht möglich.

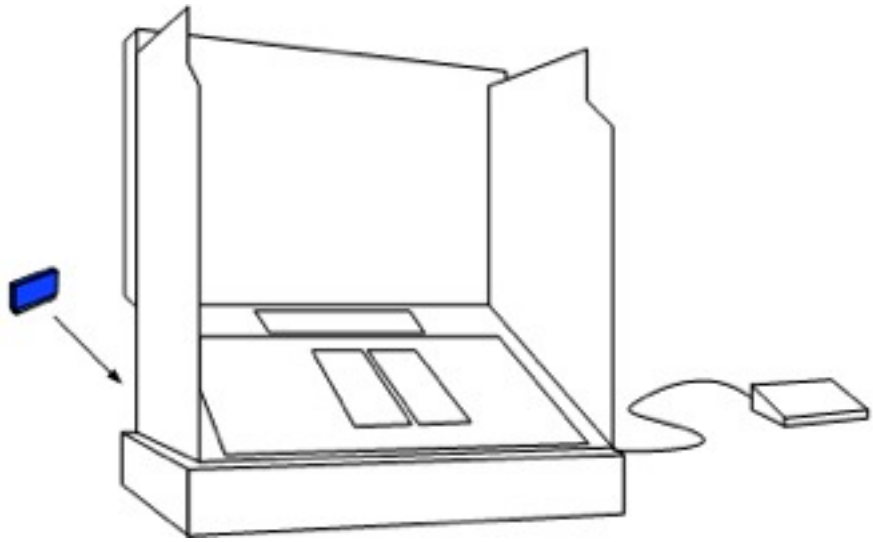
Für einen Innentäter ist der Einbau der beschriebenen Zusatzelektronik, z. B. während der normalen Wartungsprozeduren am Wahlcomputer, möglich. Die Kosten für eine derartige Manipulationselektronik liegen in Kleinserienfertigung bei etwa 50 Euro pro Stück. Der Zeitaufwand für den Einbau hängt vom genauen Ort der Platzierung ab, liegt aber bei sorgfältiger Konstruktion der Platine mit entsprechenden Anschlußbuchsen, Kabelsätzen und Befestigungsmöglichkeiten bei weniger als 30 Minuten. Ein prädestinierter und geeigneter Einbauort befindet sich im Maschinendeckel unter dem Tastenfeld bzw. im Displaygehäuse. Da hier kein regulärer Wartungszugriff geschieht und das unmanipulierte Aussehen der Elektronik den zuständigen Mitarbeitern deshalb nicht bekannt ist, existiert kaum eine Chance für eine visuelle Entdeckung.

Um eine Entdeckung bei etwaigen Funktionsprüfungen oder Testwahlen zu verhindern, wird die Manipulationsfunktion der Zusatzelektronik erst aktiviert, wenn z. B. eine bestimmte Tastensequenz auf dem Tastenfeld getippt wird. Ein Angreifer kann also während einer Wahl durch eine Tastenkombination die Manipulationsfunktion starten. Alternativ ist auch eine Aktivierung der zuvor eingebauten Manipulationselektronik per Funksignal möglich.

Eine Entdeckung derartiger Manipulationen wäre nur durch eine vollständige Demontage jedes einzelnen Gerätes durch sorgfältig geschultes Personal möglich. Dabei gilt es zu berücksichtigen, daß über die Bauzeit der NEDAP-Wahlcomputer auch innerhalb der selben Typenreihe verschiedene Elektronikvarianten verbaut wurden. Dies macht das Training zum Erkennen einer eingebrachten Zusatzplatine nochmals schwieriger. Das Erkennen eines Austausches von Chips gegen manipulierte Chips ist durch visuelle Inspektion nicht möglich.

Zusammenfassung:
Eine Manipulation der Ein- und Ausgabesysteme (Tastenfeld, Display) des Wahlcomputers stellt ebenfalls einen realistischen Angriffsweg dar, der vom Wähler und den an der Wahlvorbereitung und -durchführung beteiligten Personen nicht zu erkennen ist.

4.3 Angriff auf das Stimmspeichermodul



NEDAP-Wahlcomputer und Stimmspeichermodul (blau)

4.3.1 Umprogrammieren des Speichermoduls

Die Zuordnung der Tasten auf dem Wahlcomputer zu Stimmerfassungen für Kandidaten erfolgt mittels Konfigurationseinträgen in dem Speichermodul, in dem während der Wahl auch die Stimmen gespeichert werden. Das Speichermodul wird mit Hilfe der IWS-Software bei der Wahlvorbereitung mit den entsprechenden Einträgen versehen. Das Speichermodul wird dann in den Wahlcomputer eingesteckt und mit Hilfe eines mit dem Verriegelungsschlüssel „A154“ zu betätigenden Schloßschalters verriegelt.

Speichermodul (blau) im deutschen NEDAP-Wahlcomputer

Die Speicherung der Stimmkonfiguration wie auch der Stimmen auf dem Speichermodul erfolgt in einem einfach zu analysierenden Format, das problemlos manipulierbar ist.[13] Die Stimmen werden auf dem Speichermodul in quasi zufälliger Reihenfolge einzeln abgelegt. Zum Schutz vor Speicherausfällen wird jede Stimme dabei mehrfach gespeichert.

Es existieren keine sicheren Schutzmaßnahmen zur Gewährleistung der Nichtmanipulierbarkeit der Stimmkonfiguration oder des Wahlergebnisses auf dem Speichermodul. Ein Wahlfälscher, der Zugang zu dem Speichermodul erlangt, kann mit den entsprechenden technischen Hilfsmitteln also problemlos die Stimmkonfiguration und das Wahlergebnis überschreiben. Die einzige derzeit angewandte Maßnahme zur Erschwerung einer solchen Manipulation ist, daß das Ergebnis der „Auszählung“ mit dem kassenbonartigen Drucker am Ende der Wahl ausgegeben und dieser Ausdruck im Wahllokal zu den Wahlunterlagen gelegt wird.

[13] Beschreibung der Struktur der Daten auf dem Speichermodul, siehe Anlage 5.

Stimmspeichermodul

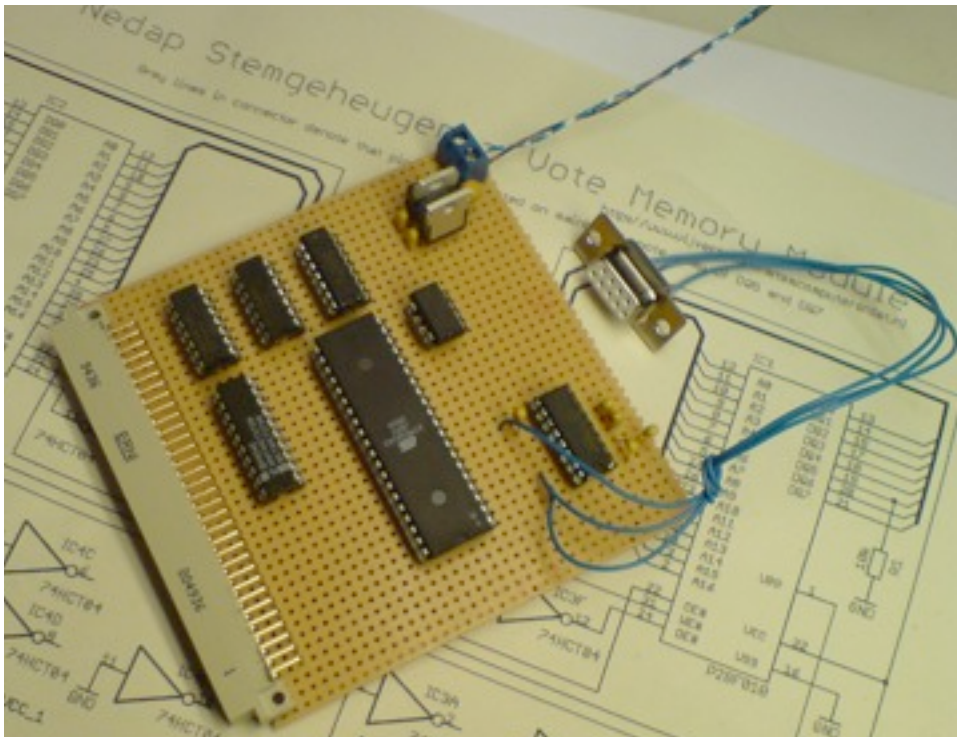
Bei den vom Chaos Computer Club durchgeführten Wahlbeobachtungen wurde uns in der Regel der Zugang zu den Räumen, in denen die Zusammenführung und Errechnung der Wahlergebnisse aus den einzelnen Wahllokalen durch Auslesen der Speichermodule durchgeführt wird, von der jeweiligen Kreiswahlleitung kategorisch verweigert. Die Begründung war stets, daß von einer Beobachtung des Auslesens der Speichermodule „nichts im Wahlgesetz“ stünde.

Nur in einem Fall gelang uns durch freundliches Insistieren die Beobachtung dieses Vorgangs. Dabei wurde festgestellt, daß die Ausdrucke der „Auszählung“ aus den Wahllokalen nicht mit den Ergebnissen vom Auslesen der Speichermodule verglichen wurden. Einzig die aus den Speichermodulen ausgelesenen Ergebnisse wurde verwendet. Zudem wurde festgestellt, daß der Gemeindemitarbeiter allein und unbeobachtet für längere Zeit mit den Speichermodulen im Auswerteraum war, bevor die Beobachtung des Chaos Computer Club zugelassen wurde. Beim Betreten des Auswerteraums wurde dann dokumentiert, daß in der Programmier- und Auswerteeinheit der Schlüssel für den Programmierschacht steckte. Zum Auslesen des Speichermoduls ist die Benutzung des Programmierschachts jedoch nicht erforderlich.

