UNIE VAN WATERSCHAPPEN

Bezoekadres
Koningskade 40
2596 AA Den Haag
Postadres
Postbus 93218
2509 AE Den Haag
Telefoon
070 351 97 51
Fax
070 354 46 42

Ministerie van Verkeer en Waterstaat
t.a.v. de Staatssecretaris
mevrouw J.C. Huizinga-Heeringa
Postbus 20904
2500 EX DEN HAAG

datum	ons kenmerk	contactpersoon
19 augustus 2008	44540 RR	J.L. Gunter
bijlage(n)	uw kenmerk	e-mail
1	-	jgunter@uvw.nl
betreft		doorkiesnummer
uw verzoek van 13 augustus jl., om reactie op de rapportage van FOX-IT dd. 12 augustus 2008		070 351 9842

Geachte Staatssecretaris,

Graag maak ik van de gelegenheid gebruik te reageren op bovenvermeld rapport .
Ik zal in mijn reactie vooral ingaan op de samenvatting en de conclusies uit hoofdstuk 6 van het rapport.
In de bijlage bij deze brief is per bevinding kort aangegeven wat er met de bevindingen, samengevat in hoofdstuk 6.3, is dan wel wordt gedaan.

Het rapport van Fox-IT komt op een belangrijk punt tot een andere conclusie dan alle eerder geschreven rapporten (bijv. het EiPSI-rapport van 24 juni jl.).
Voorafgaand aan de verkiezingen moet op grond van de wettelijke regels het referentiebestand worden gepubliceerd. Fox IT heeft geconstateerd dat, met het referentiebestand als basis, het op "relatief eenvoudige" wijze mogelijk is om stemmen te injecteren in de stembus.
Deze bevinding is voor de Unie van Waterschappen aanleiding om tot de conclusie te komen dat het op dit moment onverantwoord is om de internetstemvoorziening voor de waterschapsverkiezingen in 2008 in te zetten
Nader onderzocht moet worden of het na afloop van de verkiezingen publiceren van het referentiebestand een afdoende oplossing is om het van buitenaf injecteren van stemmen te voorkomen, waardoor de internetstemvoorziening bij volgende waterschapsverkiezingen wel kan worden ingezet. Om deze oplossing mogelijk te maken zal het Waterschapsbesluit moeten worden aangepast.

Hieronder ga ik verder in op de samenvatting en de conclusies van het rapport.

Samenvatting:

1e bullit
Fox-IT heeft tijdens hun onderzoek de op dat moment actuele versleutelingmethode beoordeeld. Bij de thans actuele versleutelingmethode wordt geen gebruik meer gemaakt van het burgerservicenummer, zodat het niet meer mogelijk is de stem en de identiteit van de stemmer met elkaar in verband te brengen.
2e bullit
Deze bevinding hebben wij ook voorgelegd aan onze deskundigen en de bevinding wordt bevestigd. Een mogelijke oplossing om het injecteren volgens deze methode te voorkomen is het later publiceren van het referentiebestand. Op basis van het Waterschapsbesluit moet dit voorafgaand aan de verkiezingen plaatsvinden. Onderzocht moet worden of het op een later moment publiceren van het referentiebestand in de toekomst haalbaar is. Voor de verkiezingen in 2008 is de bevinding van dien aard dat de internetstemvoorziening niet ingezet kan worden.
3e bullit
De bevinding is juist. Echter de op dit moment geïmplementeerde beveiligingssoftware maakt een dergelijke bevinding niet meer mogelijk. Ook zijn de beheerschermen voor de voorziening niet meer voor derden via internet toegankelijk.

Conclusies

6.1 Raad van Europa

Poststemmen is wettelijk voorgeschreven. Het internetstemsysteem RIES is opgezet als een aanvulling op poststemmen en op deze wijze wettelijk mogelijk gemaakt. Het feit dat twee stemmethoden naast elkaar bestaan, wordt in de aanbevelingen van de Raad van Europa afgewezen.
Gezien de andere wijze van versleutelen, kan het stemgeheim worden gegarandeerd.
De stemcontrole van de internetstem past niet bij de aanbevelingen van de Raad van Europa. Het is echter een bewuste keuze om de betrouwbaarheid van het systeem op deze wijze aan de stemmers zichtbaar en controleerbaar te maken.
Door organisatorische maatregelen wordt voorkomen dat sporen zichtbaar blijven van de internetstemmer.
Op basis van de aanbevelingen van de Raad van Europa zijn er naar mijn opvatting geen wezenlijke punten, op grond waarvan het internetstemsysteem zou moeten worden afgewezen. De afwijkingen op de aanbevelingen van de Raad van Europa zijn bewuste keuzes van onder andere de wetgever.

6.2 Waterschapsbesluit

Artikel 2.45, lid 1, sub a; het geheime karakter

Door het niet meer gebruiken van het burgerservicenummer in de versleutelingmethode kan het geheime karakter worden gegarandeerd.

