Elektronisch stemmen: een auditperspectief

Ed Ridderbeekx

De kans is groot dat u afgelopen maart gebruik heeft gemaakt van uw democratisch recht om uw stem uit te brengen voor de vertegenwoordiging in de gemeenteraad van uw woonplaats. De kans is ook groot dat u daarvoor gebruik hebt gemaakt van een stemcomputer. Ongetwijfeld heeft u 's avonds of daags na de verkiezingen kennis genomen van de uitslag, al dan niet met vreugde. Maar hoe weet u nu dat de uitslag klopt? Hoe weet u dat uw stem inderdaad in de uitslag is meegenomen? En, hoe weet u dat uw stem in de uitslag is meegenomen *voor de partij en kandidaat waarop u veronderstelde te stemmen* toen u plaatsnam achter het bedieningspaneel van de stemcomputer en op het knopje van uw keuze drukte?

Drs. E.J.M. Ridderbeekx RE CISA is kiesgerechtigd Nederlands staatsburger. Hij werkt als IT Audit Manager bij Fortis, is lid van de redactiecommissie van 'de EDP Auditor', en schrijft op persoonlijke titel. Reacties kunnen naar ed@ridderbeekx.com.

Elektronisch stemmen is het proces waarbij, eenvoudig gezegd, kiezers met behulp van machines of computers hun stem uitbrengen en waarbij die machines en computers zorgen voor de registratie, de opslag, en de telling van de stemmen. De term 'elektronisch' geeft het speciale karakter van dit stemproces aan: het staat in contrast met de meer traditionele manier van stemmen, waarbij de kiezer zijn stem registreert op een stembiljet, een stembus dient voor de opslag van de stemmen, en de formulieren uiteindelijk handmatig worden geteld. Voor de goede orde: we hebben het in dit artikel over het stemmen als uitoefening van een democratisch recht door burgers. Dat kan gaan om zetels in het nationale parlement, de verkiezing van gemeenteraadsleden, of afgevaardigden voor Provinciale Staten; het kan ook gaan om het peilen van de mening van kiesgerechtigden over een schijnbaar eenvoudige 'ja/nee' vraag, zoals bij een referendum.

Over elektronisch stemmen is heel veel geschreven. Zowel op politiek niveau, in de dag- en weekbladpers (met name ten tijde van verkiezingen), maar ook in de meer wetenschappelijke literatuur van informatica en informatiebeveiliging is veel lezenswaardig materiaal te vinden. Het debat tussen voor- en tegenstanders is soms hevig. De discussie (waarop we, verderop in dit artikel, uitgebreid zullen terugkomen) komt er kort gezegd op neer dat de voorstanders de accuratesse, efficiency en flexibiliteit van de inzet van computers roemen, terwijl de tegenstanders beweren dat het inzetten van dergelijke elektronische middelen dusdanig grote risico's met zich meebrengt dat afbreuk wordt gedaan aan fundamentele democratische principes en burgerrechten. Ook de NOREA heeft zich in 2004 in de discussie gemengd bij monde van Adri de Bruijn in een artikel in de Automatisering Gids [BRUIJ04][1]. Enerzijds is dat bijzonder, want naar mijn weten zijn er tot op heden geen andere professionele audit-organisaties die zich hebben uitgesproken over de pro's en contra's van elektronisch stemmen. Anderzijds is het vanzelfsprekend dat er vanuit de IT-audit-professie aandacht is voor dit thema; als deskundigen bij uitstek in de problematiek rondom betrouwbaarheid van geautomatiseerde processen zouden we in staat moeten zijn een zinvolle bijdrage te leveren aan de discussies. In dit artikel zal ik dan ook, vanuit het perspectief van een auditor en met een soort 'audit textbook approach', een aantal betrouwbaarheidsaspecten van stemcomputers bespreken en uitleggen.

Belang van verkiezingen

Het recht (en in sommige landen: de plicht) om te kiezen, is een van de fundamenten van een democratie. Verkiezingen zijn een duidelijke belichaming van dit recht: burgers kiezen hun politieke vertegenwoordiging op verschillende bestuursniveaus (gemeenteraad, provincie, nationaal en Europees parlement) en hebben daarmee invloed op maatschappelijke keuzes die door hun vertegenwoordiging zullen worden gemaakt. In al deze gevallen geven burgers uiting aan hun keuze door te stemmen. Ieder[2] heeft een stem, alle stemmen tellen mee, en de uitslag van de stemming bepaalt hoe de burgers politiek zullen worden vertegenwoordigd. Zo wordt ervoor gezorgd dat ieders individuele stem van invloed is op de maatschappelijke keuzes die de gemeenschap als geheel maakt, volgens het principe 'de meeste stemmen hebben het meeste gewicht'.

Het is dus van het grootste belang dat het verkiezingsproces betrouwbaar is, ongeacht of computers daarbij een rol spelen of niet. Wat die betrouwbaarheid precies inhoudt, zullen we later zien; het volstaat op deze plaats om te onderstrepen dat de kiezer ervan op aan moet kunnen dat zijn stem meetelt. Als dat, om welke reden dan ook, niet kan worden gegarandeerd en bewerkstelligd, dan zal ontoelaatbaar afbreuk worden gedaan aan de legitimiteit van de verkiezingsuitkomsten (bijvoorbeeld de zetelverdeling in de Tweede Kamer) en de legitimiteit van de politieke keuzes die daaruit voortkomen (bijvoorbeeld een nieuwe wetgeving). Onbetrouwbare verkiezingen zijn een zaag aan de stoelpoten van de democratie.
Essentieel is evenzeer dat de kiezers *vertrouwen* hebben in het verkiezingsproces. Ontbreekt het daaraan, dan zal dat ongewenste maatschappelijke consequenties kunnen hebben, variërend van een lage verkiezingsopkomst ('mijn stem telt toch niet mee') tot sociale onrust ('de president moet worden afgezet want hij is niet op een eerlijke manier gekozen, op de barricades!'). Een betrouwbaar proces en vertrouwen in dat proces zijn op een interessante manier aan elkaar gerelateerd. Je zou kunnen zeggen dat een betrouwbaar verkiezingsproces niet garandeert dat de burgers ook vertrouwen in dat proces zullen hebben, maar dat een onbetrouwbaar verkiezingsproces in ieder geval het vertrouwen van de kiezers zal ondermijnen. Betrouwbaarheid is een kwaliteit, die is geïncorporeerd in het ontwerp en de implementatie van het proces. Het is een inherente eigenschap, die tot op zekere hoogte kan worden geobjectiveerd, gemeten en aangetoond. Vertrouwen ligt aan de kant van de 'gebruiker' van een proces, en heeft te maken met de perceptie die de gebruiker heeft over de kwaliteit van het proces.

Vanwege hun grote belang zijn verkiezingen (en de gang van zaken rondom verkiezingen) in democratieën doorgaans verankerd in de wet (in Nederland in de Kieswet [KIES05] en, aanvullend, in het Kiesbesluit [KIES04]), en is het de verantwoordelijkheid van de overheid om de burgers niet alleen een betrouwbaar verkiezingsproces te bieden, maar ook al het mogelijke te doen om het vertrouwen van de burgers in de betrouwbaarheid van dat proces te winnen en te behouden.

Binnen een Nederlandse context kan het ter sprake brengen van betrouwbaarheid en vertrouwen mogelijk als onnodig of zelfs triviaal worden gevoeld. We leven in een relatief stabiele maatschappelijke omgeving, met een robuuste traditie als het gaat om democratie en vrijheid van meningsuiting. Politici zullen zich in Nederland waarschijnlijk eerder neerleggen bij een smadelijke verkiezingsnederlaag dan dat ze het in hun hoofd zullen halen het verkiezingsproces op een illegale manier in hun voordeel te beïnvloeden. En in Nederland ben je relatief veilig als je de buurman machtigt voor jou te stemmen. Dat is niet overal zo. Het is, bij het lezen van het vervolg van het artikel, goed om te bedenken dat verkiezingen ook worden gehouden in landen waar politieke groeperingen opereren die weinig scrupules hebben om democratische mechanismen (zoals een verkiezing) te manipuleren, om zo schijnbaar legitiem een machtspositie te verkrijgen of te behouden, en waar het onthullen van je politieke voorkeur aan de buurman je duur kan komen te staan. Juist in zulke omstandigheden wordt het belang van betrouwbaarheid van het verkiezingsproces en van het vertrouwen van het electoraat het meest duidelijk. Afgezien van deze 'regionale' verschillen hebben we dan mondiaal ook nog te maken met groeperingen die belang denken te hebben bij het verstoren van democratische en politieke stabiliteit. Voor deze lieden kunnen verkiezingen een heel dankbaar doelwit zijn.

