Richard Sietmann, Michael Janßen, Marcel van der Meer

Duistere praktijken

Zijn stemcomputers fraudegevoelig?

Over grofweg een maand is het weer zover en gaat heel Nederland naar de stembus. De kans is groot dat je je politieke voorkeur op 22 november via een stemcomputer kenbaar maakt, want in meer dan negentig procent van de Nederlandse gemeenten wordt elektronisch gestemd. Ondanks alle gemakken die digitaal stemmen met zich meebrengt, begint het wantrouwen tegen deze manier van stemmen inmiddels drastische vormen aan te nemen, ook buiten onze landsgrenzen.

In Ierland zijn de uit Nederland afkomstige stemcomputers voor de komende verkiezingen in 2007 alweer aan de kant gezet. Volgens het Algemeen Dagblad van 15 september j.l. erkent het Ministerie van Binnenlandse Zaken dat de computers fraudegevoelig zijn, maar stelt daarnaast dat ze "voldoende veilig" zijn. Maar bepaalt de huidige techniek ook al wie onze volksvertegenwoordigers in de Tweede Kamer worden of doen we dat toch nog steeds zelf?

Om het traditionele stemmen met een rood potlood door apparaten met elektronische stemregistratie te vervangen moet een hoogwaardig IT-systeem gebruikt worden. Softwarefouten of manipulaties kunnen immers voor een aantal jaren het politieke klimaat in een land bepalen. Stemmen is tenslotte een van de weinige manieren waarmee onze politieke machtsverdeling wordt bepaald. Aan de integriteit van de procedures daarbij moet je dus ook de hoogste eisen stellen.

Hoogwaardige IT-systemen worden via een omslachtige procedure ingevoerd. Eerst wordt uitgebreid in kaart gebracht aan welke eisen het apparaat moet voldoen. Vervolgens wordt een apparaat ontwikkeld en uitgebreid getest. Daarbij moet ook rekening worden gehouden met (bijna) alle denkbare risico's.

Het National Institute of Standards and Technology (NIST) beschrijft in de 'Risk Management Guide for Information Technology Systems' [1] een logische stappenprocedure met denkbare bedreigingen, zwakke plekken, mogelijk schadelijke gevolgen en tegenmaatregelen. De rode draad is het gegeven dat de risicoanalyse niet beperkt moet blijven tot het informatietechnische systeem zelf. Ook de complete taakstelling en organisatie moet in het proces worden meegenomen.

Of dit voor de stemmachines in Nederland ook geldt is discutabel. Terwijl de overheid vooralsnog geen probleem ziet en de machines "voldoende veilig" acht, zijn er burgerorganisaties zoals de stichting "Wij vertrouwen stemcomputers niet" [2] die – zoals de naam al zegt – vraagtekens plaatsen bij de veiligheid van deze systemen.

Werking

De kern van de veiligheid van de stemcomputer wordt gevormd door een functionele scheiding tussen de stemmenopslagmodule en de stemcomputer. Het softwareprogramma op de EPROMS in de computer bepaalt de algemene voortgang; hieronder vallen voornamelijk functies als het vrijgeven van het apparaat om een stem te kunnen ingeven, invoeren van je stem, corrigeren van verkeerde invoer, verwerken van je definitieve stem, opslag van het totale aantal stemmen, vergrendelen en afkoppelen van het apparaat en tenslotte de definitieve telling. De kiesgegevens voor de specifieke verkiezingen, de displayteksten en het definitieve aantal stemmen na de verkiezingen staan in de geheugenmodule die door de stemcommissie is geconfigureerd en na de verkiezingen meteen wordt verwijderd – een soort van 'elektronische stembus' dus.

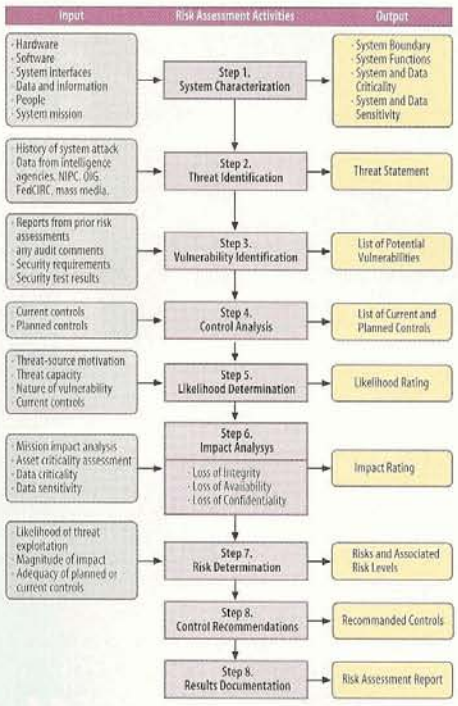
De EPROMs in de stemcomputer met de software worden geprogrammeerd bij de producent (Nedap-Groenendaal of SDU) en op de printplaat geïnstalleerd. Mochten ze in de fabriek of na het uitleveren gemanipuleerd worden, dan zouden die manipulaties een blinde gok zijn. Het is namelijk nog onbekend welke partij onder welke knop terecht gaat komen, omdat de volgorde van de partijen bij elke verkiezingen wordt veranderd. Dat is in ieder geval de theorie.