Ausleseeinheit bei einer Wahlbeobachtung, Programmierschlüssel (rot) steckt, obwohl dies zum Auslesen nicht erforderlich sein sollte

Der Chaos Computer Club hat zur Demonstration von Manipulationsmöglichkeiten am Speichermodul ein miniaturisiertes Programmiergerät entwickelt, mit dem der Inhalt des Speichermoduls ausgelesen und verändert werden kann. Das Programmiergerät führt eine vordefinierte Reihe von Manipulationen am Inhalt eines eingesteckten Speichermoduls

durch. Möglich ist z. B. das Verändern der Tastenkonfiguration. Damit wird erreicht, daß eine Taste anders als ihrer Beschriftung am Wahlcomputer entsprechend ausgewertet wird, die Stimmen also für einen anderen Kandidaten gezählt werden. Weiterhin ermöglicht dieses Programmiergerät das Abspeichern eines kompletten Wahlergebnisses auf dem Speichermodul. Mit einem derartigen Gerät kann ein Wahlfälscher an mehreren Stellen der Wahlvorbereitung und Wahldurchführung in einfacher Weise und unbemerkt Manipulationen durchführen.



Vom Chaos Computer Club erstelltes miniaturisiertes Programmiergerät für NEDAP-Speichermodul

4.3.2 Geheime Hintertür zum Konfigurationsmenu

Eine besorgniserregende, jedoch nicht dokumentierte Funktion des Speichermoduls wurde bei der Analyse der Software des niederländischen NEDAP-Wahlcomputers entdeckt und später bei der Analyse der IWS-Software verifiziert. Wenn sich ein Angreifer gegenüber der analysierten IWS-Software mit dem Paßwort „GEHEIM“ identifiziert, kann man u. a. ein Speichermodul erzeugen, das die achtstellige Modul-Identifikation „SERVICE “ hat. Wird solch ein Modul in den NEDAP-Wahlcomputer eingesteckt, wird der Service-Mode aktiviert.

Normalerweise ist dieser Service-Mode nur dann zugänglich, wenn ein spezieller, verborgener Schalter im Inneren der normalerweise mit einem Papieraufkleber versiegelten

Computereinheit umgelegt wird.[14] Mit dem Service-Mode können Teile der Konfiguration des Wahlcomputers geändert und vor allem alle Protokolldateien überschrieben werden.[15] Mit Hilfe eines solchen Service-Moduls kann also ein Angreifer problemlos Spuren von Manipulationen tilgen, sollten diese möglicherweise entstanden sein. Wie in den vorherigen Abschnitten gezeigt wurde, stehen jedoch auch ohne diesen Eingriff hinreichend viele spurenfreie Manipulationsmethoden zur Verfügung.

Mechanismen wie den „GEHEIM/SERVICE "-Zugang bezeichnet man in der Computersicherheitsforschung als „Hintertür". Hintertüren bezeichnen allgemein nicht dokumentierte und nur dem Hersteller bekannte Wege, um Sicherheitsmechanismen zu umgehen. Zugangskontrollmechanismen sind jedoch grundsätzlich nur dann vertrauenswürdig, wenn sie vollständig dokumentiert und universell gültig sind. Die Ausnutzung der gezeigten Hintertür umgeht zudem die Versiegelung der Computereinheit im Wahlcomputer, die durch die Versiegelung vor unbefugtem Zugriff geschützt werden soll. Die Hintertür ermöglicht also den einfachen und ungeschützten Zugang zum Konfigurationsmodus und das Löschen der Protokolldateien.

4.3.3 Hardware-Austausch im Speichermodul

Ein weiterer Weg des Angriffs auf das Speichermodul ist der vollständige Austausch der Hardware im Speichermodul gegen eine andere Platine mit einem Mikrocontroller, der die normale Funktion des Speichermoduls simuliert, aber zusätzliche Manipulationsfunktionen enthält.

Die Elektronik des Speichermoduls ist in eine einfache, zweiteilige Plastikhülle eingebaut, die keinen Einblick ins Innenleben gestattet. Zum Austausch der Elektronik muß ein Angreifer daher nur die Plastikhülle öffnen, seine eigene manipulierte Elektronikplatine einlegen und die Plastikhülle wieder verschließen.
Mit etwas mehr Aufwand kann ein Angreifer auch die Plastikhülle reproduzieren und dann sein gefälschtes Modul statt des Originalmoduls in den Wahlcomputer einstecken. Dazu muß er nicht einmal das Siegel der Computereinheit überwinden, da das Speichermodul einzig durch die Schlüsselverriegelung im Wahlcomputer gesichert wird (siehe nachfolgendes Kapitel). Ein solcher Austausch ist an jedem Punkt der Wahlvorbereitung in einfacher Weise durchführbar und erfordert keinerlei technischen Sachverstand.

---

[14] Siehe Kapitel 5.2 Siegel und Plomben.

[15] In den Protokolldateien werden Ereignisse dokumentiert: Inbetriebnahme, Wahlabschluß, Ausdrucke, Speichermodul voll, Speichermodul nicht lesbar, Speichermodul im Betrieb entfernt, Stimme nicht korrekt gespeichert. Die Protokollierung erfolgt ohne Aufzeichnung einer Uhrzeit, da die NEDAP-Wahlcomputer keine interne batteriegepufferte Uhr enthalten und daher nur die Zeit seit dem Anschalten messen können. Damit sind die Protokolle ohnehin nur von äußerst eingeschränktem Wert für den Nachweis von Manipulationen. Da sie einfach überschrieben werden können, sind sie in der Praxis selbst für eine forensische Analyse wertlos.

Das Entdeckungsrisiko für diese Manipulationsmethode ist äußerst gering, ein Innentäter könnte bei Bedarf sogar nach der Wahl die originalen Speichermodule wieder zurücklegen und so eine nachträgliche forensische Untersuchung von Speichermodulen unwirksam machen.

5. Physische Sicherungsmechanismen

Der physische Schutz der Wahlcomputer vor Manipulationen soll durch verschiedene Vorkehrungen wie Schlüssel, Plomben und Siegel, aber auch Vorschriften zur Handhabung gewährleistet werden.

5.1 Schlüssel

Die Sicherheit der Wahlcomputer gegen unbefugte Bedienung soll durch mechanische Schlüssel verbessert werden. Der Einsatz des Funktions- und Verriegelungsschlüssels, des Schloßverriegelungsschlüssels sowie des Programmierverriegelungsschlüssels ermöglicht die Freigabe des Wahlcomputers, die Entnahme des Stimmspeichermoduls und das Auslesen sowie die Änderung der Konfiguration des Stimmenspeichers. Diese physischen Schlüssel sind in Deutschland, in den Niederlanden und in Irland für alle Wahlcomputer vom gleichen Typ.

Der untersuchte Computer ES3B der Firma NEDAP, der in den Niederlanden eingesetzt wird, verwendet ebenso wie der in Deutschland eingesetzte Computer ESD1 für das Funktions- und Verriegelungsschloß den Typ „C&K YL Series 4 Tumbler Camlock“. Dieses Schloß hat stets die gleichen Schlüssel der Art „A126“.[16] Der Schloßverriegelungsschlüssel hat die Bezeichnung „A154“. Die Qualität beider Schlösser in puncto Sicherheit fällt durch die Schlichtheit der Schließmechanismen in die Kategorie „Briefkasten-Schloß“. Jedoch hat ein Briefkasten-Schloß gegenüber den NEDAP-Wahlcomputern den Vorteil, daß nicht alle Briefkästen mit demselben Schlüssel zu öffnen sind.

Für die deutschen Wahlcomputer des Typs ESD1 werden insgesamt vier verschiedene Schlüssel verwendet. Neben dem schon erwähnten Funktions- und Verriegelungsschlüssel „A126“ und dem Schloßverriegelungsschlüssel „A154“ wird außerdem der Programmierverriegelungsschlüssel „A384“ benutzt. Des weiteren wird der Kofferschlüssel der Art „S0“ verwendet.
Da alle angegebenen Schlüssel unabhängig vom Schloß für einen Preis von etwa einem Euro problemlos erhältlich sind und zudem bei allen Wahlcomputern einer Bauart eingesetzt werden, ist der Zugriff auf das Gerät durch Aufschließen der Schlösser ohne

---

[16] Erhältlich mit der Produktnummer 115140126.
http://www.rsonline.de/elektronische-bauelemente-de/1/775310894-Ersatzschuessel-115140126.html
In der Anlage 6 liegen der Schlüssel „A126“ sowie der Kofferschlüssel „S0“ bei.

weiteres möglich. Keiner der Schlüssel kann als Sicherheitsvorkehrung, welche einen Zugriff auf den Wahlcomputer verhindert, angesehen werden.[17]

5.2 Siegel und Plomben

Anders als der untersuchte niederländische Computer sind einige in Deutschland eingesetzte NEDAP-Wahlcomputer mit Siegeln bestückt, welche einen unbemerkten Zugriff verhindern sollen. Die Vertrauenswürdigkeit eines Wahlcomputers hängt wesentlich davon ab, ob ein solcher unbefugter Zugriff von Innen- und Außentätern wirksam verhindert wird, zumindest aber nicht unbemerkt bleibt.