Een generieke beschrijving en afbakening van elektronisch stemmen

In het voorgaande is de maatschappelijke betekenis van verkiezingen aan de orde gesteld. In deze paragraaf zullen we ingaan op elektronisch stemmen, en het thema op een zinvolle manier afbakenen ten behoeve van het verdere verloop van het artikel.

Het verkiezingsproces als geheel is tamelijk breed. Het begint bij de registratie van kiesgerechtigden, en eindigt met het vaststellen van de verkiezingsuitslag. In een rapport van Het Expertise Centrum (HEC) is een bruikbaar procesmodel opgenomen, dat aan de basis ligt van onderstaande bespreking [HEC00]. Met *stemmen* wordt in dit artikel gedoeld op een aantal onderdelen van het verkiezingsproces, te weten:

- De stemuitbrenging door een kiesgerechtigde
- De stemopneming
- Het verwerken van de stemtotalen

Zaken als de stemoproep, het vaststellen van de kiesgerechtigdheid van een kiezer, en de registratie van politieke groeperingen vallen buiten de scope van dit artikel, alhoewel ze deel uitmaken van het bredere verkiezingsproces. Er wordt

van een situatie uitgegaan, waarin de kiezer zijn stem uitbrengt in een stemlokaal waar stemcomputers staan opgesteld. De situatie waarbij de kiezer op afstand, bijvoorbeeld per telefoon of per internet, zijn stem uitbrengt, brengt een additionele problematiek met zich mee (zie onder andere [HEC00]) die in dit artikel niet aan de orde wordt gesteld. Van elektronisch stemmen is sprake als geautomatiseerde hulpmiddelen worden ingezet bij elk van de bovengenoemde drie onderdelen. De rol die geautomatiseerde hulpmiddelen daarbij zouden kunnen spelen, is als volgt te omschrijven:

Stemuitbrenging

Dit is de fase waarin de kiezer zijn stem uitbrengt. Een stemcomputer draagt zorg voor de dialoog met de kiezer. Deze maakt zijn keuze door het indrukken van een knopje op een paneel of het aanraken van een *touch screen*. De stemcomputer presenteert de gemaakte keuze ter validatie aan de kiezer, die hier nog een correctiemogelijkheid heeft. Nadat de kiezer zijn keuze heeft bevestigd, is er een confirmatie van de stemcomputer dat de kiezer daadwerkelijk heeft gestemd, en wordt de stem elektronisch door de computer geregistreerd.

Stemopneming

Nadat de termijn voor het uitbrengen van de stemmen is verlopen (bij sluiting van het stemlokaal) draait de stemcomputer een lijst uit met de stemtotalen per kandidaat, op basis van de gegevens die in zijn geheugen zijn opgeslagen. Die lijst wordt, samen met het geheugen, naar een verzamelpunt (bijvoorbeeld op gemeentelijk niveau) gebracht ter verdere verwerking.

Verwerken van de stemtotalen

De geheugens van de stemcomputers worden (mogelijk in een iteratief proces) op een centrale plaats opnieuw met behulp van geautomatiseerde apparatuur uitgelezen en de stemtotalen worden bepaald.

Stemcomputers

In de vorige paragraaf is slechts in zeer algemene zin de gang van zaken bij elektronisch stemmen uit de doeken gedaan. De exacte en specifieke werkwijze bij een stemproces met computers is sterk afhankelijk van de procedurele specificaties en de gebruikte stemcomputers. In dit artikel wordt uitgegaan van stemcomputers van het type dat in de Angelsaksische literatuur wordt aangeduid als *Direct Recording Electronic* ofwel DRE. Kenmerkend hierbij is dat een uitgebrachte stem direct elektronisch wordt opgeslagen; dit in tegenstelling tot bijvoorbeeld de ponskaartsystemen die tot zoveel commotie leidden bij de Amerikaanse presidentsverkiezingen in 2000. Daarbij werd een stem uitgebracht door het ponsen van een gaatje in een kaart; die kaarten werden vervolgens geautomatiseerd gelezen (voorzover dat mogelijk was). In feite was hier dus sprake van *computer assisted counting*. Een DRE heeft deze 'fysieke' tussenstap niet.

Er kunnen drie typen DREs worden onderscheiden [FISC03]. Bij het eerste type is het bedieningspaneel een één-op-één weergave van het oude, vertrouwde stembiljet. Alle lijsten, partijen, en namen van kandidaten zijn zichtbaar. Naast de naam van iedere kandidaat bevindt zich een knopje; indrukken van dat knopje activeert een schakeling die een lampje laat branden of de naam van de betreffende kandidaat op een display laat zien. De kiezer kan vervolgens de stem daadwerkelijk uitbrengen door het indrukken van een 'stemknop', of kan desgewenst zijn keuze nog corrigeren.
Bij een tweede type wordt de inhoud van het stembiljet op een computerscherm weergegeven (meestal op meerdere pagina's). Met behulp van navigatiemiddelen op het toetsenbord (pijltjes, de entertoets) baant de kiezer zich een weg door het virtuele biljet en maakt zijn keuze. Bij een derde type is de toetsenbordnavigatie vervangen door een touch screen.
Aangezien de problematiek die gemoeid is met het gebruik van deze typen machines, met name verschilt in de *user interface,* maar voor het overige vergelijkbaar is, zal in het vervolg van het artikel geen onderscheid worden gemaakt tussen deze typen. Als de term stemcomputer wordt gebruikt, wordt gedoeld op DREs in zijn algemeenheid.

Problematiek van elektronisch stemmen

Waar spitst de discussie rondom stemcomputers zich nu precies op toe? Op het eerste gezicht lijkt het dat we van doen hebben met een eenvoudig te automatiseren proces. Het bouwen van een dialoogje met de kiezer, het registeren van een druk op de knop of een aanraking van het scherm, het opslaan daarvan, en vervolgens een triviale sommering om een totaal te bepalen, dat alles levert schijnbaar geen al te grote uitdaging op voor goede systeemontwikkelaars en programmeurs. Bij nadere beschouwing blijkt echter dat het proces complexe karakteristieken krijgt doordat er strakke eisen aan gesteld worden die - omdat ze vaak geworteld zijn in democratische principes en fundamentele rechten van burgers - nauwelijks ruimte voor keuzes overlaten en niet persé gemakkelijk realiseerbaar zijn in een geautomatiseerde omgeving.

Hét centrale probleem bij elektronisch stemmen, is dat de kiezer geen manier heeft om vast te stellen dat zijn stem wordt geregistreerd zoals hij die heeft uitgebracht en dat zijn stem bij de verwerking van de stemtotalen wordt meegenomen. Weliswaar bevestigt de stemcomputer de keuze van de kiezer en moet de kiezer die keuze bevestigen, maar vervolgens verlaat de kiezer het stemhokje en moet hij er gewoon op vertrouwen dat de stemcomputer en het proces daaromheen betrouwbaar is, en dat de geautomatiseerde verwerking van de stemtotalen op een goede manier gebeurt. Zijn uitgebrachte stem is op dat moment niet anders dan een digitale representatie in het geheugen van de stemcomputer, en de kiezer heeft geen bewijs van hoe hij heeft gestemd, en zelfs al had hij dat wel, hij heeft geen mogelijk-

heden om vast te stellen dat zijn stem uiteindelijk op een juiste manier in de uitslag is verwerkt.

Laten we eens een vergelijking maken met het gebruik van een geldautomaat. Er zijn weinig mensen die nog aarzeling zullen voelen om 'hun geld uit de muur te halen'; het vertrouwen in een juiste afhandeling van de transactie door de achterliggende geautomatiseerde systemen is blijkbaar groot. Dat komt niet in de laatste plaats doordat een transactie bij een geldautomaat goed controleerbaar is (en dat is, althans voor velen, een essentieel verschil met het gebruik van stemcomputers). Degene die pint, kan onmiddellijk vaststellen dat het opgevraagde bedrag inderdaad wordt uitgekeerd, en op verzoek print de automaat een transactiebewijs. En later kan de pinner met zijn dagafschrift vaststellen dat het juiste bedrag van zijn rekening is afgeschreven. Doen zich eventuele fouten voor, dan kan hij altijd nog naar de bank om te reclameren. Dit zijn allemaal maatregelen die een kiezer bij elektronisch stemmen ontbeert. Er is geen 'ontvangstbewijs' voor de uitgebrachte stem. Er is geen latere terugmelding die bevestigt dat de uitgebrachte stem op een juiste manier is meegeteld. En er is dus ook geen mogelijkheid van reclamatie, afgezien van klachten over onregelmatigheden in het stembureau en dergelijke.