Artikel 2.45, lid 1, sub b; de betrouwbaarheid van de voorziening

De mogelijkheid stemmen te injecteren in de stembus maakt de internetstemvoorziening op dit moment, op basis van de huidige verplichting het referentiebestand voorafgaand aan de verkiezingen te publiceren, onvoldoende betrouwbaar.
Nader onderzoek moet aantonen in hoeverre, door het op een ander moment publiceren van het referentiebestand, het injecteren van stemmen kan voorkomen, zodat de internetstemvoorziening in de toekomst wel ingezet kan worden bij waterschapsverkiezingen.

Artikel 2.45, lid 1,sub e; inbreuken van buitenaf

De geconstateerde bevindingen in hoofdstuk 4 zijn juist.

Middels installatie van de nieuwe beveiligingssoftware in de productieomgeving zijn de geconstateerde bevindingen uit hoofdstuk 4 niet meer mogelijk.
De beheerschermen van de internetstemvoorziening zijn inmiddels niet meer via internet voor derden toegankelijk.

Artikel 2.48, lid 1 Kiesgerechtigde krijgt een unieke geanonimiseerde en vertrouwelijke code; de identiteit van de kiezer wordt geanonimiseerd geregistreerd

Door het niet meer gebruiken van het burgerservicenummer in de gebruikte code wordt het anonieme karakter en de betrouwbaarheid gegarandeerd.

Artikel 2.58, lid 1, sub c; de voorziening is toegankelijk en gebruikersvriendelijk

De toegankelijkheid en het gebruiksgemak van het stemmen per internet is in verschillende gebruikersonderzoeken de afgelopen periode uitgebreid onderzocht.

In de bijlage verwijs ik u naar het overzicht van alle genoemde bevindingen en onze reactie op de bevindingen.

Conclusie:
1. In de brief van 2 juni 2008 van Het Waterschapshuis, ingediend namens de dagelijkse besturen van de waterschappen, wordt u in kennis gesteld van het voornemen om de kiezer gebruik te laten maken van de mogelijkheid met behulp van internet zijn stem uit te laten brengen.
Op grond van de eerder genoemde bevinding wordt afgezien van het in de brief genoemde voornemen.
2. Er is nader onderzoek nodig om te beoordelen of er oplossingen zijn (bijvoorbeeld het aanpassen van het Waterschapsbesluit) om het injecteren van stemmen in de stembus te voorkomen. Op basis van de uitkomsten van dit onderzoek kan vervolgens het besluit worden genomen of internetstemmen bij volgende waterschapsverkiezingen kan worden aangeboden.

Met vriendelijke groet,

drs. J.M. de Vries
Voorzitter stuurgroep verkiezingen 2008

Reactie paragraaf 6.3 Overzicht van opmerkingen en verbeterpunten.

In de tabel van paragraaf 6.3 worden de bevindingen door Fox-IT samengevat. Volgens Fox-IT kunnen bevindingen leiden tot acceptatie van de constatering, of kunnen aanleiding geven tot aanpassingen. In een onderstaande tabel is aangegeven welke bevindingen volgens de waterschappen een constatering zijn en welke leiden tot verbetering.

De bevindingen van Fox-IT zijn gedaan op basis van de beschikbare documentatie en de (test)voorziening, zoals deze waren in juni 2008. De tekst en de bevindingen uit het rapport zijn daarop gebaseerd. Inmiddels zijn in de maanden juli en augustus aanpassingen aan documentatie en de voorziening doorgevoerd. Dit is gedaan op basis van constateringen van Fox-IT, eigen bevindingen en naar aanleiding van andere externe reviews. Zo was ten tijde van de interviews en op grond van de verstrekte documentatie, aan Fox-IT aangegeven dat het BSN de basis is voor de berekening van de stemcodes. Dit is inmiddels in de voorziening aangepast. Het BSN komt niet meer in de internetstemvoorziening voor. De stemcodes worden nu gegenereerd op basis van een betekenisloos, uniek en willekeurig volgnummer voor iedere kiezer. Dit heeft gevolgen voor verschillende onderdelen van het rapport en bevindingen. Daarnaast hebben verschillende andere aanpassingen gevolgen voor de bevindingen van het rapport, die door Fox-IT niet het rapport konden worden meegenomen. De stand van zaken van juni was daarvoor bepalend.