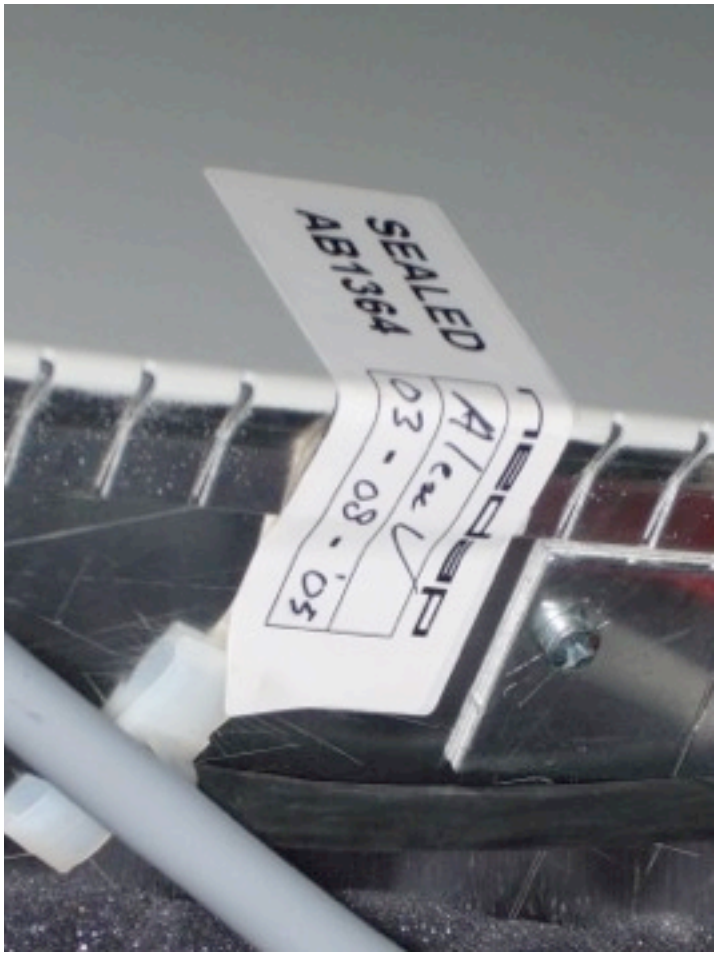
Die Beschaffenheit und Zerstöreigenschaften eines Siegels sollen sicherstellen, daß es nicht unbeschädigt entfernt und nach einer Manipulation wieder aufgeklebt werden kann. Weiterhin sollte ein Siegel fälschungssicher sein sowie Authentizitätsmerkmale aufweisen. Ebenso wichtig wie die physische Sicherheit der Siegel ist in der Praxis auch die Schulung der Anwender, denn ihnen obliegt es, eine Beschädigung oder Manipulation der Siegel aufzudecken und ggf. Maßnahmen zu ergreifen.
Das innere Siegel ist in Deutschland an den Kanten des Deckels des innerhalb des Wahlcomputers befindlichen grauen Metallkastens, der die Elektronik enthält, aufgebracht. Wie auch bei den Schlössern hat sich der Hersteller NEDAP hier für das billigste am Markt verfügbare Fabrikat entschieden.

[17] Sogar HSG bietet die Schlüssel für jedermann zum Kauf an. http://www.wahlsysteme.de/

„Siegel“ am Computermodul eines deutschen NEDAP-Wahlcomputers

Es handelt sich um einen bedruckten Papieraufkleber, der denkbar einfach zu überwinden ist. Nach den Vorgaben des BMI muß sichergestellt werden, daß vor der Inbetriebnahme und regelmäßig vor Benutzung des Wahlcomputers am Wahltag eine Kontrolle der Unversehrtheit und Korrektheit der Siegel erfolgt.
Die überprüfbaren Merkmale des Papieraufklebers sind dessen Seriennummer, seine Positionierung an dem Metallkasten sowie eine Unterschrift. Bei den durchgeführten Wahlbeobachtungen des Chaos Computer Club in Cottbus, Zeitz, Zerbst, Roßlau und

Neuss wurde festgestellt, daß einige der Siegel nicht einmal unterschrieben waren. Weiterhin wurde beobachtet, daß in keinem der Wahllokale ein Vergleich von Positionierung, Seriennummer und Unterschrift des Papieraufklebers mit separaten Kontrollaufzeichnungen durchgeführt wurde. Offensichtlich waren derartige Kontrollaufzeichnungen auch nicht vorhanden, was auf grundlegende Fehlannahmen zum Wirkungsprinzip der Sicherheitsmerkmale von Siegeln hinweist. Die schon an sich unzureichenden überprüfbaren Merkmale wurden also nicht einmal verwendet. Etwaige Beschädigungen des Papieraufklebers hatten somit gar nicht festgestellt werden können. Auch die bei den beobachteten Wahlvorständen vorherrschende vertrauensvolle Grundhaltung gegenüber den Wahlcomputern sorgte bereits dafür, daß eine etwaige offensichtliche Siegelmanipulation nicht aufgefallen wäre.



Detailaufnahme Papieraufkleber

Auf dem Papieraufkleber sind keinerlei Schutzmechanismen aufgebracht, die eine Nachbildung erschweren könnten. Diese Siegel einfacher Art sind leicht zu fälschen und zu ersetzen und stellen keine Manipulationssicherungen dar. Die verwendeten Papieraufkleber

können entweder abgelöst und wiederverwendet oder nach einer Manipulation durch neue, gefälschte Siegel ersetzt werden.

Für die Wähler sind die Papieraufkleber ohnehin nicht sichtbar, da sie hinter der Abdeckklappe auf der Rückseite des Wahlcomputers verborgen sind. Der Wähler hat auch keinen Zugang zu Kontrollaufzeichnungen mit Seriennummern, Positionierung und Unterschriftenproben, anhand derer die Authentizität nachvollzogen werden könnte. Er kann somit nicht prüfen, ob der Papieraufkleber unverletzt und korrekt ist.

Es gibt weiterhin keinerlei Maßnahmen zur Versiegelung der Chips (z. B. der EPROMs) innerhalb der Elektronikeinheit des Wahlcomputers, was einen Austausch zumindest leicht erschweren würde, obwohl dies in der Anlage 1 zu § 2 Bundeswahlgeräteverordnung (BWahlGV) vorgeschrieben ist. Der Deckel mit der Tastatur- und Anzeigeeinheit war ebenfalls in keinem beobachteten Fall versiegelt.

Bei den Oberbürgermeisterwahlen in Cottbus wurden in der Folge der Veröffentlichung der Manipulationsmöglichkeiten an den NEDAP-Geräten durch den Chaos Computer Club die Wahlcomputer vor der Auslieferung in die Wahllokale zusätzlich außen mit Plomben versehen, die einen unbefugten Zugriff verhindern sollten. Bei den Plomben handelte es sich um Billigangebote, wie sie u. a. beim Internetdienstleister „plombe-24.de“ zu beziehen sind. Auch hier wurde nicht einmal die Authentizität der Billigplombe seitens der Wahlvorstände überprüft, wie die Wahlbeobachtungen des Chaos Computer Club offenlegten. Angesichts der sehr einfachen Beschaffenheit wäre eine Fälschung aber auch kaum als solche zu erkennen gewesen.

Selbst die konsequente Verwendung hochwertiger Siegel anstelle der derzeitigen Papieraufkleber und Billigplomben würde keine wesentliche Verbesserung der Situation bringen. Anerkannter Stand der internationalen Sicherheitsforschung ist, daß es praktisch keine Siegel gibt, die nicht von einem motivierten Angreifer innerhalb weniger Minuten mit geringem Aufwand überwunden werden können.
Die umfangreichste Untersuchung zu diesem Thema wurde von der Arbeitsgruppe von Roger G. Johnston in den USA durchgeführt.[18] In einer Studie wurden 244 am Markt verfügbare Siegel für Sicherheitsanwendungen untersucht.[19] Dabei 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 geeignet sind, ein inhärent unsicheres System sicher zu machen. Siegel können nur bei disziplinierter Anwendung mit penibel geführten Kontrollaufzeichnungen

---

[18] Roger G. Johnston: The real deal on seals - Effectiveness of security seals, American Society for Industrial Security, 1997.

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

durch regelmäßig geschulte, aufmerksame Anwender einen Angriff auf ein bereits gut gesichertes System erschweren – mehr aber nicht.

5.3 „Geschützte Umgebungen“

Seitens des BMI wird behauptet, daß eine sichere Verwahrung der Wahlcomputer eine Manipulation wirkungsvoll verhindert. Dabei wird auf § 16 Abs. 2 BWahlGV verwiesen, wonach Wahlvorsteher, Gemeindebehörde und Kreiswahlleiter sicherzustellen haben, daß die Wahlcomputer für Unbefugte nicht zugänglich sind. Die BWahlGV und deren Anhang enthalten jedoch keine eindeutige Verpflichtung zur durchgängig geschützten Aufbewahrung der Wahlcomputer. In der Praxis haben die Wahlbeobachtungen des Chaos Computer Club zudem gezeigt, daß vor Ort keine wirkungsvolle Zugangssicherung besteht.

Mitglied des Chaos Computer Club allein mit unbewachtem deutschen NEDAP-Wahlcomputer während einer Wahlbeobachtung vor Eröffnung des Wahllokals

Der HSG-Geschäftsführer, Herbert Schulze Geiping, der offenbar die Manipulationsmöglichkeiten der NEDAP-Wahlcomputer realistisch einschätzt, räumt ein: „Wenn man sie

[die Wahlcomputer] nun aus dieser geschützten Umgebung herauslöst und versucht sie zu manipulieren, ist die Wahrscheinlichkeit groß, daß dieses gelingen wird."[20] Da diese „geschützten Umgebungen" weder irgendwo genau definiert noch praktisch zu beobachten sind, steht einer Manipulation der Wahlcomputer nichts im Wege. Bei der Bundestagswahl 2005 wurde ein laxer Umgang beim Transport und bei der Aufbewahrung der Wahlcomputer beobachtet. Die heute behaupteten „geschützten Umgebungen" wurden erst nach der Veröffentlichung der Manipulationsmöglichkeiten im Oktober 2006 als Versuch einer Notlösung erfunden, die jedoch in der Praxis wirkungslos bleibt. Das zeigen auch die aktuellen Wahlbeobachtungen des Chaos Computer Club im April und Mai 2007, bei denen beispielsweise nachts offenstehende Fenster am Lagerraum der NEDAP-Wahlcomputer dokumentiert wurden.

Würde man die physischen Sicherungvorkehrungen verbessern und ernstzunehmende Anforderungen an die sog. „geschützten Umgebungen" stellen, ließe sich damit jedoch nur der Zugriff von Außentätern erschweren. Gegen einen Innentäter versprechen diese Maßnahmen ohnehin keinen Erfolg.