Dit legt tevens de nadruk op de kwaliteit van de geautomatiseerde componenten in het elektronisch stemproces. Stel je eens voor dat iemand in staat is geweest de software van de stemcomputers zodanig te manipuleren dat die weliswaar een nette dialoog met de kiezer aangaat, maar in werkelijkheid een heel andere stem registreert dan de kiezer dacht uit te brengen. Zonder aanvullende maatregelen blijft dit onopgemerkt en zal het (indien het op grote schaal plaatsvindt) een desastreuze uitwerking kunnen hebben op een goed verloop van de verkiezingen.

Is dit essentieel anders dan bij het traditionele stemmen met stemformulieren? Tot op zekere hoogte wel. Bij het gebruik van stembiljetten kan de kiezer zelf vaststellen dat hij het juiste cirkeltje met potlood heeft aangekruist. Hij deponeert het biljet zelf in een stembus. Mits de integriteit van de stembus kan worden gegarandeerd (bijvoorbeeld met verzegeling en direct toezicht door de aanwezige stemcommissie), kan hij ervan op aan dat de stemuitbrenging naar behoren is verlopen. De kiezer kan vervolgens desgewenst (althans in Nederland) aanwezig zijn bij de telling van de stemmen na het sluiten van het stembureau. Die telling gebeurt handmatig door de leden van het stembureau, al dan niet in de aanwezigheid van waarnemers. De kiezer zou kunnen vaststellen dat het opgemaakte proces-verbaal overeenstemt met de telling, en zo een bepaalde mate van zekerheid kunnen krijgen over de vraag of zijn stem goed is meegeteld. Van volledige zekerheid kan echter slechts sprake zijn onder specifieke omstandigheden of bij verkiezingen op zeer kleine schaal [FISC03].

Stanton [STAN00] geeft een interessante kijk op deze problematiek in het perspectief van Braziliaanse verkiezingen. Hij stelt in grote lijnen dat identificatie van de kiezer, stemuitbrenging, stemopneming, en bepaling van de resultaten in een traditionele, handmatige setting afzonderlijke processen zijn, die afzonderlijk kunnen worden geobserveerd en gecontroleerd (door leden van het stembureau, door kiezers, en door waarnemers). Bij elektronisch stemmen zijn deze procesonderdelen als het ware samengevoegd in de stemcomputer, en zijn ze onttrokken aan directe observatie en controle[3].
Dit inherente gebrek aan controleerbaarheid van elektronisch stemmen laat sommigen koud, maakt velen bezorgd, en transformeert enkelen tot verklaarde tegenstanders van elektronisch stemmen. De eerste groep ziet vooral voordelen bij het gebruik van stemcomputers: hun flexibiliteit en gebruiksgemak, de besparingen op papier, en vooral de vermeende snellere resultaatbepaling worden dan genoemd. Ook gebruiken de voorstanders het argument dat traditionele verkiezingen evenmin controleerbaar zijn. Tegenstanders eisen aanvullende maatregelen die de transparantie van het proces moeten vergroten, of zijn principieel tegen het gebruik van stemcomputers.

Laten we het eens vanuit een auditperspectief bekijken. Ongeacht of we de individuele kiezer of de maatschappij als geheel als gebruiker ('user') van stemcomputers beschouwen, de onmogelijkheid voor die gebruiker om vast te stellen dat stemmen goed worden geregistreerd, verwerkt, en geteld, duidt in de oren van een auditor op een gebrek aan *user controls*:

'(…) there are essential controls on the automation environment that can only be carried out by the user. For example, only the user can control the completeness and correctness of the output. The user needs to be able to control the effectiveness of the functionality of the automation environment.' [BIEN96]

Toepassing van deze stellingen van Van Biene op een geautomatiseerd stemsysteem lijkt te duiden op een serieus probleem. Dat is op zichzelf al reden genoeg om wat dieper in te zoomen op een aantal vragen dat een auditor niet vreemd is. Welke eisen moeten eigenlijk aan een stemproces worden gesteld? En welke waarborgen zijn er (c.q. ontbreken er) bij elektronisch stemmen? Tot welke kwetsbaarheden leidt dit? Welke bedreigingen zijn er voor een betrouwbaar elektronisch stemproces, en welke impact kunnen deze bedreigingen hebben? Op deze vragen zal in de volgende paragrafen een antwoord worden gegeven.

Kwaliteitseisen bij stemcomputers

We hebben tot dusver gezien dat we bij elektronisch stemmen te maken hebben met een uiterst belangrijk proces, dat echter een aantal essentiële maatregelen lijkt te ontberen om de betrouwbaarheid daarvan vast te kunnen stellen. In deze

paragraaf wordt dieper ingegaan op de eisen die aan stemmen in het algemeen, en aan elektronisch stemmen in het bijzonder, moeten worden gesteld.
Een blik op de vele publicaties over elektronisch stemmen laat verschillende rubriceringen zien van eisen die aan verkiezingen en stemmen moeten worden gesteld (zie bijvoorbeeld [CRAN96] of [NEUM93]). Deze verschillen inhoudelijk en in de kern niet bijzonder veel. In het onderstaande hanteer ik de 'Zes Geboden' van Shamos [SHAM93], hier letterlijk geciteerd:

I. Thou shalt keep each voter's choices an inviolable secret.
II. Thou shalt allow each eligible voter to vote only once, and only for those offices for which she is authorized to cast a vote.
III. Thou shalt not permit tampering with thy voting system, nor the exchange of gold for votes.
IV. Thou shalt report all votes accurately.
V. Thy voting system shall remain operable throughout each election.
VI. Thou shalt keep an audit trail to detect sins against Commandments II-IV, but thy audit trail shall not violate Commandment I.

Een korte verklaring van deze enigszins luchtig geformuleerde, maar serieus bedoelde eisen is op zijn plaats. Gebod I heeft alles te maken met het *stemgeheim*. Op geen enkele wijze mag een uitgebrachte, geregistreerde, of getelde stem terug te voeren zijn op een individuele kiezer. Dat is niet verwonderlijk en we zijn allemaal gewend aan de privacy van het stemhokjesgordijn. Maar er zit een tweede dimensie aan het stemgeheim die minder voor de hand liggend is, en die tot uitdrukking wordt gebracht in het tweede deel van Gebod III (waar gesproken wordt over 'exchange of gold for votes'). Er wordt wel beweerd dat het winnen van verkiezingen het goedkoopst te bereiken zou zijn door stemmen van kiezers te kopen; dit is, met de enorme bedragen die anderszins aan campagnes zouden worden uitgegeven, niet zo onvoorstelbaar als het lijkt. Om tegen te gaan dat kiezers worden '(om)gekocht' om hun stem op een bepaalde partij uit te brengen, dient de kiezer van zijn uitgebrachte stem geen enkel bewijs te kunnen geven. Het is vanwege deze eis, dat aan een kiezer geen 'ontvangstbewijs' of 'kwitantie' van zijn stem kan worden verstrekt. Dit zou hem immers in staat stellen aan de omkopende partij te bewijzen, dat hij geleverd heeft waarvoor hij betaald werd. Dit bewijs ontbreekt nu. We zullen zien dat dit voor de controleerbaarheid van het stemproces belangrijke consequenties heeft.

Gebod II geeft aan dat iedere kiezer slechts éénmaal mag stemmen, en alleen voor de verkiezingen waarvoor de kiezer geregistreerd is. Met deze eis wordt aangegeven dat maatregelen moeten worden getroffen om te voorkomen dat op een of andere wijze extra (ongeautoriseerde) stemmen worden meegeteld (in het Engels aangeduid met de term *ballot stuffing*). Dit is nog het best voorstelbaar in de traditionele situatie, waarbij bijvoorbeeld de kiezer per ongeluk twee stembiljetten krijgt uitgereikt en deze beide in de stembus deponeert.

In Gebod III (deel 1) wordt aangegeven dat het stemsysteem (hoe dat er ook uitziet, geautomatiseerd of niet) niet mag worden beïnvloed, of, als we de term 'tampering' wat strakker vertalen, niet *ongeautoriseerd* mag worden beïnvloed. Er moeten dus maatregelen worden getroffen die waarborgen dat het stemsysteem gedurende het gehele proces robuust is en dat manipulatie van gegevens, procedures, mensen, en (indien van toepassing) programmatuur onmogelijk is.