Fraudescenario

Er schuilen wel een aantal addertjes onder het gras. Ten eerste is de volgorde van de partijen op de stembiljetten niet willekeurig. De eerste plaatsen worden bezet door de volgorde waarin de grote partijen bij de vorige verkiezingen zijn geëindigd. Dit betekent dat positie 1 wordt ingenomen door het CDA, 2 door de PVDA, 3 door de VVD, 4 door de SP, etc. Daarna volgen in willekeurige volgorde de partijen zonder zetels die zich in heel Nederland beschikbaar hebben gesteld. Als laatste komen de partijen die alleen in een bepaalde kieskring gekozen kunnen worden. De partijen die in meer kieskringen vertegenwoordigd zijn, staan hierbij verder vooraan.

Voor de fraudeur zijn de partijen met de meeste zetels natuurlijk de makkelijkste en meest interessante prooi. Van deze partijen is het namelijk het langst bekend op welke positie ze in de stemmachines staan en is aannemelijk dat ze in een nieuw kabinet zitten en dus veel invloed krijgen.

Een slimme fraudeur gaat natuurlijk niet vast programmeren dat bij het drukken van een bepaalde toets de stem wordt onderschept en dat die dan domweg aan een andere partij wordt toegekend. Slimmer is om zich te richten op het manipuleren van de softwarelaag in het stemgeheugen waar geconfigureerd wordt welke partij aan welke knop gekoppeld gaat worden. Door de functionele scheiding van geheugenmodule en stemcomputer lijken het twee gescheiden processen



Het National Institute of Standards and Technology (NIST) beschrijft in de 'Risk Management Guide for Information Systems' de procedure bij een risicoanalyse volgens de erkende regels van de techniek; het is een exact gedefinieerd stappenplan.

De EPROMS met de software voor de Nedap-stemmachines zijn op het moederbord eenvoudig aangebracht in sockets en kunnen makkelijk worden vervangen.

te zijn en dat impliceert een bepaalde mate van veiligheid. Het is echter niet zo dat de module en de computer onderling geen gegevens kunnen uitwisselen of dat de gegevens echt alleen maar in één richting lopen. Zo gebruikt bijvoorbeeld het stuurprogramma van de stemcomputer de gegevens over de toetsbezetting van de geheugenmodule om de kandidaten op de display weer te geven. Een fraudeur kan de software zo manipuleren dat deze zelf achterhaalt welke partij achter welke knop zit door de leesbare tekst te onderscheppen. Vervolgens kan een stem worden omgeleid naar de partij die volgens de fraudeur de verkiezingen moet winnen. Door maar een percentage van de uitgebrachte stemmen om te leiden is het ook maar de vraag of dit gaat opvallen – testen om het tegendeel te bewijzen zijn nooit uitgevoerd.

Daarnaast is het moederbord met de embedded software in de stemcomputer identiek aan dat van de programmeer- en leesunit. Een manipulator met de nodige kennis en tools zou de stemcomputer kunnen gebruiken als programmeerunit en de configuratie van de knoppen direct op de stemgeheugenmodule kunnen wijzigen. Hierdoor zou je bijvoorbeeld de computer op de dag van de verkiezingen in een andere telmodus kunnen zetten op het moment dat een kiezer een bepaalde toetsencombinatie indrukt.

Verdedigers

Een belangrijk punt is daarom de vraag hoe je kunt garanderen dat de software in de apparaten niet gemanipuleerd is en overeenkomt met de software die door de TNO-ITSEF getest werd. Bij de Nedap-apparaten identificeert het stuurprogramma zich bijvoorbeeld met een versienummer en twee checksums die het apparaat zelf via een algoritme in de software aanmaakt. De correctheid van het checksum-algoritme wordt geverifieerd bij de controle van het apparaat. De versie en beide checksums van de software kunnen op elk moment – in principe dus ook op de dag van de verkiezingen in het bijzijn van de kiezers –opgevraagd en geprint worden, om vervolgens met de originele gegevens vergeleken te worden. De software zou dus ook te allen tijde te identificeren zijn.