Der unbeaufsichtigte Transport der Wahlcomputer stellt ein weiteres Problem dar. Hier ist insbesondere die internationale Ausleihe in die Niederlande gängige Praxis. Für die Stadt Dortmund bestätigte der zuständige Amtsleiter der Stadtverwaltung Ernst-Otto Sommerer diese Ausleihe: Es „bestand ein zusätzlicher, zunächst unbestimmter, Bedarf an Geräten, der in den Niederlanden nicht mehr befriedigt werden konnte. Es wurden nunmehr 290 Geräte an die Firma HSG-Wahlgeräte ausgeliehen."[21] Die Wahlcomputer wurden entsprechend von HSG für die niederländischen Gemeinden umgerüstet und auf die Kommunen verteilt. Nach der niederländischen Wahl wurden die Wahlcomputer dann erneut unter der Regie von HSG für den Einsatz in Deutschland umgerüstet.

Mit dieser Ausleihe und der dabei erfolgten Um- und Neuprogrammierung sind theoretisch noch verbleibende Spuren von eventuellen Softwaremanipulationen bei vorangegangenen Wahlen überschrieben worden. Auch eine forensische Analyse würde hier keine Ergebnisse mehr zeigen.

Ob ein Wahlcomputer während eines Transport unverändert blieb und den gesamten Transportzeitraum über stets bewacht wurde, ist nicht dokumentiert. Die Sicherheit gegen Manipulationen beim Transport ist demnach fragwürdig und widerspricht den angeblichen „geschützten Umgebungen". Die Irische Kommission für elektronische Wahlen hielt bereits 2004 fest: „There is a potential risk to the security of voting equipment (hardware and embedded software) that is unaccompanied and/or unattended while in

---

[20] „Wahlnachrichten", Statement des HSG-Geschäftsführers, Herbert Schulze Geiping, Oktober 2006. http://www.wahlsysteme.de/Wahlnachrichten/2006_Niederlaender_hacken_Wahlgeraet01.pdf

[21] Heise online: Alles legal – Wahleinspruch in Cottbus abgelehnt, 21.11.2006. http://www.heise.de/newsticker/meldung/81327

transit from the Manufacturers by road and sea internationally and also during local delivery to individual Returning Officers."[22]

Zusammenfassung:
Es gibt weder effektive physische Sicherungsmechanismen gegen Innentäter noch hinreichende Vorschriften für eine Sicherung gegen Außentäter. Die Manipulationsfreiheit der NEDAP-Wahlcomputer wird durch die Gesamtheit der physischen Sicherungen nicht gewährleistet.

6. Interpretation der technischen Analyse

6.1 Praxis der Zertifizierung

Die PTB empfiehlt dem BMI die Zulassung oder die Ablehnung der NEDAP-Wahlcomputer. Sie prüft die zur Verfügung gestellten Computer prototypisch durch Hard- und Softwaretests dahingehend, ob sie den vom Gesetzgeber vorgegebenen Kriterien entsprechen. Es handelt sich hier um eine bloße Bauartprüfung. Die IWS-Software wurde dabei nicht geprüft.

Die Richtlinien dieser Tests sind in enger Zusammenarbeit zwischen PTB und dem Hersteller NEDAP im Vorfeld des formellen Prüfauftrages entwickelt worden. Unabhängige Dritte wurden nicht hinzugezogen.

Aus dem PTB-Prüfbericht sind keine Details der durchgeführten Tests ersichtlich. Dieter Richter von der PTB erläutert hierzu: „Prüfberichte sind nicht als Beschreibung angelegt, wie die Prüfung durchgeführt wurde, um sie für Dritte verständlich und nachvollziehbar zu machen, oder daß Außenstehende die Qualität oder den Inhalt der Prüfung bewerten können."[23]
Details und ausführliche Beschreibungen der durchgeführten Prüfungen sind für die Öffentlichkeit nicht einsehbar, das BMI und die PTB halten sie unter Verschluß. Diese Intransparenz ist nicht mit dem Grundsatz der Überprüfbarkeit des Wahlsystems durch den Bürger vereinbar. Selbstverständlich wäre in diesem sensiblen Bereich der Demokratie Transparenz weitaus angemessener.

---

[22] Commission on Electronic Voting: First Report, 2004, Appendix 7a.
http://www.cev.ie/htm/report/first_report.htm
„Es besteht ein potentielles Risiko für die Sicherheit der Wahlcomputer (Hardware und eingebettete Software), wenn sie während des Transports vom Hersteller, international per Straße oder Schiff, unbegleitet und/oder unbewacht sind, und auch, wenn sie lokal an die einzelnen Wahlleiter ausgeliefert werden."

[23] c't - Magazin für Computertechnik, 24/2006, S. 72: Eine neue Situation - E-Voting in Deutschland nach dem Wahlmaschinen-Hack.

6.2 Anforderungen nach BWahlGV

In Anlage 1 zu § 2 BWahlGV wird als Anforderung an ein Wahlgerät u. a. definiert:[24]

Konstruktion
Das Wahlgerät entspricht in seiner Konstruktion dem allgemeinen Stand der Technik und ist unter Beachtung der für Systeme mit schwerwiegenden Schadensfolgen bei Fehlverhalten (hohe Kritikalität) anerkannten Regeln der Technik aufgebaut.
Das Wahlgerät ist so konstruiert, daß eine Veränderung des technischen Aufbaus und bei rechnergesteuerten Geräten auch der installierten Software durch unbefugte Dritte nicht unbemerkt bleibt.

Die durchgeführten Untersuchungen zeigen auf, daß:

1. die NEDAP-Wahlcomputer nicht dem Stand der Technik für Systeme hoher Kritikalität entsprechen,
2. die installierte Software durch Dritte unbemerkt verändert werden kann und
3. der technische Aufbau durch Dritte unbemerkt verändert werden kann.

Die Verwendungsgenehmigung für die NEDAP-Wahlcomputer hätte bereits unter Betrachtung der oben beschriebenen einfachen Angriffe nie erteilt werden dürfen.

Die BWahlGV offenbart hier sehr deutlich, warum Computer als Wahlgeräte grundsätzlich nicht zu sichern sind. Der Computersicherheitsforschung ist bis heute kein System bekannt, mit dem ein unbemerkter Austausch von Software oder Hardware in einem Computersystem, das sich in der Hand eines Angreifers befand, erkannt werden kann, ohne eine individuelle Einzelanalyse mit Mitteln der Computerforensik vorzunehmen.

6.3 Security by Obscurity

Praktisch ist es unmöglich nachzuprüfen, ob ein bei Wahlen eingesetzter Computer mit dem von der PTB zugelassenen Prototypen identisch ist. Es existiert lediglich eine Baugleichheitserklärung des Herstellers NEDAP, eine darüber hinausgehende Prüfung erfolgt nicht.

Wie die meisten Hersteller von Wahlcomputern arbeiten die NEDAP-Geräte nach dem Prinzip *Security By Obscurity*.[25] Dieses Prinzip besagt, daß die Sicherheit eines Systems auf einem Wissensmonopol und dem Verstecken von Informationen basiert und die angewendeten Sicherheitsmaßnahmen nicht öffentlich sind. Für die NEDAP-Wahlcomputer

---

[24] Verordnung über den Einsatz von Wahlgeräten bei Wahlen zum Deutschen Bundestag und der Abgeordneten des Europäischen Parlaments aus der Bundesrepublik Deutschland, Anlage 1 (zu § 2), Richtlinien für die Bauart von Wahlgeräten.

[25] Auch: Security Through Obscurity.

bedeutet dies konkret, daß die technischen Details der Geräte sowie der Quellcode der Software geheimgehalten werden. Ein Anspruch der Öffentlichkeit auf Einblick in diesen Quellcode besteht bisher nicht. Die NEDAP-Wahlcomputer sind also vollständig proprietär und damit nicht sinnvoll überprüfbar.
Das Prinzip *Security By Obscurity* wird in der IT-Branche nicht als ernsthaftes Sicherheitskonzept anerkannt, denn ist ein System tatsächlich sicher, gibt es keinen Grund, Informationen darüber zu verheimlichen.

Für den Bereich der Sicherheit von Computern ist nicht erst seit dem Standardwerk[26] des Computersicherheitsexperten Bruce Schneier klar, daß das Prinzip *Security By Obscurity* nicht funktioniert. Die Sicherheit eines Systems wird vielmehr dadurch bestimmt, welche anerkannten, nachprüfbaren Sicherheitstechnologien angewendet werden. Keinesfalls wird also die Anwendung des erwiesenermaßen unpraktikablen Prinzips *Security By Obscurity* die Sicherheit einer Wahl erhöhen, sondern zusätzlich vermindern, wie in den vorherigen Kapiteln nachgewiesen wurde.

Der PTB-Direktor Dieter Richter räumt ein, daß *Security By Obscurity* kein vertretbares Prinzip und „aus IT-Sicherheitssicht nicht das Idealkonzept ist".[27] Auch die Irische Kommission für Elektronische Wahlen schätzt *Security By Obscurity* als unakzeptables Konzept ein: „This is a mantra for IT security experts. It's a how-not-to-do-it mantra. Security Through Obscurity is the computational equivalent of hiding the key under the mat."[28]

6.4 Betriebsgeheimnisse

Die Baupläne, die Hardware und die Software der untersuchten Wahlcomputer werden von der PTB zu „Betriebsgeheimnissen" der Hersteller NEDAP und Groenendaal B.V. erklärt. Angesichts der in den vorangegangenen Kapiteln dargestellten technischen Schlichtheit der NEDAP-Wahlcomputer ist es fragwürdig, welche Art von „Betriebsgeheimnissen" hier überhaupt geschützt sein mögen. Der Chaos Computer Club konnte an der simplen Hard- und Software der NEDAP-Wahlcomputern kein schützenswertes Geheimnis entdecken.

---

[26] Bruce Schneier: Secrets & Lies. IT-Sicherheit in einer vernetzten Welt, Wiley Computer Publishing, New York, 2001.