Gebod IV legt een verband tussen de door de kiezers uitgebrachte stemmen en het uiteindelijke resultaat van de verkiezing. Het gebod stelt, dat alle uitgebrachte stemmen op een juiste manier in de bepaling van het uiteindelijke resultaat moeten worden meegenomen en gerapporteerd.

In Gebod V zijn beschikbaarheidsaspecten geïncorporeerd. Het stemsysteem moet gedurende de verkiezing operationeel zijn. Zou dat niet of onvoldoende het geval zijn, dan bestaat het risico dat kiezers hun stemrecht niet kunnen uitoefenen, waardoor (als er sprake is van beschikbaarheidsproblemen op grote schaal) de uitslag van de verkiezingen geen goed beeld geeft van de mening van het electoraat. Maar zelfs op kleine schaal zouden beschikbaarheidsproblemen er snel toe kunnen leiden dat kiezers hun vertrouwen in het stemsysteem verliezen.

In Gebod VI vinden we een term die in onze beroepsgroep wel meer gehanteerd wordt: de *audit trail*. Shamos stelt dat deze voor handen moet zijn om overtredingen tegen geboden II tot en met IV te detecteren, echter zonder het stemgeheim geweld aan te doen[4].

Shamos' geboden zijn kernachtig en doen ter zake. Bij nadere beschouwing hebben ze alle te maken met het kwaliteitsaspect dat auditors onder de noemer 'betrouwbaarheid' brengen. In het navolgende tabelletje zijn de Geboden afgezet tegen de kwaliteitsattributen van betrouwbaarheid [SUER02] zoals auditors die kennen.

In publicaties over elektronisch stemmen ziet men weinig discussie over de validiteit van Geboden I tot en met V (alhoewel over de te treffen maatregelen wel degelijk onenigheid bestaat, waarover later meer). Over Gebod VI, de controleerbaarheid, wordt echter wel gediscussieerd. Sommigen pleiten hier voor controleerbaarheid in enge zin, zoals Shamos dat ook doet; het systeem dient te voorzien in maatregelen om het 'niet voldoen aan een aantal andere eisen' te kunnen detecteren. Een simpel voorbeeld van zo'n maatregel is het aansluiten van het totaal aantal ingeleverde oproepingskaarten met het aantal uitgebrachte stemmen per stemlokaal. Als deze totalen niet overeenstemmen, kan dat duiden

Gebod	Omschrijving	Kwaliteitsattribuut
I	Thou shalt keep each voter's choices an inviolable secret.	Exclusiviteit
II	Thou shalt allow each eligible voter to vote only once, and only for those offices for which she is authorized to cast a vote.	Volledigheid
III	Thou shalt not permit tampering with thy voting system, nor the exchange of gold for votes.	Exclusiviteit
IV	Thou shalt report all votes accurately.	Juistheid
V	Thy voting system shall remain operable throughout each election.	Volledigheid[1]
VI	Thou shalt keep an audit trail to detect sins against Commandments II-IV, but thy audit trail shall not violate Commandment I	Controleerbaarheid

1 Natuurlijk stelt dit gebod ook eisen op het gebied van het kwaliteitsaspect 'continuïteit', met attributen als 'bedrijfszekerheid', 'robuustheid', en 'herstelbaarheid'. Het artikel beperkt zich echter tot het kwaliteitsaspect 'betrouwbaarheid'.

op ballot stuffing (Gebod II) of manipulatie van het stemsysteem (Gebod III). Anderen pleiten voor een ruimere definitie van controleerbaarheid die de nadruk legt op een meer actieve en voor iedereen hanteerbare verificatiemogelijkheid van de betrouwbaarheid. HEC heeft bijvoorbeeld, in zijn publicatie *Stemmen op afstand* [HEC00], een analyse gemaakt van de eisen die de Nederlandse kieswet inherent aan het stemproces stelt en noemt dan als aanvullende eis onder het kopje 'Verificatie':

'Iedereen dient in staat te zijn onafhankelijk en eenduidig vast te stellen dat alle uitgebrachte stemmen correct zijn geteld (controleren achteraf van de accuratesse).'

HEC baseert zich hierbij op Cranor [CRAN96], die een gelijkluidende verifieerbaarheidseis formuleert, en die verder stelt:

'A weaker definition of verifiability used by some authors allows that a system is verifiable if it allows voters to verify their own votes and correct any mistakes they might find without sacrificing privacy. Less verifiable systems might allow mistakes to be pointed out - but not corrected - or might allow verification of the process by party representatives but not by individual voters.'

Fischer [FISC03] brengt een verdere nuance aan en spreekt van twee soorten verifieerbaarheid. Op de eerste plaats is dat *voter verifiability*: de mogelijkheid van de kiezer om vast te stellen dat zijn stem is geregistreerd volgens de intentie die hij had bij het uitbrengen van die stem. Op de tweede plaats is er *results verifiability*, het vermogen van kiezers om vast te stellen dat in het uiteindelijke totaalresultaat alle door de kiezers uitgebrachte stemmen zijn meegeteld, en dat (dus) geen stemmen zijn verwijderd, toegevoegd of gewijzigd.
Deze verschillende interpretaties van controleerbaarheid en verificatie maken duidelijk dat hier belangrijke nuances spelen. Er spelen twee vragen: *wat* moet kunnen worden gecontroleerd, en *wie* moet die controle kunnen uitvoeren? Welbeschouwd is de eis die HEC formuleert wellicht terecht, maar in de praktijk is het ondenkbaar dat een burger zou kunnen vaststellen dat, bijvoorbeeld bij Tweede-Kamerverkiezingen, 'alle uitgebrachte stemmen correct zijn geteld', alleen al vanwege de schaalgrootte van die verkiezingen. Het lijkt erop dat die eis veel meer moet worden geïnterpreteerd als een soort morele verplichting aan de 'ontwerpers' van een verkiezingsproces: zij moeten voldoende transparantie en verificatiemogelijkheden in dat proces inbouwen en het bestaan van betrouwbaarheidsmaatregelen ook actief aantonen. Een dergelijke transparantie moet ervoor zorgen dat de burger, alhoewel hem de mogelijkheid ontbreekt, het *gehele* proces *en detail* te controleren, voldoende vertrouwen krijgt in het betrouwbaar verloop van het elektronisch stemmen. Dit zou, als een aanvullend Gebod, als volgt geformuleerd kunnen worden:

VII. Thou shalt provide thy voters with sufficient proof that design and operation of thy voting system honours Commandments I –VI.

Hiermee breiden we de door Shamos ietwat passief geformuleerde eis van een audit trail (als repressieve controle) uit naar een meer actieve verplichting om aantoonbaar te maken dat voldoende maatregelen zijn genomen om een betrouwbaar elektronisch stemproces te garanderen.

Bedreigingen bij elektronisch stemmen

In [SUER02] worden bedreigingen gedefinieerd als 'negatief geformuleerde kwaliteitseisen'. Als we dat ook toepassen op de bovenstaande kwaliteitsattributen, resulteren de volgende bedreigingen voor elektronisch stemmen:

a. doorbreking van het stemgeheim (exclusiviteit)
b. ongeautoriseerde uitgebrachte stemmen (volledigheid)

c. ongeautoriseerde beïnvloeding van het stemsysteem (exclusiviteit)
d. onjuiste resultaatbepaling (juistheid)
e. onbeschikbaarheid van het stemsysteem (volledigheid)
f. onvoldoende functionerende audit trail (controleerbaarheid)
g. onvoldoende bewijs van een solide ontwerp en werking van het stemsysteem voor de kiezers (controleerbaarheid/aantoonbaarheid)

Zonder dit hier te bewijzen, zou ik durven stellen dat de kans dat één of meerdere van deze bedreigingen zich voordoet, groter is dan nul. Volgens de theorie hebben we hier dan te maken met reële *risico's*. Indien we kijken naar de *impact* die deze risico's hebben, dan kunnen die als volgt worden benoemd:

1. een verkiezingsuitslag die niet in overeenstemming is met de door de kiezers uitgebrachte stemmen (denk aan het risico van slecht functionerende of frauduleuze programmatuur in de stemcomputers)
2. het verlies van vertrouwen van burgers in een betrouwbaar verkiezingsproces (denk aan het risico van het ontbreken van voldoende transparantie)
3. het schenden van fundamentele rechten van burgers (denk aan het risico van doorbreking van het stemgeheim).