Hiermee geeft het voorwerp dat gecontroleerd moet worden zelf een bewijs af voor zijn eigen identiteit. Bij deze gang van zaken kun je vraagtekens zetten. Er is bijvoorbeeld geen mechanisme waarmee gegarandeerd wordt dat het programma de checksum daadwerkelijk berekent. Voor hetzelfde geld wordt gewoon het juiste getal gegeven.

Doordat stemmachines tegenwoordig op grote schaal worden ingezet kunnen de verkiezingen op een 'niet-klassieke' wijze worden gemanipuleerd. Bij 'traditionele' fraudepogingen gaat men ervan uit dat één persoon de stemmen in een enkel stemlokaal op het dag van de verkiezingen probeert te veranderen. Dankzij stemmachines kunnen veel apparaten tegelijk worden gemanipuleerd. Als de software niet goed is geprogrammeerd of er zich logische fouten in het stemproces bevinden, hebben manipulerende groeperingen veel meer tijd om zich op hun coup voor te bereiden. Je kunt het met een bedrijf vergelijken dat alle computers van de werkplek centraal laat beheren door een dienstverlener: elke fout in het besturingssysteem of de applicatiesoftware heeft dan meteen effect op alle computers.

Buitenom

Je hoeft niet noodzakelijk de hand te leggen op een Nederlandse stemmachine om verkiezingen te kunnen manipuleren: Nedap verkoopt dezelfde stemapparaten ook in het buitenland. Al is de software per land ietwat verschillend, het basisconcept van de computer is in grote lijnen hetzelfde, zodat je voor het voorbereiden van een coup waarschijnlijk ook een Duitse of lerse stemmachine kunt gebruiken – en andersom. Hoewel het voor vastberaden manipulators handig is om de broncode te hebben, is dat zeker niet noodzakelijk. Via reverse engineering of het decompileren van uitvoerbare programma's is het eveneens mogelijk om manipulaties doelgericht uit te voeren. Welk resultaat de manipulatie oplevert is geheel afhankelijk van wat de aanvaller wil bereiken en hoeveel moeite hij daarvoor wil doen.

Het is dus voor een gewiekste fraudeur geen onoverkoombaar obstakel als de exacte werkwijze van de programma's en de machines geheim is. Dat 'security by obscurity' weinig betrouwbaar is, wordt duidelijk uit het feit dat er regelmatig lekken in Windows gevonden worden, die vervolgens door Microsoft gedicht moeten worden – als het achterhouden van broncode zou helpen zouden deze lekken überhaupt niet mogen bestaan.

Binnenin

Zoals bij alle veiligheidsproblemen in de IT zijn het ook bij verkiezingen met name de mensen die nauw betrokken zijn bij het proces, dus met directe toegang tot de software en stemcomputers, die het grootste gevaar vormen. Een gefrustreerde werknemer die wraak wil nemen, omgekochte medewerkers, adviseurs of ander personeel – allemaal hebben ze in principe toegang tot het systeem en eventueel ook specifieke kennis van zwakke plekken. Vergeleken met fraudeurs van buitenaf hebben ze dus veel meer keuze aan manipulatiemogelijkheden. Manipulatie van binnenuit is het moeilijkst op te sporen omdat er vaak geen of nauwelijks routinecontroles worden uitgevoerd. Ook worden verdachte aanwijzingen in logbestanden genegeerd. Wat ook regelmatig voorkomt is dat de officiële procedures met betrekking tot het veiligheidsbeleid in stemlokalen niet altijd even nauwlettend gevolgd worden.

Je kunt op 22 november natuurlijk ook nog – en misschien wel voor de laatste keer – op papier stemmen. In twaalf van de 458 gemeenten staan namelijk nog geen stemmachines. Je zou met je stembiljet dus naar een van deze gemeenten kunnen gaan om daar helemaal zonder elektronica te stemmen. Deze gemeenten zijn: Oirschot, Schijndel en Sint Anthonis (Noord-Brabant), Leeuweradeel en Ooststellingwerf (Friesland), Schermer en Zeevang (Noord-Holland), Zoeterwoude en Nederlek (Zuid-Holland), Zuidhorn (Groningen), Meijel (Limburg) en Neerijnen (Gelderland). Het zou natuurlijk wel voor de nodige logistieke problemen zorgen als de meer dan twaalf miljoen stemgerechtigden in Nederland zouden besluiten naar deze gemeenten te trekken om ouderwets te stemmen.

Literatuur

[1] NIST SP 800-30: Risk Management Guide for Information Technology Systems

[2] www.wijvertrouwenstemcomputersniet.nl c't