Gonggrijp et al. („NEDAP-Hack“)

Im Oktober 2006 hat die niederländische Stiftung „Wij Vertrouwen Stemcomputers Niet“ eine unabhängige Analyse der niederländischen Wahlgeräte ES3B vorgelegt.

Anlage B 19

Die niederländischen Geräte ES3B entsprechen technisch weitgehend den in Deutschland eingesetzten Geräten des Typs ESD1. Im Rahmen ihrer Untersuchung haben *Gronggrijp et al* eine detaillierte Analyse der Hard- und Software der Wahlcomputer durchgeführt. Außerdem haben Sie eine manipulierte Gerätesoftware erstellt, die einer zuvor bestimmten Partei Stimmen zuordnen, die eigentlich für eine andere Partei abgegeben worden sind.

Die Untersuchung wurde ohne Wissen und Einverständnis des Herstellers und ohne Einblick in die technische Dokumentation durchgeführt. Auch der Quellcode der Gerätesoftware stand den Autoren nicht zur Verfügung. Für Ihre Untersuchung benötigte die Gruppe nach eigenen Angaben einen Zeitraum von einem Monat. Zuvor hatte die Initiative mehrere gebrauchte Geräte legal von niederländischen Gemeinden erworben.

Der für Wahlgeräte zuständige Abteilungsdirektor der Physikalisch-Technischen Bundesanstalt, Prof. Richter, bewertet die Bedeutung der Ergebnisse von *Gonggrijp et al.* gegenüber dem Computermagazin c't (Heft 24/2006, S. 72, **Anlage B 4**):

„Wir haben deren Vorgehen inzwischen so weit nachvollzogen, dass wir davon ausgehen, dass das System ohne Kenntnis des Quellcodes analysiert und die entsprechenden Eingriffe gemacht wurden. Auch wenn für das Hacken der in Deutschland verwendeten Software … wohl noch einmal etwas Zeit aufzuwenden wäre, sind das neue Fakten. Der Schritt von

einer theoretischen Option zur Realisierung wird zu einer neuen Bewertung führen.“

1. Nedap-Schach

Bei den Nedap-Geräten handelt es sich um gewöhnliche (wenn auch technisch betagte) Computer, die jedes beliebige Programm ausführen, das auf den beiden Programmspeichern (EPROMs) im inneren der Geräte installiert ist. Die beiden Speichermodule sind gesockelt, sie lassen sich innerhalb kürzester Zeit gegen solche mit einer anderen Software austauschen. Der Grund für die Austauschbarkeit der Gerätesoftware liegt in der Notwendigkeit, im Rahmen der Wartung der Computer neue Software-Versionen einspielen zu können. Dies ermöglicht das Beheben von Programmierfehlern, die Erweiterung der Funktionalität sowie die Reaktion auf Wahlrechtsänderungen.

Für einen Austausch der Software ist das Öffnen der Geräteelektronik mithilfe eines Schraubendrehers erforderlich, ein entsprechender Eingriff dauert etwa zwei Minuten. Er kann deshalb nicht unbemerkt während einer öffentlichen Wahl erfolgen, wohl aber zu jedem beliebigen Zeitpunkt vor der Wahl.

Der Hersteller hatte noch im Sommer 2006 behauptet, es handele sich bei den Geräten nicht um Computer, sondern um speziell für Wahlen ausgelegte Geräte, die für nichts anderes zu verwenden seien (*"Hacker haben absolut keine Chance.... Den Beweis der Aussage, dass man mit unserer Wahlmaschine auch Schach spielen kann, würde ich gerne vorgeführt bekommen.",* **Anlage B 42**)

Zur Widerlegung dieses Statement des Herstellers haben *Gonggrijp et al.* die Softwarespeicher der Geräte neu programmiert und eine Schachsoftware aufgespielt (Kapitel 4.7). Weil der in den Geräten installierte Microprozessor (Motorola 68000) Ende der 80er Jahre in zahlreichen Heimcomputern eingesetzt wurde, konnten die Autoren frei verfügbare und gut dokumentierte Programme und Werkzeuge ver-

wenden. Der Bericht stellt fest, die eigentliche Herausforderung habe in der Befestigung der Schachfiguren auf dem schrägen Bedientableau des Wahlcomputers gelegen. Der sehr kleine Arbeitsspeicher der Nedap-Geräte habe zudem einige Kompromisse erfordert und führe dazu, dass der Wahlcomputer kein besonders starker Schachspieler sei