Het is onnodig te zeggen dat dit zeer ongewenste gevolgen zijn. De beelden van de heisa rond het bepalen van de uitslag van de Amerikaanse presidentsverkiezingen in de staat Florida in 2000 staat velen nog op het netvlies; er was gerede twijfel over de juistheid van de uitslag (impact 1), wat leidde tot een ernstige crisis in de fiducie van burgers in hun eigen democratisch bestel (impact 2). Het is duidelijk dat de maatschappij hier een zware verplichting heeft om maatregelen te nemen die deze bedreigingen voldoende indammen.

In onderstaande tabel is de relatie tussen risico's en impact eenvoudig samengevat.

Eerder in dit artikel is al aangestipt dat de belangen bij verkiezingen groot zijn. Ze gaan immers altijd - in enige vorm - om wie het voor het zeggen heeft, om macht. En dat betekent dat de betrokken partijen invloed zullen uitoefenen op het verkiezingsproces. Dat kan op een legitieme manier, bijvoorbeeld door het voeren van campagne. Het kan ook op een onwettige wijze; mondiaal zijn er helaas voorbeelden te over van verkiezingsfraude op kleinere of grotere schaal. We spreken dan over de dreiging van een ongeautoriseerde beïnvloeding van het resultaat van verkiezingen, zodanig dat dat - mogelijk in tegenstelling tot de werkelijke wens van het electoraat - in het voordeel is van een bepaalde kandidaat, partij, of denkbeeld. Van alle denkbare bedreigingen zoals hierboven genoemd, lijkt dit de meest ernstige, omdat daarmee rechtstreeks de doelstelling van het verkiezingsproces in gevaar wordt gebracht: het vaststellen van de wil van het electoraat. Hierbij moet wel worden opgemerkt, dat voor een succesvolle 'aanval' op de verkiezingsuitslag twee factoren zeer belangrijk zijn, namelijk *schaal* en *competitie*. Het is onwaarschijnlijk dat een enkele ongeautoriseerde stem een bepalende invloed zal hebben op de uitslag van verkiezingen; daarvoor is een beïnvloeding op grotere schaal nodig. Echter, hoe meer er sprake is van een nek-aan-nek race tussen kandidaten of partijen (competitie), hoe minder frauduleuze acties nodig zijn om de uitslag beslissend te beïnvloeden [FISC03][5].
Voorts wordt er in de publicaties over elektronisch stemmen ook wel op gewezen dat er groeperingen zijn die belang hebben bij aanvallen op het democratisch bestel (te denken valt aan terroristische groeperingen). Deze zijn wellicht niet zozeer uit op het gericht beïnvloeden van een verkiezingsuitslag, als wel op het ondermijnen van het vertrouwen van burgers in hun regering en het creëren van maatschappelijke onrust, bijvoorbeeld door pogingen tot sabotage van het verkiezingsproces.

Risico	Impact		
	1	2	3
a. doorbreking van het stemgeheim		X	X
b. ongeautoriseerde uitgebrachte stemmen	X	X	
c. ongeautoriseerde beïnvloeding van het stemsysteem	X	X	
d. onjuiste resultaatbepaling	X	X	
e. onbeschikbaarheid van het stemsysteem	X	X	X
f. onvoldoende functionerende audit trail	X	X	
g. onvoldoende bewijs van een solide ontwerp en werking van het stemsysteem	X	X	

Kwetsbaarheden van elektronisch stemmen en te treffen maatregelen

Het elektronisch stemproces zoals eerder beschreven, is een geautomatiseerd systeem. Met geautomatiseerde systemen doen zich nu eenmaal betrouwbaarheidsproblemen voor, als IT-auditors weten we dat als geen ander. Sterker nog, we danken ons bestaansrecht daaraan. Geautomatiseerde systemen kunnen slecht functioneren omdat ze belabberd ontworpen zijn, onvoldoende zijn getest of omdat ze niet gebruikersvriendelijk zijn. Als gevolg daarvan kunnen ze kwetsbaarheden bevatten die met opzet door derden worden uitgebuit. Voor elektronische stemsystemen is dat niet anders; onvoldoende kwaliteit maakt ze kwetsbaar voor beïnvloeding - al dan niet gericht - van hun betrouwbaar functioneren.
De stemcomputers spelen in de discussie rondom kwetsbaarheden een centrale rol. In een elektronisch stemproces zorgen zij immers voor de stemopname, de stemregistratie, en de telling van stemmen. Rubin, die (samen met een aantal collega's) in een veelbesproken artikel ernstige beveiligingsproblemen meldde op basis van onderzoek van een in de VS veel gebruikt type stemcomputer [KOHN04], vat het kernachtig samen:

'My greatest concern with paperless DREs is that whoever makes the machines has the capacity to rig election results however they like.' [RUBI]

In de navolgende subparagrafen worden enkele belangrijke kwetsbaarheden van elektronisch stemmen nader toegelicht. Doelstelling daarbij is niet zozeer volledigheid, maar het noemen van de meest in het oog springende aspecten. Dit zal gebeuren aan de hand van het volgende citaat van Mercuri [MERC02]:

'Since it is, in principle, impossible to verify that a computational device is free from programming errors or nefarious code, no electronic voting system can be verified for 100 percent accuracy, reliability, and integrity. It is also, in principle, impossible for a computational device to provide full fail-safe internal verification, hence any ballot audit produced from self-stored data could reflect errors or manipulation that occurred between the time the voter cast their ballot and the time the ballot was recorded. Errors and manipulation of ballots can also occur if data is transmitted between devices or over networks. It is essential, therefore, that each voter provide an independent check of their ballot at the time of voting, using human-readable media as the manual audit capacity for the voting system.'

In deze stelling worden drie aspecten van elektronisch stemmen genoemd die we achtereenvolgens bespreken:

- Software
- Netwerkverbindingen
- Audit trail

Ter afsluiting van de paragraaf zal tevens kort iets worden opgemerkt over de procedurele en de menselijke factor in een geautomatiseerd stemproces.

Bij ieder onderdeel wordt een korte inschatting gemaakt van de maatregelen die een IT-auditor ten aanzien van deze aspecten zou (kunnen) eisen of adviseren, niet zozeer om een volledig controleprogram voor elektronisch stemmen samen te stellen, maar om het audit perspectief te benadrukken. Ik heb daarbij het scenario in gedachte gehad dat u als IT-auditor door de Europese Unie wordt gevraagd als waarnemer aanwezig te zijn bij de parlementsverkiezingen in een ver land met een jonge en nog kwetsbare democratie, waarbij op grote schaal stemcomputers worden gebruikt. Men vraagt u op basis van uw expertise en ervaring met betrouwbaarheidsaspecten van geautomatiseerde systemen te beoordelen of voldoende maatregelen zijn getroffen om een betrouwbaar elektronisch stemproces te garanderen. Welke overwegingen zou u dan maken?

Software

De programmatuur van stemcomputers vervult een cruciale rol. De functionaliteit van de machines wordt er hoofdzakelijk door bepaald. In algemene zin zorgt de software voor de dialoog met de kiezer, de registratie en opslag van de stemmen, en de telling van de geregistreerde en opgeslagen stemmen. In termen van de in de vorige paragraaf genoemde eisen moeten we bovendien op de programmatuur steunen voor de realisatie van een aantal doelstellingen; ze moet zorgen voor:

- Een gebruikersvriendelijke dialoog met de kiezer;
- Registratie van (alle) stemmen zoals uitgebracht door de kiezer;
- Opslag van stemmen op een zodanige wijze dat de identiteit van de stemmer niet kan worden herleid;
- Een redundante opslag van stemmen (bijvoorbeeld in een apart geheugen) voor het geval er problemen ontstaan met het hoofdgeheugen;
- Een betrouwbare telling van de opgeslagen stemmen en het rapporteren daarvan.

Dit rijtje kan gemakkelijk worden aangevuld met additionele zaken, zoals het leveren van controles op de identiteit van de kiezer, controle op het aantal uit te brengen stemmen per kiezer, en het zorgen voor een audit trail (waarover later meer). Als er sprake zou zijn van tekortschietende programmatuur, heeft dat potentieel een versterkende invloed op het bestaan van alle (a tot en met g) in de vorige paragraaf genoemde risico's.