[27] c't - Magazin für Computertechnik, 24/2006, S. 72: Eine neue Situation - E-Voting in Deutschland nach dem Wahlmaschinen-Hack.

[28] Charlie Daly, David Gray, Michael Scott, Renaat Verbruggen: Review of Hardware, Software Security and Testing, in: Commission on Electronic Voting, First Report on the Secrecy, Accuracy and Testing of the Chosen Electronic Voting System, Dublin (2004); Appendix 2B, S. 145.
http://www.cev.ie/htm/report/first_report.htm
"Dies ist ein Mantra für IT-Sicherheitsexperten. Es ist ein ‚Wie man es nicht macht'-Mantra. ‚Security Through Obscurity' ist in der realen Welt damit vergleichbar, seinen Haustürschlüssel unter der Fußmatte zu verstecken."

Die Schutz dieser „Betriebsgeheimnisse“ steht in keinem Verhältnis zu dem Schaden, welcher der Demokratie entstehen kann, wenn sie die grundlegenden Prinzipien der Nachvollziehbarkeit und Transparenz von Wahlen aufgibt.

6.5 Praktische Relevanz der Manipulationsmöglichkeiten

In der Computer-Sicherheitsforschung wird in der Regel für eine Sicherheitsbeurteilung ein Angreifer mit bestimmten realistischen Motivationen, Fähigkeiten und Zugangsrechten modelliert, um die tatsächliche Wirksamkeit von Sicherheitsmaßnahmen zu beurteilen. Für die Untersuchung werden schwerpunktmäßig Angriffsmethoden beurteilt, die in der Praxis für einen Angreifer realisierbar sind.
In der Praxis sind die potentiellen Hauptinteressenten an einer Wahlfälschung ein Kandidat oder eine Partei, die zur Wahl stehen bzw. mit ihnen verbundene Interessengruppen.

Die Wahlergebnisse in den letzten Jahren haben oftmals knappe Ausgänge der Wahlen gezeigt. Das bedeutet, daß zum Gewinn der Wahl nur eine kleine Menge gefälschter Stimmen nötig ist. Es ist also wahrscheinlich, daß schon die Manipulation einiger weniger Wahllokale den Ausgang einer Bundestagswahl ändern kann. Je knapper das zu erwartende Ergebnis, desto weniger Wahlcomputer müssen für eine erfolgreiche Wahlfälschung manipuliert werden. Eine geringere Anzahl von manipulierten Geräten 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 offensichtlicher statistischer Abweichungen erkannt werden kann. Die Ergebnisse der Meinungsforschungsinstitute vor großen Wahlen ermöglichen ebenfalls keinen sinnvollen Rückschluß auf eventuelle Manipulationen, da die Abweichung zwischen Umfragewerten und Wahlergebnis in den letzten Jahren durchaus erheblich war.

Wie dargelegt, sind die finanziellen sowie organisatorischen Mittel, die zu einer erfolgreichen Wahlcomputermanipulation nötig sind, nicht sehr umfangreich. Im Vergleich zu den Wahlkampfetats von Parteien sind nur geringe Aufwendungen für eine erfolgreiche Wahlfälschung notwendig.

Für einen motivierten Wahlfälscher ist es ohne Schwierigkeiten möglich, das technische Personal für die Erstellung der Manipulationsmittel (Software oder Hardware) zu finden. Das Manipulationssystem kann so gestaltet werden, daß es auch von technisch nicht versierten Tätern vor Ort angewandt werden kann, ohne Spuren zu hinterlassen.

Zugang zu den Wahlcomputern kann durch Mitglieder und Sympathisanten in den Gemeindeverwaltungen erfolgen, welche die Wahlcomputer für eine Wahl vorbereiten oder sich anderweitig verdeckten Zugang zu den Wahlcomputern verschaffen können. Die mit der Wahlvorbereitung befaßten Mitarbeiter in den Gemeinden unterliegen in der Praxis

keiner besonderen Überwachung oder Kontrolle. Sie haben freien, kaum kontrollierten Zugang zu den Wahlcomputern, wie die Wahlbeobachtungen des Chaos Computer Club zeigten.
Die Einführung von Überprüfungen und Kontrollen des Zugangs durch Mehrpersonen-Regelungen wären in der Praxis nicht hilfreich, da in einer Gruppe handelnde Innentäter weiterhin problemlos arbeiten bzw. die zur Kontrolle abgestellten Mitarbeiter eine technische Manipulation nicht von regulären Wartungsarbeiten unterscheiden können.

Eine weitere mögliche Gruppe von Innentätern bilden alle Personen, die Zugang zu den Lagerräumen erlangen können, in denen die Wahlcomputer verwahrt werden. Wie bei den Wahlbeobachtungen festgestellt wurde, besteht die „geschützte Umgebung", in der laut BMI die Wahlcomputer gelagert werden sollen, in der Regel aus einem einfachen Lagerraum im Rathaus, der mit einem simplen Schließzylinder in Baumarktqualität verschlossen ist. Einen Nachschlüssel für den Lagerraum zu erlangen, stellt für einen motivierten Innentäter kein Problem dar. Die dargestellten Manipulationshandlungen dauern pro Wahlcomputer nur wenige Minuten, d. h. auch ein nicht mit der Wahlvorbereitung befaßter Täter kann realistisch annehmen, ohne großes Entdeckungsrisiko vorgehen zu können.

6.6 Innentäter in der Praxis

Die vom BMI und dem Hersteller immer wieder angenommene Bedrohung durch den einsamen Außentäter, der versucht eine Manipulation durchzuführen, entspricht nicht den tatsächlichen Bedrohungsszenarien. Bisherige aufgedeckte Fälle von Wahlfälschungen sind ausschließlich durch Innentäter durchgeführt worden, die Zugang zu den Wahlmitteln hatten.

Beispielhaft ist hier der Fall der Gemeinde Landerd in den Niederlanden. Dort wurde im März 2006 mit Hilfe von NEDAP-Wahlcomputern gewählt. Dabei kam ein vorherigen Umfragen auffällig widersprechendes Wahlergebnis heraus. Der einzige Begünstigte war Guus te Meerman, der Wahlvorstand in dem betroffenen Wahllokal. Die Manipulation fand durch einfaches Ausnutzen der Unwissenheit der Wähler statt, wie diese später zu Protokoll gaben. Sie wurden offenbar um die Abgabe ihrer Stimme durch „Vergessen" des Hinweises, nach der Auswahl des Kandidaten den Bestätigungsknopf zu drücken, betrogen. Der Wahlfälscher löschte dann die Stimmauswahl und vollzog später Stimmabgaben zu seinen Gunsten, bis die Gesamtzahl der registrierten Wählenden erreicht war. Der vermutliche Täter Guus te Meerman jedoch wurde aus Mangel an Beweisen in erster Instanz freigesprochen, da keinerlei forensische Beweise an den Wahlcomputern mehr zu sichern waren. Die Manipulation der Wahl konnte also technisch nicht mehr nachvollzogen werden, da Wahlcomputer dies nicht erlauben.[29]

---

[29] Bericht zum Fall Guus te Meerman des Ministerie van Justitie Nederlands Forensisch Instituut. http://www.wijvertrouwenstemcomputersniet.nl/images/6/60/NFI_rapport_Te_Meerman.pdf

Die Behauptung, ein Innentäter-Angriffsszenario sei unwahrscheinlich, läßt sich nicht aufrechterhalten. In der Literatur finden sich im Gegenteil keine Hinweise auf Wahlfälschungsversuche, die von Außentätern versucht wurden. Alle bekannt gewordenen Versuche sind von Innentätern mit Zugang zu den Wahlmitteln begangen oder wesentlich unterstützt worden.
Auch in der allgemeinen Kriminalität sind mit einer Wahlfälschung vergleichbare komplexe Betrugshandlungen vorwiegend Innentäterdelikte. Finanzinstitute gehen z. B. aus Erfahrung davon aus, das Betrugsversuche überwiegend von Innentätern begangen werden und richten ihre Sicherheitsprozeduren entsprechend aus.
Wir können daher das Innentäter-Angriffsszenario als die praxisrelevante Bedrohung annehmen, gegen welche die Sicherheitsmaßnahmen eines Wahlsystems wirksam sein müssen.

7. Weitere Manipulationsmöglichkeiten

7.1 Nicht-technische Manipulation

Bei Wahlen im Ausland wurde wiederholt beobachtet, daß per administrativer Entscheidung Wahlcomputer, die gewisse Funktionseinschränkungen aufweisen, bestimmten Wahlbezirken zugewiesen wurden. Typischerweise handelt es sich dabei um Einschränkungen wie geringe Geschwindigkeit der Wahlhandlung, kleine oder schlecht lesbare Kandidatenbeschriftungen, häufigere Ausfälle der Wahlcomputer und ähnliche, die Effektivität der Wahlhandlung beeinträchtigende Probleme. Dadurch wurde die Anzahl der abgegebenen Stimmen in diesen Wahlbezirken gesenkt, was in der Regel zur Benachteiligung der in diesem Bezirk stärkeren Partei führte. Für eine solche Manipulation genügte es, die nachteiligen Eigenschaften bestimmter Wahlcomputer zu erkennen oder subtil zu fördern. Die Manipulation z. B. der Software zu Gunsten einer Partei war nicht dann erforderlich.[30]

7.2 Passive Abstrahlung als neues Risiko

Eine weiteres durchgeführtes Experiment, neben der Erprobung von Manipulationsmöglichkeiten, war die Untersuchung auf elektromagnetische Abstrahlungen, die Rückschlüsse auf die Stimmabgabe zulassen. Anders als bei einem Wahlverfahren mit Papier und Stift entstehen durch die elektromagnetischen Abstrahlungen von Computer neue Risiken für das Wahlgeheimnis des Wählers.

