

Creatief met stemcomputers

Stemcomputers blijken manipuleerbaar. Minister Nicolai gaat de lekken dicht, maar dat lost niet alles op. 'Het probleem met stemcomputers blijft dat de verkiezingsuitslag niet te controleren is.'

Door Michael Persson

Toen hacker en internetmiljonair Rop Gonggrijp op 7 maart dit jaar voor het eerst van zijn leven een knop van een elektronische stemmachine indrukte, wist hij het meteen. Dit nooit weer. Een paar maanden later richtte hij de stichting *Wij vertrouwen stemcomputers niet op*.

Nu, weer een paar maanden later, loopt hij op kousenvoeten door de hobbykamer van zijn huis in de Amsterdamse Watergraafmeer. Er zitten vlekken op de plavuizen, er staat een halfliep blikje cola-light tussen het gereedschap en de computeronderdelen. In een hoek staat een Nedap/Groenendaal ES3B stemcomputer.

Die is inderdaad niet te vertrouwen. Gonggrijp en collega's hebben de software vervangen door een eigen programma, waardoor de Frauderende Partij 2006 zojuist in deze kamer de verkiezingen won. Zonder dat één stem op die partij is uitgebracht. Bovendien bleek dat elke stem op het CDA met een radio-ontvanger afgeluisterd kon worden. Dag stemgeheim.

De stunt, vorige week ook gedemonstreerd tijdens een persconferentie in Nieuwspoor in Den Haag, heeft effect gehad. Verantwoordelijk minister Nicolai van Bestuurlijke Vernieuwing heeft deze week de Tweede Kamer beloofd alle lekken te zullen dicht. Donderdag zei de VVD-bewindsman dat nieuwe software, een extra verzegeling en betere bewaking betrouwbare verkiezingen zullen garanderen.

Maar volstaat dat? Zelfs al kunnen hackers straks niet meer in de machines inbreken, dan nog kunnen de fabrikanten zelf de verkiezingen manipuleren, vrezen Gonggrijp en de zijnen. 'Het probleem met stemcomputers blijft dat de verkiezingsuitslag niet te controleren is.'

De grote vraag is hoeveel mensen nodig zijn om de democratie te controleren. 'Ik vind het zeer vreemd dat er maar een paar mensen zijn in Nederland die weten hoe de stemmen geteld worden', zegt Bart Jacobs, hoogleraar computerbeveiliging aan de Radboud Universiteit Nijmegen. 'Dat zijn de mensen die de software kennen. Daar is niemand van de overheid bij.'

Rood potlood

De eerste stemmachines arriveerden in 1967 in de Nederlandse stemlokalen. Straks, op 22 november, stemt ruim 99 procent van de kiezers via een van de 9300 Nederlandse stemcomputers. Er zijn nog slechts tien plaatsen waar je met een ouderwets rood potlood een vakje kunt aankruisen.