Om deze functionaliteiten op een goede manier te kunnen leveren, moet er sprake zijn van betrouwbare programmatuur, mede omdat - zoals eerder gesteld - de software doelwit kan worden van gerichte beïnvloeding. Software van stemmachines kan worden aangemerkt als betrekkelijk complex [FISC03]. Dat maakt het ontwerpen en bouwen van functi-

oneel adequate en beveiligingstechnisch robuuste applicaties voor stemmachines niet gemakkelijk. In de discussie rond elektronisch stemmen zien we hier twee uitersten. Het ene kamp (veelal bestaande uit vertegenwoordigers uit de security-gemeenschap) is zeer kritisch over de toereikendheid van de softwarekwaliteit in stemcomputers. Ze wijst op de inherente moeilijkheid om goede software te bouwen en om die kwaliteit aantoonbaar te maken. Het andere kamp (waartoe, niet verwonderlijk, de producenten van stemcomputers behoren) voert interne kwaliteitsstandaarden, strakke testprocedures, en certificering aan als argumenten waarom de kwaliteit van software feitelijk niet ter discussie staat.

Het kamp van de critici heeft een aantal terzake doende argumenten. Op de eerste plaats is dat een ijzeren wet uit de hoek van beveiliging: naarmate de complexiteit van software toeneemt, neemt ook de kwetsbaarheid van die software voor beveiligingsincidenten toe. Men wijst erop, dat correctheid van programmatuur slechts bij zeer triviale en kleine softwarecomponenten aan te tonen is [CANT91]. Voor de meer complexe stemcomputer-software is dat onmogelijk. Men kan zich natuurlijk afvragen, of *correctheid* wel een vereiste is. Het lijkt erop dat we zouden kunnen volstaan met *betrouwbaarheid* van de software, en dat is wat anders. Maar zelfs met betrouwbaarheid als eis bestaat er een probleem, namelijk op het vlak van transparantie. De critici pleiten voor het openbaar maken van de software code, zodat deze bij voortduring bloot staat aan reviews door (onafhankelijke) experts, die zich zo een beeld kunnen vormen van de degelijkheid van het ontwerp en het bestaan van kwetsbaarheden *(open source)*. Over het algemeen echter is de software van de stemcomputers *proprietary*; fabrikanten zien de software als een commercieel object en staan niet te popelen om de resultaten van hun research- en ontwikkelinspanning in de etalage te zetten. Bovendien, zo argumenteren zij, is er geen bewijs dat open source software van betere kwaliteit is dan proprietary software. Overigens kennen landen waar stemcomputers worden gebruikt over het algemeen een certificeringstraject waarbij onafhankelijke instanties de te gebruiken stemcomputers testen tegen een vastgestelde set normen. Daarbij wordt door de leveranciers vaak wel, onder voorwaarde van *non-disclosure*, inzage gegeven in de software code. In Nederland gebeurt deze certificering door TNO.

Een ander argument dat de critici noemen, is het feit dat software verborgen functionaliteit kan bevatten, of dat deze *malware* in de stemcomputers kan worden ingevoegd tijdens de verschillende fases van het bouw-, implementatie-, en plaatsingstraject van de stemcomputers. Deze malware is zeer moeilijk traceerbaar, en zal volgens critici (indien 'goed' gebouwd) met traditionele testprocessen niet kunnen worden ontdekt.

Op grond van het bovenstaande zult u, als waarnemer-IT-auditor, bij uw missie voor de Europese Unie, waarschijnlijk zeer geïnteresseerd zijn in:

- ***De leveranciers van stemcomputers en hun selectie***
  Indachtig de eerder genoemde uitspraak van Rubin hebben de fabrikanten en leveranciers van stemcomputers een zeer kritieke rol. Daarom zal aandacht besteed moeten worden aan de manier waarop deze leveranciers worden geselecteerd, en hun *track record* in het ontwerpen en bouwen van stemcomputers. Een ander aandachtspunt kan de hoeveelheid leveranciers (en dus de hoeveelheid verschillende typen stemcomputers) zijn. Het idee is natuurlijk dat een grotere variëteit de kwetsbaarheid voor frauduleuze hard- en software kleiner maakt.

- ***Het ontwikkel- en testproces en het beveiligingsbeleid bij deze leveranciers***
  De kwaliteit van software in de stemcomputers wordt in belangrijke mate bepaald door de methodes en standaards die bij het ontwikkelproces gehanteerd worden. Alhoewel het onmogelijk is om aantoonbaar *correcte* software van enige omvang te produceren, zijn er wel specifieke ontwikkelmethoden die de kans op ontwerpfouten minimaliseren en daarmee bijdragen aan stabiele en meer betrouwbare functionaliteit. Een voorbeeld daarvan is *Cleanroom Software Engineering* [FISC03, MILL87], waarbij ontwikkelactiviteiten, quality review werkzaamheden en het testen sterk gebaseerd zijn op mathematische en statistische technieken, en waarbij grote nadruk wordt gelegd op de deugdelijkheid van het ontwerp en de verificatie daarvan. Een IT-auditor zal zich een indruk willen vormen van de standaards die de leverancier van stemcomputers in dit opzicht gehanteerd heeft.
  Bovendien is het interessant om te kijken naar het beleid van de leverancier(s) op het gebied van informatiebeveiliging; een IT-auditor kan zich een beeld vormen van de naleving van dat beleid. Uitgangspunt is dat het beveiligingsbeleid - alhoewel op zichzelf geen garantie voor een veilige situatie - wel de basis legt voor de manier waarop de leverancier met confidentialiteit, integriteit, en vertrouwelijkheid van resources zegt om te gaan.

- ***De functionele specificaties van de programmatuur, met name de controlemaatregelen***
  Het is niet waarschijnlijk dat de leverancier van stemcomputers ons, als waarnemer-IT-auditor, inzicht zou geven in de software code; dit vanwege het *proprietary* karakter daarvan. En al zou hij dat wel doen (en als wij de nodige expertise zouden hebben), dan nog zouden we niet in staat zijn op basis van een code review te garanderen dat de software volledig betrouwbaar is. Maar we zullen ons toch minstens een beeld moeten vormen van de functionele specificaties van de software, in het bijzonder van de geprogrammeerde controles. De eerder genoemde risico's a tot en met g kunnen een leidraad zijn bij die beeldvorming.

- ***Het certificatieproces***
  De waarnemer-IT-auditor zal met meer dan gemiddelde interesse kijken naar de manier waarop de stemcomputers

worden gecertificeerd, ook al zal dat wellicht niet gemakkelijk zijn. Vragen liggen hier op het gebied van de normen op basis waarvan wordt gecertificeerd, de certificaatgever en de opdrachtgever voor de certificering. In zijn oratie stelt Jacobs dat zich een interessante situatie zal voordoen als software, ondanks certificatie, in de praktijk toch niet voldoet [JACO03]. Rubin presenteert een interessante uitdaging door voor te stellen om te proberen, onder strikt gecontroleerde omstandigheden, een stemcomputer met onveilige software door de normale certificatieprocedures te loodsen [RUBI].

- ***De procedures van plaatsing van de stemcomputers***
  Tijdens elke stap van het ontwerp, bouw, en *roll out* zijn stemcomputers kwetsbaar voor beïnvloeding van buitenaf. Dit stelt dus ook eisen aan hun opslag, vervoer, en plaatsing. De omstandigheden daarvan zullen controleerbaar moeten zijn.

- ***De handleidingen en instructies voor bediening van de stemcomputers (gebruikers en personeel)***
  Voor het personeel dat doorgaans moest werken met fysieke stembiljetten en stembussen betekent het werken met stemcomputers een verandering. Men zal de stemcomputers - als een soort *operator* - moeten bedienen (starten, vrijgeven voor stemming, afsluiten, en het tellen in werking zetten). Het is noodzakelijk dat dit personeel, dat veelal uit vrijwilligers bestaat, op een goede manier wordt geïnstrueerd over hoe om te gaan met de automatiseringsapparatuur, en er moeten heldere procedures voorhanden zijn die ingaan op de normale operatie en op probleemsituaties, zoals storingen.

- ***De mate van disclosure***
  De mate waarin de waarnemer-IT-auditor betrouwbare informatie ter beschikking kan krijgen over bovengenoemde punten zal een indicatie zijn van de mate van openheid die de organisatoren van de verkiezingen betrachten. Disclosure van de softwarecode aan een certificerende instantie of blootstelling van die software aan het publiek zou een bijzondere mate van openheid indiceren. Zoals eerder gesteld, is transparantie van groot belang, omdat het rechtstreeks gerelateerd is aan de mate van vertrouwen die de bevolking in de verkiezingen zal hebben. Dat belang is nóg groter als de verkiezingen plaatsvinden in een context van grote tegenstellingen en maatschappelijke spanning.