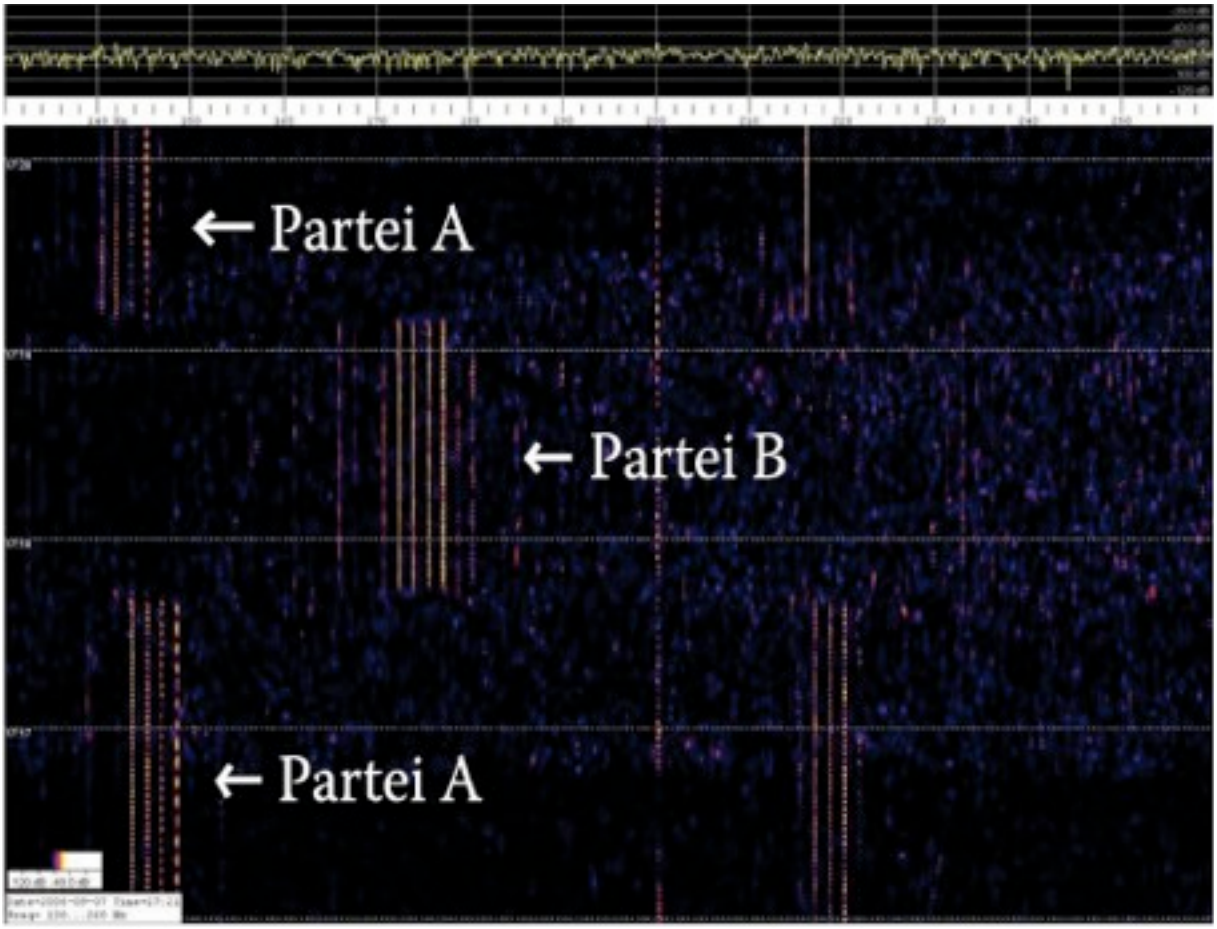
Computer, also auch die NEDAP-Wahlcomputer, arbeiten mit elektrischen Signalen im Hochfrequenzbereich. Diese Signale erzeugen schwache elektromagnetische Abstrahlungen, die mit entsprechenden Empfängern aufgefangen und analysiert werden können.

---

[30] Greg Palast: An Election Spoiled Rotten – A Million Votes In The Electoral Trash Can, 2004. http://www.gregpalast.com/an-election-spoiled-rotten/

Diese Abstrahlungen sind auch unter dem Begriff „Kompromittierende Emissionen“ oder “van Eck Strahlung” bekannt.

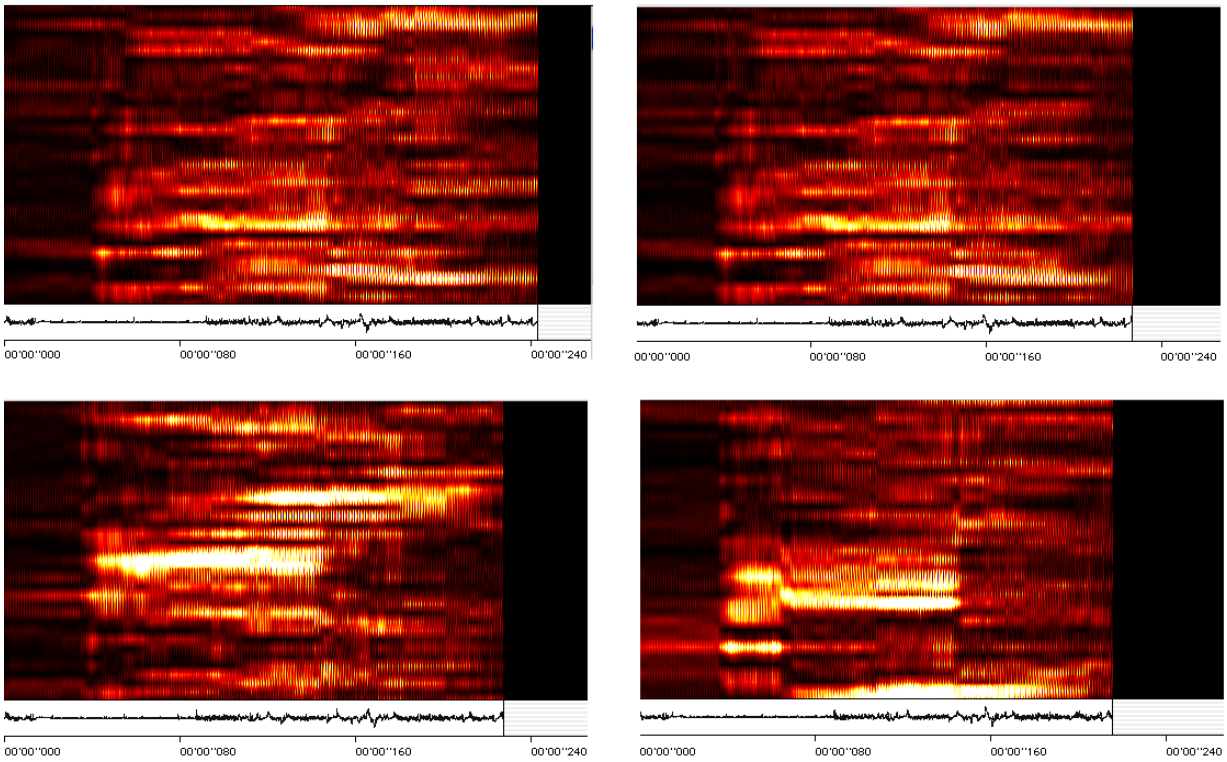
An den zur Untersuchung vorhandenen Wahlcomputern des Typs ES3B, welche nur minimale Bauartabweichungen zu den in Deutschland verwendeten ESD1 und ESD2 aufweisen[31], wurden mit Hilfe von einfachen, handelsüblichen Amateurfunkempfängern Abstrahlungen festgestellt, die Rückschlüsse auf die Stimmabgabe aus einer Entfernung von etwa 25 Metern erlaubten.[32]



Spektrum eines aufgefangenen elektromagnetischen Signals eines NEDAP-Wahlcomputers. Deutlich sichtbar sind die Unterschiede im Signal bei zwei verschiedenen Parteien A und B im Display.

[31] Siehe Anlage 1, Bericht der niederländischen Zertifizierungsbehörde TNO.

[32] Siehe Anlage 4, Bericht des niederländischen Inlandsgeheimdienstes AIVD, welcher die Abstrahlungsmessungen nachvollzogen und bestätigt hat, und Anlage 2, DVD-Videosequenzen Nr. 2 und Nr. 3 zur Verdeutlichung der Auswirkungen der Abstrahlungen in der Praxis.



Wiedererkennen von Anzeigeinhalten. Die beiden Spektren in der oberen Bildhälfte zeigen das Signal für gleiche Anzeigeinhalte, die beiden unteren für verschiedene Anzeigeinhalte. Mittels dieser Technik lassen sich aus der Ferne die von den verschiedenen Anzeigeinhalten (gewählte Kandidaten) verursachten Signalmuster unterscheiden. Bei Anwendung moderner Signalverarbeitungstechniken ist das Verfahren automatisierbar.

Die PTB hat erklärt, daß Abstrahlungen im Rahmen der deutschen Bauartzulassungen erkannt und durch bauliche Maßnahmen unterbunden wurden. Eine unabhängige Verifikation dieser Behauptung war uns nicht möglich, da die Prüfprotokolle mit Hinweis auf das zu schützende „Betriebsgeheimnis“ des Herstellers nicht publiziert sind. In der vom BSI publizierten Liste von abstrahlungsgeprüften Geräten finden sich die NEDAP-Wahlcomputer jedoch nicht.[33]

Das heißt, daß die Prüfung bei der PTB offensichtlich nicht nach den für sensitive Systeme gültigen Richtlinien des BSI erfolgte, sondern nur nach den allgemeinen Standards zur elektromagnetischen Verträglichkeit (EMV) für beispielsweise Haushaltsgeräte u. ä. erfolgte. Der PTB-Direktor Dieter Richter bestätigte diese Vorgehensweise, elektromagnetische Abstrahlungen seien nur „unter der Zielstellung der Konformitätsfeststellung mit

33 Bundesamt für Sicherheit in der Informationsechnik: Technische Leitlinie für staatliche VS zugelassene abstrahlsichere/-arme Hardware, 2005.
http://www.bsi.de/literat/doc/vshardw/TL_03305.pdf

den einschlägigen Normen zur elektromagnetischen Abstrahlung durchgeführt“[34] worden. EMV-Standards gewährleisten, daß Ein- und Abstrahlungen eingeschränkt oder verhindert werden, die z. B. zu einem Fehlverhalten benachbarter Geräte führen könnten. Für die Wahlcomputer sind solche Messungen jedoch nicht aussagekräftig. Um das Wahlgeheimnis gefährdende Abstrahlungen zu entdecken, müßten vielmehr Charakteristiken eines Signals gemessen werden, um Aussagen zur Informationssicherheit machen zu können. Außerdem liegen die Strahlungsintensitäten, die ausreichen, um Informationen über den internen Zustand des Wahlcomputers feststellen zu können, um Größenordnungen unter der definierten EMV-Standardnorm.