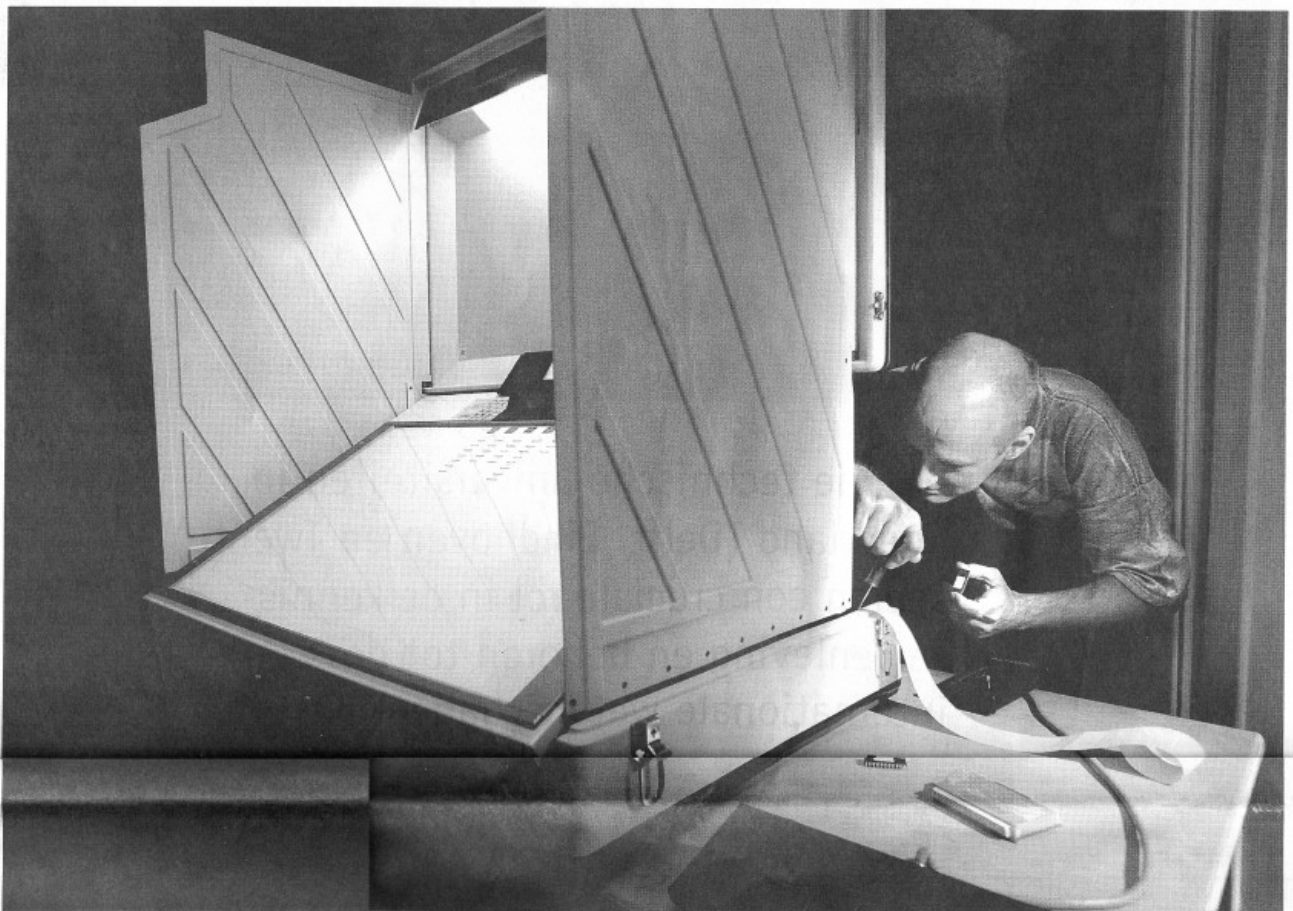
Dat de bezorgdheid nu pas een stem gekregen heeft, komt doordat de bezorgdheid in Amsterdam woont: Amsterdamers zoals Gonggrijp zijn pas bij de gemeenteraadsverkiezingen in maart dit jaar met de stemmachines in aanraking gekomen. 'Het sunderde bij mij al langer', zegt Gonggrijp, 'maar die ervaring heeft de alarmbellen pas echt laten afgaan.'

Het merendeel van de Nederlandse stemcomputers, 8100 om precies te zijn, is afkomstig van fabrikant Nedap uit Groenlo. Hacker Gonggrijp, mede-oprichter van internetprovider Xs4all, wist twee van die machines op de kop te tikken bij een gemeente waarvan hij de naam niet wil noemen.

De apparaten zijn met een kruiskopshroevendraaier open te maken, waarna een grote printplaat zichtbaar wordt met forse chips en schakelingen. Het brein is een Motorola-68000 microprocessor, bekend van de Atari en Commodore computers uit de jaren tachtig.

De hackers haalden de twee geheugenchips (zwarte blokjes van een centimeter of drie) met de verkiezingssoftware uit de computer en lazen de inhoud af met een 'Epson-reader', een in de winkel verkrijgbaar chip-leeskastje.

Wie dat doet, ziet op het scherm van een aangesloten computer een waslijst aan cijfers en letters verschijnen. Deze machinaal is on-



Hacker en internetmiljonair Rop Gonggrijp bij de gemanipuleerde stemcomputer in zijn Amsterdamse hobbykamer.

FOTO JEAN-PIERRE JANS - DE VOLKSKRANT

begrijpelijk, en wordt daarvoor door een *disassembler* omgezet in duidende regels computercommando's, die er samen enigszins uitzien als een - zeer gebruiksvriendelijk - computerprogramma. Gonggrijp en zijn mede-hackers zijn vervolgens wekenlang gaan *reverse engineeren*. Bij dit proces van omgekeerd uitvinden haal je een product helemaal uit elkaar, om vervolgens van elk onderdeel de functie te doorgronden.

Gonggrijp en consorten konden op deze manier de werking van het programma reconstrueren zonder de broncode te kennen. De broncode is het in normale computer taal geschreven programma, dat voor een goedgeend lezer makkelijk te begrijpen is. Fabrikant Nedap had altijd volgehouden dat de stemcomputers veilig zijn, omdat de broncode geheim is.

Niet dus. De hackers vervingen de chips door een eigen programma, dat na de verkiezingen de uitgebrachte stemmen naar andere partijen verschuift. Door slechts een paar procent te veranderen zou de gemanipuleerde uitslag niet opvallen, denkt Gonggrijp. 'Dat betekent wel dat je zoveel mogelijk stemcomputers moet aanpassen.'

