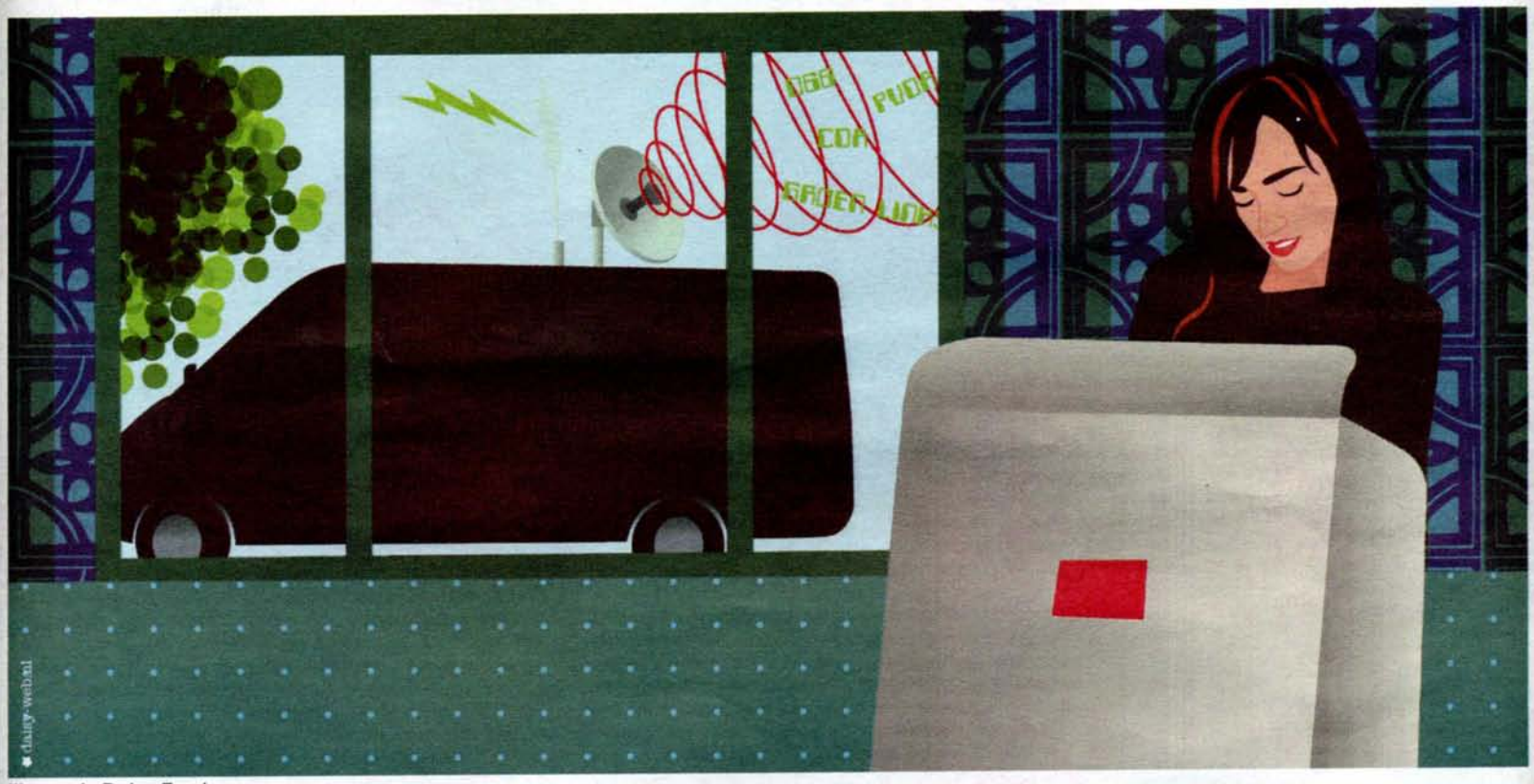

Illustratie Daisy Erades

Nieuwe risicosport: stemmen

Geen enkele garantie dat stemcomputer nu wel betrouwbaar is

▸ Het is goed mogelijk dat kiezers bij de Provinciale-Statenverkiezingen van 7 maart moeten stemmen met de NewVote-stemcomputers.