Prinzipiell wird bei der Beurteilung der Sicherheit gegen ungewollten Informationsabfluß durch elektromagnetische Abstrahlungen die Entfernung, in der mit üblichen Empfangsgeräten noch ein informationsenthaltenes Signal aufgefangen werden kann, als Bewertungskriterium angenommen. Das BSI verwendet ein Zonenmodell, in dem Geräte mit stärkerer Abstrahlung in den Gebäudekern verlegt werden. Dadurch müssen eventuell kompromittierende Signale durch mehrere Wände bzw. extra installierte Abschirmeinrichtungen gelangen und sollen so weit gedämpft werden, daß eine Auswertung nicht mehr möglich ist. Für Wahllokale, die üblicherweise in Schulen und anderen öffentlichen Einrichtungen angesiedelt sind, ist die Einhaltung des vorgeschriebenen Zonenmodells nicht vorstellbar.

Der Bereich des Schutzes vor kompromittierenden elektromagnetischen Emissionen ist ein hochkomplexes Themengebiet. Bereits geringfügige Änderungen an eigentlich gut gegen das Entweichen von Abstrahlungen geschirmten Geräten können zu einer Vervielfachung des abgestrahlten Signals führen. Ein Beispiel hierfür ist ein nicht vollständig schließendes Abdeckblech eines Wahlcomputers. Manipulationen, die normalerweise nicht als auffällig oder kritisch angesehen würden, können so zu einem Abfluß von Informationen führen, die das Wahlgeheimnis gefährden.

Die Dimension der kompromittierenden Emissionen ist ein weiteres Beispiel für die für den Wähler nicht mehr überschau- und nachprüfbare Komplexität, die mit Wahlcomputern in den Wahlvorgang eingeführt wird. Daß seine Wahlentscheidung möglicherweise drahtlos von einem Lieferwagen auf der Straße vor dem Wahllokal aufgefangen werden kann, ist für den Wähler nicht mal im Ansatz nachvollziehbar. Es stehen ihm auch keine Mittel und Methoden zur Verfügung, um sicherzustellen, daß der von ihm genutzte Wahlcomputer ordnungsgemäß abgeschirmt ist.

Die Weiterentwicklung der verfügbaren Empfangstechnik, die sich in den letzten Jahren dramatisch beschleunigt hat, kann außerdem zu nichh43.22.901Tm 3 Tm (tw) Tj 12 06079 463 Tm (s a

Schirmungen in wenigen Jahren obsolet machen. Es existieren im zivilen Umfeld keine geeigneten Methoden und Prozesse, um eine Weiterentwicklung von Bedrohungen dieser Art zuverlässig zu erkennen und ihnen vorzubeugen.

Bis zur Publikation[35] des Berichts zum ES3B-Wahlcomputer wurde allgemein angenommen, daß die Auswertung von Informationen aus kompromittierenden elektromagnetischen Abstrahlungen nur mit sehr teuren Spezial-Meßgeräten möglich sei. Dabei wurde übersehen, daß handelsübliche Empfängertechnik in den letzten Jahren wesentlich verbessert wurde. Zudem kommen über Gebrauchthändler hochwertige Meßgeräte für wenig Geld auf den Markt, die bis vor kurzem für den privaten Käufer unerschwinglich waren. Dieser Trend wird sich fortsetzen und voraussichtlich noch beschleunigen.

8. Dynamik neuer Angriffsmethoden

Die Einführung von computerisierten Wahlverfahren führt zu einer dynamischen Entwicklung von Angriffs- und Manipulationsmöglichkeiten. Für Wahlen mit Papier und Stift sind mögliche Manipulationsverfahren seit mehr als hundert Jahren bekannt und werden mit sehr einfach zu befolgenden und logisch erschließbaren prozeduralen Methoden verhindert. Die einfache Überprüfbarkeit von Papier-und-Stift-Wahlen durch jeden Wähler bildet einen großen Sicherheitsfaktor, der in der Vergangenheit die Entdeckung von Wahlfälschungen auch unter widrigen Umständen erlaubte.
So entsendet die Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE) international regelmäßig Wahlbeobachter, um eventuelle Unregelmäßigkeiten im Laufe eines Wahlverfahrens feststellen zu können. Eine effektive Kontrolle des Wahlprozesses ist mit dem Einsatz von Wahlcomputern nicht mehr möglich.

Die Entwicklung von Angriffs- und Manipulationsverfahren in der Computertechnik ist ein hochdynamischer Prozeß, bei dem in sehr kurzen Abständen neue Erkenntnisse entstehen. Diese neuen Erkenntnisse machen häufig die vorherigen Annahmen über die notwendigen Sicherheitsmaßnahmen obsolet. Das kontinuierliche Verfolgen der letzten Entwicklungen, das Nachvollziehen der Angriffsmethoden und die Beurteilung der Risikoentwicklung für den spezifischen Anwendungsfall ist nur von Experten zu leisten. Dies erfordert erhebliche Aufwendungen und führt in der Praxis immer nur zu einem beschränkten Erfolg. Die Überprüfbarkeit etwaiger Schutzmaßnahmen durch den Wähler ist nicht zu realisieren.

Im Falle der Wahlcomputer könnte z. B. die Publikation eines neuen Angriffsverfahrens kurz vor einer Bundestagswahl dazu führen, daß kurzfristig eine Umrüstung oder Ausmusterung von Wahlcomputern erforderlich würde, die logistisch in der Kürze der Zeit nicht zu leisten wäre. Eine solche Situation entstand in den Niederlanden bei den letzten

---

[35] Rop Gonggrijp, Willem-Jan Hengeveld: Nedap/Groenendaal ES3B voting computer - A security analysis, 2006. http://www.wijvertrouwenstemcomputersniet.nl/images/9/91/Es3b-en.pdf

Parlamentswahlen. Nachdem die Sicherheitsmängel an den dort verwendeten Wahlcomputern der Firmen NEDAP und SDU bekannt wurden, war die Durchführung der Wahl gefährdet. Durch die praktisch flächendeckende Verwendung von Wahlcomputern in den Niederlanden entstand so die Situation, daß eine Verfassungskrise, bei der das Staatsnotrecht angewandt worden wäre, im Bereich des Möglichen lag. Die niederländische Regierung ließ als Notfallmaßnahme zunächst 100.000 Bleistifte beschaffen. Die NEDAP-Wahlcomputer wurden trotz der bekannten schwerwiegenden Probleme ausdrücklich nur provisorisch wieder zugelassen, um die termingerechte Durchführung der Wahl zu gewährleisten. Die OSZE entschloß sich daraufhin, Wahlbeobachter in die Niederlande zu entsenden. Den Wahlcomputern der Firma SDU, die nur in kleinerer Anzahl im Einsatz waren, wurde die Zulassung entzogen. Die Stadt Amsterdam und mehrere andere Gemeinden wählte daraufhin wieder mit Papier und Stift.

Die deutsche Firma HSG vermarktet die NEDAP-Wahlcomputer in Deutschland. Inhaber der Firma sind Herbert Schulze Geiping und die niederländische Firma Groenendaal B.V. Die Software der NEDAP-Wahlcomputer sowie das IWS zur Berechnung der Wahlergebnisse stellt Groenendaal B.V. her. Sie ist ebenfalls für die Wartung der Software zuständig.

In den Niederlanden entstand erst aufgrund dieser Monopolstellung des Wahlcomputer-Software-Herstellers kurz vor der Wahl die prekäre Situation, 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. Der niederländische Staat macht das Funktionieren seiner Demokratie mithin von einem kleinen Unternehmen und dessen Besitzer abhängig, ohne dessen Aktivität und Bereitschaft er keine Wahlen durchführen kann.[36] Auch Deutschland begibt sich in eine ähnliche Abhängigkeit, sobald in immer mehr Wahlkreisen NEDAP-Wahlcomputer eingesetzt werden.

Die nach Bekanntwerden der Manipulationsmöglichkeiten an den NEDAP-Wahlcomputern in den Niederlanden von der Regierung eingesetzte unabhängige Kommission „Commissie Besluitvorming Stemmachines“ hat im April 2007 ihren ersten Bericht vorgelegt. Darin wird die Entstehung der Abhängigkeit der Wahldurchführung von der Kooperation des Software-Herstellers Groenendaal dokumentiert und kritisiert.[37]

Die von der PTB für die Bauartzulassung der NEDAP-Wahlcomputer durchgeführten Prüfungen sind im Lichte der hier dargelegten Untersuchungen ein repräsentatives

---

[36] Hervorgegangen aus amtlichen Dokumenten, die durch das niederländische Informationsfreiheitsgesetz erlangt wurden. http://www.wijvertrouwenstemcomputersniet.nl/English/Groenendaal

[37] Commissie Besluitvorming Stemmachines: Stemmachines, een verweesd dossier, April 2007. http://www.minbzk.nl/aspx/download.aspx?file=/contents/pages/86914/rapportstemmachineseenverweesddossier.pdf

Beispiel dafür, wie schnell Sicherheitsannahmen von der Realität möglicher Angriffe überholt werden, ohne daß eine adäquate, schnelle Reaktion erfolgen kann.