Netwerkverbindingen

Er zijn elektronische stemprocessen waarbij niet alleen stemcomputers worden gebruikt, maar waarbij die computers ook nog voorzien zijn van netwerkverbindingen met andere computers. Een toepassing daarvan is bijvoorbeeld het doorsturen van de verkiezingsresultaten van individuele stemcomputers in een stembureau naar een centrale server op gemeentelijk, regionaal of landelijk niveau. Zo verstuurt het *Newvote*-systeem van leverancier SDU, dat tijdens de recente gemeenteraadsverkiezingen onder meer in Amsterdam werd gebruikt, de lokale stemgegevens draadloos via een GPRS- verbinding naar het gemeentehuis [NEWV06]. Als IT-auditors kennen we de problematiek die met de aanwezigheid van netwerken gepaard gaat maar al te goed. Het verzenden van gegevens via een netwerkverbinding betekent per definitie dat die gegevens aan beïnvloeding blootstaan; afhankelijk van de aard van het netwerk zal dit risico groter of kleiner zijn. Daarnaast betekent een gekoppelde computer ook dat er in beginsel een toegangspad tot die computer is gecreëerd, dat kwaadwillenden zouden kunnen gebruiken om zich toegang tot de op de stemcomputers opgeslagen programmatuur en data te verschaffen of om de werking van die computers te verstoren. Als de functionaliteit van het stemproces vereist dat computers gegevens moeten uitwisselen, speelt er ook nog een uitdaging op het gebied van authenticatie en identificatie. In contrast: ook het 'traditionele' vervoer van stembiljetten, of van processen verbaal met de uitslagen van stemkantoren is kwetsbaar, maar waarschijnlijk eenvoudiger te beveiligen, en pogingen om die papieren te pakken te krijgen zijn in ieder geval beter te observeren en te detecteren. Dat geldt zeker ook voor de manipulatie van de inhoud van een stembus.

Het moge duidelijk zijn dat een 'genetwerkte' systeemopstelling additionele maatregelen vereist, met name waar het gaat om exclusiviteit van de data op de stemcomputers en tijdens transport over het netwerk. De technologieën die daarvoor kunnen worden gebruikt, liggen op het vlak van netwerkbeveiliging: firewall-oplossingen, beveiligde virtual private networks. Fischer [FISC03] pleit voor het zogenaamde *air gapping*: men moet ervoor zorgen dat geen enkele computer (niet de stemcomputers maar evenmin de computers die voor consolidatie en telling van de stemmen worden gebruikt) op enigerlei wijze zelf verbonden is met een onveilig netwerk, noch met andere computers die een dergelijke connectie hebben.

Stemcomputers in een netwerk lijken vooral het risico van 'ongeautoriseerde beïnvloeding van het stemsysteem'(c) te vergroten, met mogelijke gevolgen als ongeautoriseerd uitgebrachte stemmen (b), een onjuiste resultaatbepaling (d) of beïnvloeding van de beschikbaarheid (e). De waarnemer-IT-auditor zal zich een zeer goed beeld willen vormen van de functionaliteit van deze *networking*; hij zal zich zowel van de netwerktopologie als van de technische specificaties en de getroffen maatregelen op het gebied van beveiliging op de hoogte willen stellen.

Audit trail

We hebben gezien dat de verificatie van uitgebrachte stemmen (voter verifiability) en van de verkiezingsresultaten (results verifability) bij stemcomputers een probleem vormt. De stemcomputer is voor de kiezer een black box: na het uitbrengen van zijn stem heeft hij geen mogelijkheid om vast te stellen dat zijn stem inderdaad zoals bedoeld wordt geregi-

streerd en opgeslagen; bovendien heeft het electoraat als geheel slechts beperkte mogelijkheden om vast te stellen dat de verkiezingsuitslag een juiste afspiegeling is van de uitgebrachte stemmen. Dit is een serieus probleem. Indien een aanvaller erin zou slagen de software van stemcomputers zodanig te manipuleren dat deze stemmen wijzigt, verwijdert, of toevoegt, en/of anderszins ervoor kan zorgen dat het tellen en totaliseren van de stemmen frauduleus plaatsvindt, is dat niet per definitie gemakkelijk vast te stellen. In het verlengde van Gebod VII zou eigenlijk ook moeten worden gepleit voor een solide verificatiemogelijkheid, zodat het vertrouwen van de kiezers in het proces als zodanig wordt verkregen en behouden. Dat is echter evenmin eenvoudig, aangezien het stemgeheim dicteert dat de kiezer geen bewijs mag hebben van zijn stem, en dat een uitgebrachte stem niet tot een individuele kiezer herleidbaar mag zijn.

Gezien het belang van deze audit trail is het niet verwonderlijk dat naar werkbare en effectieve oplossingen wordt gezocht. We bespreken de belangrijkste daarvan (die in de praktijk ook daadwerkelijk wordt toegepast), namelijk *voter verifiable paper ballot* (VVPB) of *voter verified ballot systems*. In tegenstelling tot de *paperless DREs* vervaardigen de stemcomputers met VVPB een 'ontvangstbewijs' van de stem zoals die door de kiezer is uitgebracht. Dat is een ticket, een fysiek papiertje, dat wordt afgedrukt door de stemcomputer of een daaraan gekoppelde printer direct nadat de kiezer zijn keuze heeft gemaakt, en waarop staat aangegeven hoe de kiezer heeft gestemd. De kiezer verifieert dat dit een correcte weergave is van zijn stem[6], en deponeert vervolgens de *paper ballot* in een (traditionele) stembus. De paper ballots kunnen vervolgens onafhankelijk van de stemcomputers worden geteld. Dit kan handmatig (zoals bij de traditionele stembiljetten), maar ook met een separate optische lezer als de ballots zijn voorzien van een barcode[7]. Ten aanzien van het tellen van deze biljetjes zijn er grofweg twee mogelijkheden:

1. Er wordt slechts overgegaan tot het tellen van (een gedeelte van) de biljetjes als er een dispuut ontstaat over de uitslag, die is vastgesteld op basis van de gegevens van de stemcomputers.
2. Er wordt, na sluiting van de stembureaus, altijd een steekproef genomen van de stembussen; daarvan wordt de inhoud geteld en vergeleken met de totalen zoals vastgesteld door de respectievelijke stemcomputers. Afwijkingen of disputen leiden tot een volledige hertelling, waarbij de definitieve uitslag wordt bepaald door telling van de paper ballots.

De voordelen van een VVPB systeem zijn [FISC03]:
- Hertellingen zijn gebaseerd op een onafhankelijke en door de kiezer geverifieerde vastlegging;
- Er is een audit trail die voorziet in voter verifiability én mogelijkheden voor *results verifiability*;
- Bij een manuele hertelling zou de 'traditionele' transparantie en observatie mogelijk zijn;
- Een dergelijke aanpak versterkt het vertrouwen van de kiezer in de legitimiteit van de verkiezingen, omdat deze weet dat de door hem geverifieerde stembiljetjes voor hertelling beschikbaar zijn.

De bezwaren tegen deze methode liggen in veronderstelde hogere kosten van de apparatuur, een grotere storingsgevoeligheid en de tijd die een (steekproefsgewijze of volledige) hertelling vergt. Voor een uitgebreide bespreking van VVPB zij verwezen naar [MERC02, MERC02a]. VVPB-gebaseerde systemen worden in de praktijk daadwerkelijk gebruikt.

Naast VVPB worden andere wegen gezocht om verifieerbaarheid van een elektronisch stemproces te garanderen. Een goed voorbeeld daarvan is een ontwerp van Chaum [CHAU04], waarin cryptografische technieken (met name elektronische handtekeningen) worden gebruikt om een hoge mate van verifieerbaarheid te garanderen, met behoud van het principe van stemgeheim en met een kleinere afhankelijkheid van de betrouwbaarheid van stemcomputers. Er wordt echter op gewezen dat dergelijke concepten nog niet aan een onafhankelijke beoordeling zijn onderworpen of in de praktijk zijn getest. Bovendien zijn er twijfels aan de mate waarin deze technieken het vertrouwen van de kiezer zullen bevorderen, aangezien de achterliggende protocollen en fundamenten betrekkelijk complex zijn.

