

Stemcomputer vraagt om fraude

Bart Jacobs

Recent is ophef ontstaan over stemcomputers. De actiegroep 'wij-vertrouwen-stemcomputers-niet' heeft op legale wijze de hand weten te leggen op stemcomputers van Nedap/Groenendaal en heeft de apparaten grondig geanalyseerd. De beveiliging bleek ondeugdelijk. De reactie vanuit de politiek richt zich vooral op het strakker controleren van de toegankelijkheid, via richtlijnen aan gemeentes en verzegeling van de apparaten.

De onderliggende beveiligingskwesties zijn echter volkomen genegeerd. Er zijn drie soorten problemen aan het licht gekomen.

1. De opslag en toegang tot stemcomputers zijn bar slecht geregeld. Iedereen die fysieke toegang krijgt tot een stemcomputer kan andere software installeren en daarmee de manier van tellen naar je hand zetten. Van deze kwetsbaarheid bleken maar weinigen zich bewust, getuige de opslag van 400 stemcomputers in een onbeveiligde loods in Rotterdam. De reactie van minister Nicolaï – en van verschillende Kamerleden en gemeenteraden – concentreert zich op dit punt: er moeten strakkere procedures en zegels op apparaten komen. Dat zal enigszins helpen, maar het blijft gerommel in de marge: een gemotiveerde aanvalser houdt je er niet mee tegen.

Moeten we eigenlijk wel met een aanval rekening houden? Verkiezingsfraude in Nederland? Hoe kan dat nou? We hebben echter ook een grote bouwfraude gehad, die onvoorstelbaar leek. Maar stel nu eens dat de PvdA zou meedelen dat zij de Nederlandse troepen uit Afghanistan terugtrekt wanneer zij aan de macht komt. Op dat moment krijgt de huidige nek-aan-nekrace een sterk internationale dimensie, en wordt de uitslag zeer relevant voor allerlei binnen- en buitenlandse krachten. Is verkiezingsfraude dan nog steeds onvoorstelbaar, zeker wanneer duidelijk is dat manipulatie van onze stemcomputers zo eenvoudig is?

2. De software in computers kan überhaupt vervangen worden. Dat is niet meer van deze tijd. Moderne computersystemen met kritische taken controleren eerst de integriteit van de programmatuur die ze gaan draaien, typisch via een elektronische handtekening. Dit is standaard in mobiele telefoons en spelcomputers. Maar niet in de Nedap stemcomputers waarvan

het ontwerp zo'n twintig jaar oud is. Zulke elementaire controlemechanismen van software krijg je niet meer toegevoegd in deze generatie stemcomputers. Naar hendaagse maatstaven zijn ze echter onontbeerlijk.

3. Het derde probleem betreft het stemgeheim, zoals vereist in de Kieswet. Dit punt heeft relatief weinig aandacht gekregen maar is misschien wel het ernstigste. De actiegroep heeft aangetoond dat op afstand informatie verkregen kan worden over de uitgebrachte stem.

Het display van de stemcomputer toont bij een stem op het CDA de volledige naam van deze partij in oude spelling, met een accent grave op de è in appel. Dit aparte teken vereist een speciale aansturing van het display waarvan de elektromagnetische straling tot op een meter of 25 herkend kan worden. Met wat meer moeite kunnen mogelijk ook stemmen op andere partijen op afstand herkend worden.

Dit fenomeen is bekend onder de naam 'tempest' en is een constante zorg in de militaire wereld. Het is verbazingwekkend dat de Nederlandse stemcomputers hierop niet gecontroleerd zijn. De gevolgen zijn namelijk groot, omdat via zulke elektronische lekkage in een stembureau van iedereen die een stem uitbrengt vastgesteld kan worden of die stem op het CDA is.

Dit is een principieel punt: je zou stemcomputers ook onder Saddam Hussein moeten durven gebruiken. Durft u dat? Het falen van het stemgeheim maakt stemcomputers strijdig met de Kieswet. Dit zal ongetwijfeld een grote rol spelen in de door de actiegroep aangekondigde rechtszaak. Ook deze lekkage krijg je niet meer goed met de huidige stemcomputers. Een extra zegeltje helpt hier echt niet tegen.

De conclusie is dan ook dat de huidige manier van stemmen met computers (technisch) kapot is en niet meer gerepareerd kan worden. Wat eind jaren tachtig een vooruitstrevend idee was, is nu niet meer verdedigbaar. Voortschrijdend inzicht in de aard en risico's van uitbesteding en automatisering van cruciale taken vraagt om een heroverweging.

Bart Jacobs is hoogleraar computerbeveiliging aan de universiteiten van Nijmegen en Eindhoven.