▸ Dat is een slechte zaak.

Door Jaap-Henk Hoepman

Volgens Bert Jongsma, directeur van Sdu-uitgevers, staat het ministerie van Binnenlandse Zaken en Koninkrijksrelaties op het punt de NewVote-stemcomputers weer toe te laten voor bij de Provinciale-Statenverkiezingen van 7 maart. Dat is een slecht vooruitzicht.

De NewVote-stemcomputers worden door Sdu Uitgevers ontwikkeld, en mochten bij de laatste Tweede-Kamerverkiezingen niet worden gebruikt, omdat het stemgeheim niet kon worden gegarandeerd. Door de straling van de computers zou een uitgebrachte stem op afstand te ontcijferen zijn. Volgens de AIVD, die de nieuwste versie heeft getest, zou deze versie de straling afdoende beperken. Deze tests zijn niet openbaar, en daarmee niet verifieerbaar. Met andere woorden: de kiesgerechtigde wordt geacht het oordeel van een min-of-meer geheime, en een zich deels aan de democratische controle onttrekkende, organisatie te vertrouwen, juist voor een proces dat aan de basis ligt van ons democratisch bestel. Dat is onverantwoord.

En dat is nog niet eens het belangrijkste bezwaar. De stemcomputers worden toegelaten zodra ze geen bedreiging voor het stemgeheim meer vormen. Nergens wordt echter uitgesproken of deze stemcomputers voldoen aan alle andere eisen voor een betrouwbare en controleerbare stemming.

En dat is nu juist, in het geval van de NewVote-stemcomputers, maar helemaal de vraag. De NewVote-stemcomputer is een omgebouwde, op Windows XP gebaseerde pc met een touchscreen, draadloze modem, en speciale verkiezingssoftware. Met andere woorden: een extreem gecompliceerd apparaat, waarvan de precieze werking door niemand ooit exact te controleren is. De aanwezigheid van een draadloze modem maakt het mogelijk dat hackers van buiten toegang zoeken of krijgen tot de stemcomputer zonder dat iemand daar iets van merkt.

Een besturingssysteem als Windows XP is zo complex dat daarin op allerlei plekken programmeerfouten te vinden zijn. Dit soort lekken kunnen worden gebruikt om toegang te krijgen tot de stemcomputer. Bovendien is de broncode – en daarmee de precieze werking – van Windows XP niet openbaar. Het is dus in principe mogelijk dat het systeem moedwillig aangebrachte zwakheden bevat om het stemproces te saboteren. Bijvoorbeeld om een stem op een bepaalde politieke partij niet of juist dubbel te tellen.

Ten slotte positioneert NewVote zich als een partij die graag alle zorgen voor de verkiezingen uit handen van de gemeente neemt, onder het motto: wij de verkiezingen, u de uitslag. Of, zoals op de website van NewVote wordt geschreven: 'Kies [...] voor het gemak van NewVote: Een complete dienstverlening voor een geslaagde verkiezingsdag.'

Het voorstellen van verkiezingen als een dienst die één organisatie aan de samenleving kan aanbieden, is een fundamenteel foute benadering. De verantwoordelijkheid en uitvoering van verkiezingen moet juist niet bij één organisatie worden gelegd. Hiervoor zijn meerdere, van elkaar onafhankelijke, partijen noodzakelijk, om zo de kans op fraude te verminderen.

De Nederlandse kiesgerechtigde mag hopen dat het ministerie op het laatste moment zal afzien van toelating van de NewVote-stemcomputer. Veilige verkiezingen draaien niet om het stemgeheim alleen. Net zo belangrijk zijn zaken als betrouwbaarheid, integriteit, transparantie en controleerbaarheid. Beter ten halve gekeerd dan ten hele gedwaald.

Jaap-Henk Hoepman is senior-onderzoeker security en cryptografie bij TNO ICT en de Radboud Universiteit Nijmegen.

Meer informatie over NewVote op www.newvote.nl. Meer over tegenstanders van de stemcomputers op – aan elkaar geschreven – www.wijvertrouwenstemcomputersniet.nl