Wat betekent dat nu voor het perspectief van een IT-auditor? Die ziet, bij het gebruik van paperless DREs, een belangrijk geautomatiseerd proces met vrij grote risico's en inherente kwetsbaarheden. Een audit trail gebaseerd op VVPB zoals hierboven beschreven, kan een aantal tekortkomingen oplossen, met name controleerbaarheids- en aantoonbaarheidsaspecten. De Bruijn heeft gelijk als hij stelt dat 'weging van risico's en te nemen maatregelen (*ten aanzien van stemmachines, ER*) uiteindelijk een politieke en maatschappelijke afweging is' [BRUIJ04], maar ik denk dat wij IT-auditors desgevraagd een krachtige aanbeveling zouden doen om, in het licht van het belang van controleerbaarheid en transparantie, een systeem als VVPB (inclusief minimaal steekproefsgewijze controle) ten zeerste te overwegen. Het is een van de weinige mogelijkheden om het eerder gesignaleerde gebrek aan *user controls* te compenseren. Het valt echter niet te ontkennen dat een VVPB gebaseerd systeem elementen van het traditionele, handmatige proces herintroduceert, als verificatiemiddel voor het elektronisch stemmen. En dat lijkt een merkwaardige situatie, waardoor we terugkomen bij de vraag: *waarom* schakelen we eigenlijk over op elektronisch stemmen als het traditionele systeem goed is?

Procedures en mensen

In de paragrafen hierboven is aandacht besteed aan software, netwerken, en een audit trail. Er zijn andere factoren die eveneens veel aandacht verdienen, maar waaraan we hier verder geen grote aandacht besteden. Volledigheidshalve zij

opgemerkt dat hierbij gedacht kan worden aan (1) het menselijke aspect en (2) het beleid en de procedures. Mensen spelen, ook in een geautomatiseerd verkiezingsproces, een essentiële rol; van de ontwikkelaar van software bij de leverancier tot en met de vrijwilliger die in een stemlokaal de stemcomputers bedient, ieder is in meer of mindere mate in staat de betrouwbaarheid van het geautomatiseerde proces als zodanig te beïnvloeden. Om dat in goede banen te leiden, zijn maatregelen nodig, zoals een screening van de programmatuurontwikkelaar, en duidelijke (bedienings)instructies voor de medewerker in het stemlokaal.

Slotopmerkingen

Ik heb in dit artikel een aantal facetten van elektronisch stemmen de revue laten passeren, gepaard aan de dilemma's die daarbij spelen. Ik neem niet direct een positie in als voor- of tegenstander van stemcomputers, maar projecteer de normen die we als IT-auditors in een bedrijfsmatige setting hanteren op een proces dat maatschappelijk van enorm belang is. En dan ontwikkelt zich toch een zekere scepsis, niet zozeer gericht op de toepassing van stemcomputers, als wel op de randvoorwaarden die daarbij volgens onze betrouwbaarheidscriteria zouden moeten gelden, maar die we in de praktijk niet altijd terugzien. En het lijkt dat we daar - niet alleen als auditors, maar als maatschappij als geheel - al te gemakkelijk aan voorbijgaan. Jacobs doet als het ware een oproep om vragen te stellen en antwoorden te forceren, als hij stelt:

'Wij hebben als burgers het recht om het tellen van gewoon met potlood en papier uitgebrachte stemmen bij te wonen en te controleren, maar wij hebben geen inzage in de werking van deze stemcomputers. Vinden wij dit acceptabel? Het lijkt me interessant om deze merkwaardige gesloten-heid eens aan een bestuursrechter voor te leggen, met een beroep op de Wet Openbaarheid van Bestuur'. [JACO03]

Ik wil het artikel afsluiten met een tweetal stellingen van Mander [MAND92], wiens kritische houding ten opzichte van technologie (of beter, ten opzichte van een niet-kritische adoptie van technologie) wel tot enig verder nadenken zal stemmen bij de discussie over stemcomputers.

'Never judge a technology by the way it benefits you personally. (...) The operative question is not whether it benefits you, but who benefits most? And to what end?'

'Make distinctions between technologies that primarily serve the individual or the small community (...) and those that operate on a scale of community control (...). The latter is the major problem of the day.'

Met dank aan Jan Perlee van HEC voor zijn toelichting op de problematiek.

Noten

1 De Bruijns artikel gaat echter vooral in op de wijze waarop een onderzoeksrapport over dit onderwerp zou moeten worden geduid, en hoe risico's gezien moeten worden in een context van een groter proces.
2 Dat wil natuurlijk zeggen: iedere kiesgerechtigde.
3 In Brazilië wordt (bij de verkiezingen die Stanton beschrijft), een persoonlijk identificatienummer van de kiezer door het stembureau ingevoerd om de stemcomputer vrij te geven voor het uitbrengen van de stem. De identificatie van de stemmer is daarmee (meer dan in Nederland) een onderdeel van het geautomatiseerde stemproces, waarmee ook het stemgeheim duidelijk in het geding komt.
4 Het zou mijns inziens juister zijn geweest als Shamos hier ook Gebod III deel 2 had genoemd als onderdeel van het stemgeheim.
5 De presidentsverkiezingen van 2000 in de Verenigde Staten werden uiteindelijk beslist met een marge van slechts 537 stemmen in de swing state Florida.
6 Als dit niet het geval is, dient een procedure te voorzien in een correctiemogelijkheid.
7 In dat geval zal natuurlijk ook de betrouwbaarheid van de apparatuur waarmee de barcodes worden gelezen beoordeeld moeten worden.

Literatuurlijst

[BIEN96] Biene-Hershey, M.E. van, IT Auditing, an object oriented approach. Delwel, Wassenaar, 1996.
[BRUI04] Bruijn, A.J.M. de, Plaats risico van stemmachines in perspectief. In: De Automatisering Gids, juni 2004.
[CANT91] Cantwell Smith, B., Limits of correctness in Computers. In: Computerization and Controversy, Value Conflicts and Social Choices (R. Kling ed.), Academic Press, New York, 1991.
[CHAU04] Chaum, D., Secret-ballot receipts: true voter-verifiable elections. In: IEEE Security & Privacy, januari 2004.
[CRAN96] Cranor, L.A., Electronic Voting. Zie www.acm.org/crossroads/xrds2-4/voting.html
[FISC03] Fischer, E., Election Reform and Electronic Voting Systems (DREs): Analysis of Security Issues. The Library of Congress, 2003.
[HEC00] Het Expertise Centrum. Definitierapport Stemmen op afstand; Eindrapport. Den Haag, 2000.
[JACO03] Jacobs, B., De Computer de Wet Gesteld, Inaugurele Rede, mei 2003.
[KIES04] Besluit van 19 oktober 1989, houdende vaststelling van nieuwe voorschriften ter uitvoering van de Kieswet. Zie www.kiesraad.nl/contents/pages/7451/kiesbesluit.pdf
[KIES05] Wet van 28 september 1989, houdende nieuwe bepalingen inzake het kiesrecht en de verkiezingen. Zie www.kiesraad.nl/contents/pages/7451/kieswet.pdf
[KOHN04] Kohno, T., A. Stubblefield et alt., Analysis of an electronic voting system. IEEE Computer Society Press 2004.
[MAND92] Mander, J., In the Absence of the Sacred: The Failure of Technology and the Survival of the Indian Nations. Sierra Club Books, 1992.
[MERC02] Mercuri, R., Explanation of Voter-verified ballot systems. In: The Risks Digest, ACM Committee on Computers and Public Policy, vol 22 juli 2002.

[MERC02a] Mercuri, R., A Better Ballot Box? In: IEEE Spectrum, oktober 2002.

[MILL87] Mills, H., M. Dyer en R. Linger, Cleanroom Software Engineering. In: IEEE Software 4, 5 september 1987.

[NEUM93] Neumann, P.G., Security Criteria for Electronic Voting. NCS Conference, 1993. Zie www.csl.sri.com/users/neumann/ncs93.html

[NEWV06] Newvote Volledig in Verkiezingen. Website, zie www.newvote.nl.

[RUBI] Rubin, A., Can a voting machine that is rigged for a particular candidate pass certification? Zie www.avirubin.com/vote/ita.challenge.pdf

[SHAM93] Shamos, M.I., Electronic Voting: evaluating the threat. Conference on Computers, Freedom and Privacy, 1993. Zie www.cpsr.org/prevsite/conferences/cfp93/

[STAN00] Stanton, M., The importance of recounting votes. Zie: www.notablesoftware.com/Press/electronic_voting_in_brasil.htm

[SUER02] Suerink, H., en J. van Praat, Inleiding EDP-auditing. Ten Hagen Stam, Den Haag, 2002.

Voor een uitgebreid overzicht (inclusief links) van specifiek Nederlandse feiten op het gebied van elektronisch stemmen, zie de site van het Nijmeegs Instituut voor Informatica en Informatiekunde: http://www.sos.cs.ru.nl/research/society/voting/main.html