En dat is mogelijk. 'In Rotterdam konden we zo in een loods met vierhonderd opgeslagen apparaten. Er is geen reden aan te nemen dat het in andere plaatsen anders is.' Het wisselen van de chips kost zo'n tien minuten per computer, de loods in Rotterdam zou met twintig man een nacht werk zijn geweest, zegt Gonggrijp. 'Als we niet hadden gewaarschuwd, was Rotterdam nu van ons geweest.'

Het testen van de stemcomputers, direct voorafgaand aan de verkiezingen, zou geen zin hebben. De hackers kunnen regels toevoegen waardoor hun programma de stemmen alleen gaat verschuiven als er meer dan vijfhonderd stemmen zijn uitgebracht, als er steeds enige tijd tussen twee uitgebrachte stemmen heeft gezeten, en als de computer langer dan acht uur heeft gedraaid. Een snelle test zal aan dat soort voorwaarden niet voldoen.

Voor een landelijke verkiezingen-

'Als we niet gewaarschuwd hadden, was Rotterdam nu van ons geweest'

Stemcomputers ook elders fraudegevoelig

Nederland is niet het enige land waar ophef over stemcomputers is ontstaan. Nadat Ierland in 2004 Nederlandse Nedap-machines had aangekocht, verschenen enkele vernietigende rapporten. De 7500 machines zijn nog niet uitgetekend en zullen bij de komende verkiezingen, in 2007, niet worden gebruikt. In de Verenigde Staten ligt vooral de grootste fabrikant van stemmachines, Diebold, onder vuur. Computerwetenschappers van Princeton University brachten op 13 september een rapport naar buiten waarin bleek dat de Diebold AccuVote-TS stemcomputers zeer



fraudegevoelig zijn. Net als de Nederlandse hackers ontwikkelden ze software die stemmen van de ene partij steelt en aan de andere toedeedt. Met een soort mini-bar sleuteltje maakten de onderzoekers de computer open, waarna zij een geheugenkaart met de stemmenstelsende software in de computer plaatsten. In minder dan een minuut wisten ze het programma op de compu-

ter te installeren. Diebold raakte in opspraak in de aanloop naar de presidentsverkiezingen van 2004. De baas van het bedrijf, Wally O'Dell, schreef aan Republikeinen in Ohio dat hij zich zou inzetten om de stemmen uit die staat aan president Bush te geven. Dat sloeg niet op de Diebold-machines, haastte Diebold zich daarna te zeggen. O'Dell moest december 2005 opstappen vanwege een onderzoek naar beurshandel met voorkennis. Inmiddels eisen 27 staten dat stemcomputers zichtbaar voor de kiezer een papieren afdrukken met de uitgebrachte stem.

manipulatie voorziet Gonggrijp het omkopen van Nedap-werknemers, of van de transporteurs. 'Het zou misschien een paar jaar duren. Maar dat heb je wel er wel voor over als je de macht wil grijpen.'

Verzegeld

Dus zit nu verkoopleider Hans van Wijk van Nedap in de auto, op weg naar Den Haag voor overleg op het ministerie van Binnenlandse Zaken. Nedap heeft toegezegd alle stemcomputers te controleren. In elke computer worden de twee geheugenchips met de verkiezingssoftware vervangen door nieuwe chips, die 'niet overschrijfbaar' zijn. Daarna worden ze verzegeld.

Lost dat wat op? De hackers manipuleerden de machines niet door de oorspronkelijke chips te herprogrammeren, maar door die te vervangen door eigen chips, met een eigen programma. En dat kan nog steeds, erkent ook Van Wijk: 'Maar om dat straks te kunnen doen moet je iets fysiek kapotmaken. Dan is forensisch vast te stellen dat een computer gemanipuleerd is, en daar gaat het om.'

Er is nog een ander probleem. De Nedap-stemcomputers hebben een klein groot beeldschermje, dat naam en partij weergeeft van de kandidaat waarop de kiezer heeft gedrukt. Niemand kan de tekst op dat groene beeldschermje meelezen. Dat is ook de bedoeling: in een democratie hoeft niemand te weten op wie je hebt gestemd.

Maar wie nu met een wereldontvanger bij een stembureau gaat staan en afstemt op een frequentie van 36 megahertz, ontvangt een vette bromtoestel: dat is het beeldschermje van de stemcomputer. De bromtoestel heeft een hoogte van 72 hertz. Totdat de kiezer in het hokje op een CDA-kandidaat drukt. Dan wordt het hoorbaar een stukje lager, 60 hertz. Zo kan iedereen met een wereldontvanger horen wanneer en door wie er op het CDA wordt gestemd.

Dat komt doordat het goedkope Japanse schermjes zijn, zegt Gonggrijp. Het schermgeheugen bevat alleen normale letters. Voor de è van Christen Democratisch Appèl moet de computer in een ander geheugen graven, met speciaal gedefinieerde tekens. Dat kost

rekentijd, en dus gaat de frequentie van het scherm omlaag.