Die grundlegende Dynamik der Angriffsentwicklung ist einer der wesentlichen Risikofaktoren computergestützter Wahlverfahren. Im Gegensatz zum altbewährten Verfahren können jederzeit bislang unbekannte, nicht absehbare Angriffsmethoden entwickelt werden, die unerkannt bleiben und eine Wahlfälschung ermöglichen. Selbst ein sehr gründlicher Zertifizierungsprozeß ermöglicht es nicht, diesen Risikofaktor zu eliminieren, und ersetzt nicht die Überprüfbarkeit durch den Wähler.

9. Verifizierbarkeit der Wahl durch den Wähler

Das Bedürfnis, Wahlcomputer einzusetzen, resultiert im Kern aus dem Wunsch der Gemeinden nach einem schnellen Ergebnis bei Verringerung des Aufwands für die Durchführung der Wahl. Um diese Ziele mit den Grundanforderungen einer demokratischen Wahl zu vereinbaren, ist es notwendig, daß das Wahlverfahren vom Wähler im Wahllokal ohne technische Kenntnisse überprüfbar ist. Jede durch Technologieeinsatz erzeugte Notwendigkeit zur Delegierung der tatsächlichen Überprüfbarkeit bedeutet unausweichlich, daß Möglichkeiten zur nicht mehr nachweisbaren Manipulation entstehen. Im vorliegenden Fall der NEDAP-Wahlcomputer ist dies nachvollziehbar belegt.

Aus Sicht der Sicherheitsanalyse erscheint es als der einzig sinnvolle Weg, daß eine Stimme auf Papier als endgültiger Ausdruck des Wählerwillens definiert wird, deren Nachzählung jederzeit von jedem verlangt werden kann. Elektronische Wahlmittel sind als Hilfsmittel zur Erzielung eines schnellen vorläufigen Ergebnisses nur dann vertretbar, wenn zweifelsfrei geregelt ist, daß das Computer-Ergebnis nur vorläufiger Natur ist und bei jeder Art von Zweifeln der Wähler eine Auszählung des Papierergebnisses verlangen kann, welches dann endgültig ist.

Im Gegensatz zum bewährten Wahlverfahren mit Papier und Stift ist eine computergestützte Wahl nicht mehr vom Wähler nachvollziehbar und überprüfbar. Durch die vom BMI praktizierte Delegierung der Überprüfung an eine Behörde, wird dem Wähler das Recht genommen, sich von der Korrektheit der Wahl zu überzeugen. Er soll genau denjenigen sein Vertrauen schenken, die am ehesten als Innentäter in Betracht kommen.

Das BMI vertritt die Position, daß – wie in so vielen Bereichen der Gesellschaft – der Bürger seine Überprüfungsmöglichkeiten an Experten und Behörden abtreten soll. Dies erscheint angesichts der grundsätzlichen Bedeutung von Wahlen für die Demokratie unangemessen und höchst problematisch. Die für die Einführung von Wahlcomputern vorgelegten Gründe haben nicht einmal im Ansatz das gleiche Gewicht wie das Recht auf transparente und verifizierbare Wahlen. Die Idee von Wahlcomputern ist typisch für eine „Schönwetter-Demokratie“, die sich der Illusion hingibt, niemals einen extremistischen Gegner abwehren zu müssen, der sich ihrer Institutionen bedient und den Wählerwillen

verfälscht. Ein Wahlverfahren muß aber so beschaffen sein, daß es unter allen, also auch unter widrigen Umständen funktioniert und überprüfbar bleibt.
Selbst unter den Bedingungen der DDR war der inoffizielle Nachweis der Wahlfälschung durch Beobachtung der Auszählung in den Wahllokalen, Zusammentragen der Ergebnisse aus den einzelnen Wahllokalen und Vergleich mit den offiziellen Zahlen möglich. Mutige Bürger haben so versucht, den systematischen Wahlbetrug in der DDR aufzudecken. Mit Wahlcomputern wäre dies nicht möglich gewesen, die Ergebnisse hätten bereits unsichtbar in den Computern manipuliert werden können.

Das Interesse totalitärer Staaten an Wahlcomputern ist ein Hinweis auf die zahlreichen und problemlosen Manipulationsmöglichkeiten. Die für Wahlen und Wahlbeobachtung zuständige Arbeitsgruppe ODIHR der OSZE fordert deshalb, keine Wahlcomputer ohne vom Wähler überprüfbares Papierergebnis mehr zu verwenden.[38] Deutschland hat eine Vorbildrolle für viele junge Demokratien und für die demokratische Opposition in totalitären Staaten, daher sollte es nachvollziehbare, transparente Standards für seine Wahlen haben.

10. Internationale Situation

Direct Recording Electronic (DRE) bezeichnet eine Klasse von Wahlcomputern, zur der auch die NEDAP-Wahlcomputer zählen, die eine ausschließlich elektronische Zählung der Stimmen der Wähler ohne Wahlbelege auf Papier kennzeichnet. Eine sinnvolle Möglichkeit für eine Beobachtung der Auszählung der Stimmen bzw. eine unabhängige Nachzählung der Stimmen ist demnach nicht vorgesehen. DRE-Wahlcomputer erfüllen somit nicht die von der OSZE geforderten Kriterien[39] der Transparenz und Nachprüfbarkeit von Wahlen.

Die in den letzten Monaten erschienenen Berichte nationaler und internationaler Institutionen haben hinsichtlich DRE-Wahlcomputer klare Empfehlungen gegeben. Der OSZE-Report des Büros für demokratische Institutionen und Menschenrechte (ODIHR) hält fest: „Software dependent vote recording mechanisms which do not permit an independent check on their operation should be phased out."[40]

Auch der EU-Rat findet in seinen Empfehlungen zu elektronischen Wahlen klare Worte: „Bearing in mind that the right to vote is one of the primary foundations of democracy, and that, consequently, e-voting system procedures shall comply with the principles of democratic elections and referendums; [...] that only those e-voting systems which are

---

[38] Office for Democratic Institutions and Human Rights: Election Assessment Mission Report (2007), S. 16.
[39] OSZE/ODIHR: The ODIHR Election Observation Handbook, 1999, Warschau, S. 3.
[40] Office for Democratic Institutions and Human Rights: Election Assessment Mission Report (2007), S. 16. „Software-abhängige Mechanismen zur Aufzeichnung der Stimmen, die keine unabhängige Kontrolle ihrer Funktionsweise erlauben, sollten aus dem Verkehr gezogen werden."

secure, reliable, efficient, technically robust, open to independent verification and easily accessible to voters will build the public confidence which is a pre-requisite for holding e-voting."[41]

[41] Council Of Europe: Recommendation Rec(2004)11 and Explanatory Memorandum of the Committee of Ministers to Member States on Legal, Operational and Technical Standards for E-Voting, Straßburg 2004. „Berücksichtigend, daß das Recht zu Wählen eines der elementaren Fundamente der Demokratie ist, und infolgedessen die Prozeduren der elektronischen Wahlsysteme den Prinzipien demokratischer Wahlen und Referenden entsprechen sollten; [...] nur solche elektronischen Wahlsysteme, die sicher, zuverlässig, leistungsfähig, technisch robust, offen für eine unabhängige Verifikation und einfach zugänglich sind, werden das öffentliche Vertrauen aufbauen, welches eine Voraussetzung für die Durchführung elektronischer Wahlen ist."

11. Fazit

Die Analyse der NEDAP-Wahlcomputer hat zu einer Widerlegung der Behauptungen des Herstellers, des BMI und der PTB über die Sicherheit des Systems geführt. Im Rahmen der Untersuchungen wurden mehrere sehr unterschiedliche Angriffsklassen gefunden und implementiert, die jede für sich genommen schon zur Rücknahme der Bauartzulassung hätte führen müssen. Die Untersuchung hat gezeigt, daß:

- die Software der Wahlcomputer problemlos manipulierbar ist,
- Manipulationen an der Hardware einfach möglich sind,
- die Programmier- und Auswertesoftware in einfacher Weise angreifbar ist,
- die Zulassungs- und Prüfverfahren ungeeignet sind, Manipulationen aufzudecken,
- die Annahmen des BMI und der PTB über mögliche Wahlfälscher unrealistisch sind,
- die aus diesen Annahmen resultierenden Anforderungen und Maßnahmen („geschützte Umgebungen“) unwirksam sind,
- Versiegelungen und Plomben keinen wirksamen Schutz bieten,
- dem Wähler eine effektive Kontrolle und Verifikation der Wahl nicht mehr möglich ist,
- neue Risiken und Angriffsmethoden fortlaufend entstehen,
- im internationalen Vergleich eher die Abschaffung als die Einführung von Wahlcomputern als sinnvoll erachtet wird und
- eine Manipulation der Wahlcomputer zur Bundestagswahl 2005 nicht mit Sicherheit ausgeschlossen werden kann.

Die Untersuchung zeigt exemplarisch die prinzipiellen Schwierigkeiten bei der Verwendung von Wahlcomputern, unabhängig von der Bauart. Keines der Probleme ist auf technischem Wege mit ausreichender Zuverlässigkeit lösbar, da mehr technische Sicherheitsmaßnahmen zwangsläufig zu komplexeren Systemen führen, die von noch weniger Menschen verifiziert werden können. Wenn der geringe Nutzen und die erheblichen Risiken objektiv gegenübergestellt werden, erscheint es sinnvoll, von der Nutzung von Wahlcomputern zukünftig abzusehen und beim nachvollziehbaren und bewährten Wahlverfahren mit Papier und Stift zu bleiben.

Mitarbeit an diesem Bericht:

Ingo Albrecht, Andreas Bogk, Wolfgang Coy, Dirk Engling, Verena Hafner, Willem-Jan Hengeveld, Jan Krissler, Stephanie Lange, Felix Lindner, Pavel Mayer, Hannes Mehnert, Sam Nemeth, Henryk Plötz, Tim Pritlove, Frank Rosengart, Pascal Scheffers, Lisa Thalheim, Barry Wels, Harald Welte und Maurice Wessling.