2. Manipulation einer Wahl durch Austausch der Software

Die Möglichkeit einer Wahlmanipulation durch Austausch der Gerätesoftware wird bereits im ersten Bericht der irischen „Kommission für elektronische Wahlen“ diskutiert (CEV-2004, S. 139 f., **Anlage B 43**)

Gonggrijp et al. haben mit Methoden des Reverse Engineering die Funktionsweise der Gerätesoftware untersucht, und dann an bestimmten Stellen ihre eigene Manipulationssoftware eingefügt. Dabei bleibt der überwiegende Teil der Original-Software intakt und stellt so sicher, dass sich das Gerät nach außen scheinbar normal verhält. Tatsächlich speichert das Gerät jedoch nicht alle abgegebenen Stimmen unverändert auf dem Stimmenspeicher, sondern verschiebt einen Teil der Stimmen zu einer vorher festgelegten Partei, die begünstigt werden soll.

Technisch bleibt die ursprüngliche Software fast unverändert. An bestimmten, definierten Stellen unterbricht die Originalsoftware ihre Ausführung, springt in zusätzliche, neue Programmteile und setzt anschließend die normale Verarbeitung fort. Durch dieses Vorgehen waren die Autoren bei ihrer Manipulation nicht auf den Quellcode der Originalsoftware angewiesen, um ihre Änderungen vorzunehmen.

Um bei einfachen Testwahlen nicht entdeckt zu werden, entscheidet die manipulierte Software erst am Ende der Wahl, ob die Manipulation der Stimmen tatsächlich ausgeführt werden soll. Die Autoren diskutieren ausführlich, wie eine manipulierte Software eine Testwahl erkennen kann (Kap. 5.2). Dabei führen Sie u.a. die Zahl und Frequenz der

abgegebenen Stimmen an und die Dauer der Wahl. Durch die Auswertung der statistischen Verteilung der Zeitintervalle zwischen den einzelnen Bedienschritten der Wähler könne man zudem erkennen, ob einige wenige Testwähler die Wahl durchführten. Weil die einmal im Stimmenspeicher abgelegte Stimme (vom Wahlcomputer) nicht mehr verändert werden kann, werden die zur Manipulation vorgesehenen Stimmen zunächst im Gerät zwischengespeichert, und erst am Ende der Wahl in das Speichermodul übertragen.

3. Wirksamkeit einer Softwaremanipulation

Das Bundesministerium des Innern führt in seiner Stellungnahme vom 03.05.2006 aus, die auf den Geräten installierte Software enthalte lediglich Informationen über den generellen Ablauf der Wahl, während die Daten der Wahlvorschläge und andere konkrete Daten auf dem Speichermodul gespeichert würden (**Anlage B 19**, Kapitel 3.2.3). Das Speichermodul werde von den Gemeindebehörden programmiert und erst kurz vor dem Wahlgang in das Gerät eingebracht. Da sich die manipulierte Software zu diesem Zeitpunkt bereits im Gerät befinde, müsse eine manipulierte Software blind entscheiden, wie z.B. die Stimmen zwischen Bewerber A und B oder Liste 7 und 8 aufgeteilt werden sollen. Deshalb sei eine Manipulation der Software unsinnig. Diese Auffassung macht sich auch der Bundestag zu eigen (Drs. 16/3600, S. 22, **Anlage B 37**).

Die Ausführungen des BMI sind aus mehreren Gründen fehlerhaft. Selbst die nicht manipulierte, zugelassene Wahlgeräte-Software greift während des Wahlgangs auf die Speichermodule zu und liest die Zuordnung der Parteien zu den einzelnen Tasten des Wahlgerätes aus. Dies geschieht, damit dem Wähler seine Auswahl auf dem Display des Gerätes angezeigt werden kann. Eine manipulierte Software kann deshalb die im Speichermodul hinterlegte Tastenbelegung durchaus ermitteln. Deshalb muss bei der Manipulation der Software lediglich der Name der Partei bekannt sein, die begünstigt werden soll. Eine Manipulation der Wahlsoftware muss somit keinesfalls blind erfolgen.