Van Wijk van Nedap zegt dat het probleem op te lossen is, door bijvoorbeeld ook de spatie als speciaal teken te definiëren, en dat teken vervolgens bij elke partij in het scherm te stoppen. Dan is dus bij elke partij een lagere toon te horen, en is er geen verschil meer.

Maar volgens Gonggrijp is daarmee het probleem niet verholpen. Want niet alleen zenden de speciale tekens op het beeldscherm specifieke radiosignalen uit, ook heeft elke knop op het stempaneel zijn eigen unieke *burst*. Met betere apparatuur dan een simpele wereldontvanger wordt elke ingedrukte knop herkend. Als de kiezer niet stemt maar piano speelt.

Daar houdt het ministerie van Binnenlandse Zaken geen rekening mee. Evenmin houdt het al rekening met de problemen die de andere twaalfhonderd Nederlandse stemcomputers, van fabrikant Sdu Uitgevers, met zich meebrengen. 'Daar ben ik eerlijk gezegd nog veel bang voor', zegt Gonggrijp. 'Die zijn wel ongrijpbaarder.'

Deze New Vote computers worden gebruikt in 28 gemeenten, waaronder Tilburg en Amsterdam. De apparaten blijven eigendom van Sdu. Aan het eind van de verkiezingsdag bellen ze via een GPRS-verbinding naar het commandocentrum in Den Haag, waar de stemmen worden verwerkt. Het gevaar van die verbinding zou zijn dat derden zich toegang tot het systeem kunnen verschaffen.

Zo erg is dat niet, zeggen verkiezingsleiders in Amsterdam. Het gaat om een voorlopige uitslag. De definitieve uitslag is gebaseerd op een uitdraai uit de stemcomputer (op papier en op een schijfje), die niet wordt doorgeleed.

Een fundamenteel gevaar, zegt hoogleraar Jacobs in Nijmegen, is dat er maar een paar mensen zijn die weten hoe de software in de computers precies werkt. Bij het stemmen met het potlood controleren tienduizenden burgers de verkiezingen. Fraude is mogelijk, maar niet op grote schaal. Bij gebruik van stemcomputers zijn er maar enkele die de verkiezingssoftware maken en bewaken.

Voor de gemeenten is het een kwestie van vertrouwen. 'Elk systeem is te manipuleren en berust uiteindelijk op vertrouwen', zegt Rob Kalse, hoofd verkiezingen in

Amsterdam. 'Dus moet je zorgen dat de procedures in orde zijn.'

Het gaat hem daarbij uiteindelijk om controle. Die is uitbesteed aan TNO, dat als enige inzage heeft in de broncode van de Sdu-computers. Althans, de broncode waarvan Sdu zegt dat die in de computers zit. Wat er precies in de apparaten zit die aan de gemeente worden geleverd, weet vrijwel niemand. De geheimzinnigheid is strategisch, blijkt uit een reactie van Sdu-directeur Huib Cuperus. 'Onze beveiliging werkt mede op basis van het geheim houden hoe de beveiliging geregeld is.'

Betrouwbaarheid

De rol van TNO is daarbij mistig. Hoeveel gemeente-ambtenaren zoals Rob Kalse zeggen zich voor de betrouwbaarheid van de stemmachines geheel op het instituut te verlaten, zegt het ministerie van Binnenlandse Zaken dat 'TNO nooit gekeken heeft naar de beveiliging in de zin van manipuleerbaarheid'. Er is alleen gekeken of er iets uit de computers rolt. Of de uitslag klopt, is een tweede.

TNO zelf laat zich niet over zijn rol uit. Hoeveel de minister het instituut deze week aanprees als 'onafhankelijke keuringsinstelling', met 'deskundigheid en een onafhankelijk oordeel', verwijst TNO voor elk commentaar naar het ministerie van Binnenlandse Zaken.

Het is deze *security through obscurity* die computerdeskundigen zorgen baart. En dat blijft een probleem met stemcomputers, onbepaald de mate waarin die minister heeft aangekondigd, zoals het openbaar maken van de software. Jacobs: 'Het vrijgeven van broncodes helpt iets, maar het probleem daarbij is dat je niet weet of de gepubliceerde software ook echt op de stemcomputers draait. Dat moet dan alsnog gecontroleerd. Eenvoudig is het dus niet.'

Kalse denkt dat een *paper trail* naast de computer de controleerbaarheid van de uitslag kan vergroten. Uiteindelijk, denken velen, is alleen papier betrouwbaar.

Minister Nicolai besloot donderdag een commissie met deskundigen in te stellen die dergelijke mogelijkheden gaat onderzoeken. Gonggrijp wacht dat niet af. Hij gaat op 22 november stemmen in Zoeterwoude. Een van de laatste gemeenten met een rood potlood.