PETER FÖRSTER / DPA

Wahlmaschine (in Sachsen-Anhalt): *Zum Schachcomputer umfrisiert*

WAHLEN

Ergebnis nach Wunsch

Hacker haben Wahlcomputer untersucht und warnen in einem Bericht für das Bundesverfassungsgericht: Die Geräte sind leicht zu manipulieren.

Für Oskar Mürell, Wahlleiter der hessischen Stadt Obertshausen, haben Wahlabende ihren Schrecken verloren. Kurz nach 18 Uhr schließen seine Leute die Rückseite ihrer neuen, koffergroßen Computer auf, drücken Knöpfe – und schon rattern kassenzettelgroße Papierstreifen mit den Ergebnissen heraus.

Wo früher oft noch stundenlang Stimmzettel ausgezählt wurden, könne er die Helfer heute schon zehn Minuten nach Schließung der Wahllokale nach Hause schicken, sagt Mürell. Die neuen Wahlcomputer, Stückpreis rund 4500 Euro, seien „eine super Sache“.

Doch die Bequemlichkeit hat ihren Preis: Niederländische Hacker haben mit Mitgliedern des deutschen Chaos Computer Clubs (CCC) mehrere Wahlmaschinen geknackt, die mit den in Deutschland eingesetzten Geräten fast baugleich sind. In einem 54-seitigen Gutachten für das Bundesverfassungsgericht beschreiben die CCC-Aktivisten jetzt gravierende Sicherheitsmängel in dem System: Es sei für einen durchschnittlich begabten Informatikstudenten kein Problem, auch Bundestags-Wahlergebnisse einzelner Stimmbezirke nach Belieben zu manipulieren.

In den Niederlanden, wo Wahlcomputer weiter verbreitet sind als in Deutschland, hat die Hacker-Aktion eine breite Debatte über die Sicherheit der Abstimmungen ausgelöst. Und auch hierzulande wurden bei der Bundestagswahl vor zwei Jahren nach einer Statistik des Innenministeriums bereits 1850 derartige Geräte eingesetzt – die Wähler mussten in den Kabinen keine Kreuzchen machen, Knopfdruck reichte. Vorreiter sind Kommunen in Nordrhein-Westfalen. Aber auch in Hessen, wo im Januar 2008 der Landtag neu gewählt wird, stehen rund 130 Wahlcomputer.

Hessens Landeswahlleiter Wolfgang Hannappel sieht dennoch keinen Grund, auf die Geräte zu verzichten: „Sie sind bei uns zugelassen und gelten damit als sicher.“ Die Maschinen der niederländischen Firma Nedap, die in Deutschland bislang zum Einsatz kamen, seien von der Physikalisch-Technischen Bundesanstalt (PTB) geprüft und für gut befunden worden: „Wir haben aber nach Rücksprache mit der PTB unsere Wahlordnung jetzt noch einmal verschärft und die Kommunen verpflichtet, die Geräte an einem sicheren Ort aufzubewahren, wo sie für Unbefugte nicht zugänglich sind.“

Da genau liegt das Problem: Schon 60 unbeaufsichtigte Sekunden in der Nähe einer Maschine reichten versierten Bastlern aus, um dem Gerät einen manipulierten Chip einzusetzen, der vom Original nicht zu unterscheiden ist, sagt Constanze Kurz, Informatikerin an der Berliner Humboldt-Universität und CCC-Mitglied. Die Schlüssel für die Geräte könne man bequem übers Internet bestellen, die Papiersiegel mit normalen Druckern kopieren.

Wie flott Ergebnisse zu frisieren sind, können sich die Verfassungsrichter jetzt in Echtzeit auf einer DVD anschauen, die der CCC seinem Gutachten beigelegt hat. Die Karlsruher Juristen wollen mit Hilfe der Expertise über die Beschwerde eines hessischen Bürgers entscheiden, der die letzte Bundestagswahl wegen des Maschineneinsatzes wiederholen lassen will.

In dem Gutachten wird ausführlich dokumentiert, wie die niederländisch-deutsche Truppe um den Amsterdamer Hacker Rop Gonggrijp eines der Geräte sogar zum Schachcomputer umfrisierte. Auch das Wahlgeheimnis haben die Computerfreaks geknackt: Mit einer hochsensiblen Antenne und einem umgebauten Navigationsgerät konnten sie aus 25 Meter Entfernung feststellen, welche Partei-Taste jemand in der Kabine gerade drückte.

Für einen Praxistest sind CCC-Hacker dann durch hiesige Kommunalwahllokale getourt. Fast immer fanden sie Gelegenheiten, unbeobachtet an den Geräten herumzufingern – im Einzelfall bis zu 20 Minuten lang, weil etwa ein Hausmeister die Maschinen aufstellte, lange bevor ein Wahlvorstand vor Ort war.

Die Software könne dann so verändert werden, dass das Testprogramm vor dem Wahlgang ohne Beanstandungen durchlaufe, sagt Kurz. Aber bei der eigentlichen Wahl spucke der Rechner schließlich ein vorher programmiertes Wunschergebnis aus: „So etwas schaffen viele meiner Studenten schon im ersten Semester.“

Überdies stießen die Elektronikspezialisten auf Manipulationsmöglichkeiten, für die sie die Geräte nicht einmal öffnen müssen. Anfällig seien etwa kleine Speichermodule, die nach der Wahl aus dem Computer genommen und zu einem zentralen PC im Gemeindewahlamt gebracht werden. Dort werden die Ergebnisse addiert und an die Landesbehörden übertragen. Das Programm in diesem Zentral-PC sei durch seine Internet-Verbindung ein leichtes Ziel für Hacker-Angriffe.

HOLLANDSE HOOGTE / LAIF

Hacker Gonggrijp
60 Sekunden reichen

Dass all diese Geräte immer sicher wegzusperren seien, hält der CCC für illusorisch. Nicht selten verfügten in Gemeindeverwaltungen schon die Putzfrauen über Generalschlüssel. Und auch mancher Bürgermeister könnte vielleicht der Versuchung nachgeben, durch einen kurzen Besuch im Lagerraum des Rathauses seiner Wiederwahl ein wenig nachzuhelfen.

MATTHIAS BARTSCH, TIM KLIMEŠ, OLIVER REZEC