Die Behauptung des BMI ist durch *Gonggrijp et al* nun auch experimentell widerlegt (Gonggrijp et al., Kap. 5.1, **Anlage B 7**). Die manipulierte Software der Autoren durchsucht die im Stimmenspeicher einprogrammierten Wahlvorschläge nach dem Parteinamen der zu begünstigenden Partei. Dieser wird dann nach einem festgelegten Algorithmus ein Teil der für andere Parteien abgegebenen Stimmen zugerechnet.

Im Übrigen können die Gemeindebehörden die Reihenfolge der Kandidaten und Listen ohnehin nicht frei wählen. Die Reihenfolge der Wahlvorschläge auf den amtlichen Stimmzetteln ergibt sich zwingend aus § 30 BWG. Diese Reihenfolge ist gemäß § 8 Abs. 2 BWahlGV auch bei der Darstellung der Wahlvorschlägen an den Wahlgeräten einzuhalten. Die Reihenfolge der Wahlvorschläge am Wahlcomputer ist deshalb schon lange vor der Wahl bekannt und nicht erst nach der erfolgten Konfiguration der Geräte.

4. Manipulation der Stimmenspeicher

Die Stimmenspeicher der NEDAP-Wahlcomputer haben, bedingt durch das Alter der eingesetzten Technologie, etwa die Größe von Zigarettenschachteln. In einem Volumen dieser Größe lassen sich heutzutage Mikrocomputer (einschließlich einer Stromversorgung) unterbringen, die die Rechenleistung der NEDAP-Computer um ein Vielfaches übersteigt. Die Autoren skizzieren deshalb einen Angriff, der eine solche aktive Elektronik im Gehäuse der Speichermodule einsetzt (Kap. 7.2).

Ein solcher manipulierter Stimmenspeicher würde sich gegenüber dem Wahlcomputer zunächst normal verhalten, also die abgegebenen Stimmen richtig speichern. Am Ende der Wahl würde der Stimmenspeicher jedoch nicht die die tatsächlich abgegebenen Stimmen zurückliefern, sondern einen Teil der Stimmen der gewünschten Partei zuschieben. Da ein solches manipuliertes Speichermodul nicht mit

den begrenzten Mitteln der NEDAP-Computer auskommen müsste, ließe sich zudem eine intelligentere Logik zum Erkennen von Testwahlen realisieren.

Dieser Angriff ist nur deshalb überhaupt möglich, weil die Geräte in zweierlei Punkten nicht dem Stand der Technik entsprechen:

- Zum einen werden die Stimmen auf dem Speichermodul nicht verschlüsselt abgelegt. Nur deshalb ist eine Veränderung des Speicherinhalts überhaupt möglich. Auch ein Minicomputer im Stimmenspeicher wäre nicht in der Lage, einen angemessen verschlüsselten Speicherinhalt zu fälschen.
- Zum anderen ist der Stimmenspeicher nicht durch eine Schnittstelle vom Wahlcomputer isoliert: Der Wahlcomputer greift unmittelbar über seinen Datenbus auf die Stimmenspeicher zu. Das bedeutet umgekehrt, dass auch eine aktive Elektronik im Gehäuse des Stimmenspeichers Zugriff auf den kompletten Speicherinhalt des Wahlcomputers hat und der Wahlcomputer keinerlei Informationen vor dem manipulierten Stimmenspeicher verbergen kann. Würde der Wahlcomputer die Stimmen auf dem Stimmenmodul verschlüsselt ablegen, hätte das Stimmenmodul Zugriff auf den entsprechenden Schlüssel im Speicher des Wahlcomputers und könnte den Sicherheitsmechanismus damit umgehen.

5. Manipulation des Bedientableaus

Gronggrijp et al. schlagen noch eine weitere Attacke mit aktiver Elektronik vor, bei denen ein Mikrocomputer im geräumigen Gehäuse des Bedientableaus untergebracht wird (Kap. 7.1). Die Elektronik würde zwischen de Tastatur und die Geräteelektronik geschaltet und die Stimmen schon bei der Abgabe manipulieren. Weil sich auch das Kontrolldisplay des Wählers in diesem Gehäuse befindet, könnte eine sol-

che Elektronik dem Wähler vorgaukeln, die Stimme sei unverändert abgespeichert worden.

Weil der mechanische Einbau einer solchen Elektronik in das Gehäuse des Bedientableaus aufwändig ist, ist dieser Angriff aber weniger wahrscheinlich als die Angriffe auf die Gerätesoftware und die Stimmenspeicher.