Bevinding	**Constatering/ Aanpassing**	**Toelichting**
2.1 Gedateerde methoden voor versleutelen van gevoelige informatie	Constatering en aanpassing	In de bevinding wordt aangegeven dat de "houdbaarheid van versleutelde informatie aanzienlijk zou kunnen worden verlengd". Het BSN maakt als gegeven geen onderdeel meer uit van de internetstemvoorziening. Zie verder bevinding 5.1.
2.2 Machtspositie waterschappen en SURFnet	Constatering en aanpassing	In de bevinding wordt aangegeven dat er geen onafhankelijke partij is geïntroduceerd die alle informatie versleutelt. Dit kan nog wel worden geïntroduceerd, sowieso is onafhankelijk toezicht voorzien bij de versleuteling.
2.3 Tijd-/datuminformatie mag niet worden opgeslagen	Constatering	Er zijn technisch en organisatorische maatregelen genomen dat tijd-/datuminformatie niet wordt opgeslagen.
2.4 Stem kan achterhaald worden met internetstemkaart	Constatering	Op de internetstemkaart staat geen enkel gegeven dat een kiezer kan identificeren. Het is niet bewijsbaar dat een internetstemkaart van een bepaalde kiezer was. Dat een kiezer na het stemmen zijn internetstemkaart moet vernietigen staat op een aantal plaatsen duidelijk aangegeven in het stempakket.
2.5 Stemkwitantie is niet falsificeerbaar zonder technische stemcode	Constatering	Inherent aan de voorziening is dat bij een dispuut de kiezer zijn technische stemcode moet hebben opgeslagen en aan de scheidsrechter (umpire) geven. Anders kan de scheidsrechter geen oordeel vellen over het dispuut.
2.6 Insiders kunnen stemmen vervangen	Constatering	Er zijn organisatorische en technische maatregelen genomen die dit signaleren respectievelijk voorkomen. Zie ook toelichting bij bevinding 3.10.
2.7 Stemserver in 2004 niet adequaat afgesloten, bevinding niet opgevolgd	Constatering	Constatering bij een testverkiezing in 2004. Daarna is de stemvoorziening herhaaldelijk gebruikt, en altijd consequent afgesloten.
2.8 Technische beveiligingstest serverconfiguratie niet uitgevoerd	Aanpassing	Aanbeveling over beveiligingstest is meegenomen.

Bevinding	Constatering/ Aanpassing	Toelichting
2.9 Risico van relatieve onbekendheid MDC-2	Constatering	Een constatering, waarbij in het rapport wordt opgemerkt dat MDC al sinds de jaren '80 door IBM wordt gebruikt in haar cryptografische producten en dat er ondanks die lange tijd geen problemen met het algoritme bekend zijn.
2.10 Geen calamiteitenplan	Aanpassing	Zoals in het rapport staat aangegeven komt er nog een calamiteitenplan.
2.11 Stemsite voldoet niet aan toegankelijkheidseisen overheidswebsites	Aanpassing	Inderdaad is aangegeven dat er wel degelijk uitgebreid aandacht is en wordt besteed aan de toegankelijkheid van de stemsite voor visueel gehandicapten. Echter door de toepassing Javascript kan nooit voldaan worden aan alle eisen. Volgens de richtlijnen is dat ook niet nodig als een ander kanaal beschikbaar is. Dat is in dit geval poststemmen.
2.12 Stemsite werkt niet goed in sommige browsers	Aanpassing	Er waren al browser compatibiliteitstests gepland. De aangegeven zaken van deze bevinding, zullen inderdaad voor november 2008 zijn opgelost.
3.1 Toegankelijkheid en bedieningsgemak	Aanpassing	Bedoelde onderzoeken zijn er wel en worden nog gedaan in 2008.
3.2 Kiezer kan stem later ongeldig maken	Constatering	In de bevinding is een voorbeeld van een theoretische mogelijkheid gegeven, die zich in praktijk niet voor kan doen. Als er een storing is, dan moet de kiezer nogmaals inloggen om zijn stem uit te brengen of te controleren of zijn stem is ontvangen door de stemservers. Indien niet twee stemservers de stem hebben opgeslagen, dan kan de kiezer het uitbrengen van zijn stem vervolgen. Is de stem wel opgeslagen, dan is dat zichtbaar in het statusoverzicht van de kiezer en kan hij niet nogmaals stemmen.
3.3 Versleutelde stemmen worden opgeslagen	Aanpassing	De bevindingen van 4.1 en 5.1 zijn inmiddels hersteld. Derhalve wordt wel voldaan aan Aanbeveling 11 van de Raad van Europa.
3.4 Foutmelding meldt niet dat ook blanco kan worden gestemd	Aanpassing	Constatering is inmiddels aangepast en heeft zich overigens nooit voorgedaan bij eerder gebruik.
3.5 Anonimiteit niet onbeperkt gewaarborgd	Aanpassing	Bevinding 5.1 is niet meer actueel. Het BSN maakt geen onderdeel meer uit van de stemvoorziening. Derhalve wordt voldaan aan de Aanbevelingen 17 en 78 van de Raad van Europa.
3.6 Uitproberen stemsysteem niet gedocumenteerd	Aanpassing	Er is een testversie van de stemsite beschikbaar, die in 2008 is gebruikt voor gebruikersonderzoeken. Het is de bedoeling dat deze versie wordt ingezet om de kiezers kennis te laten maken met het stemsysteem.
3.7 Kwitantie en stembevestiging in strijd met aanbevelingen Raad van Europa	Constatering	Constatering is inherent aan de opzet van de internetstemvoorziening. En is ook inherent aan het plaatsonafhankelijk stemmen. Zie verder toelichting bij bevinding 2.4.
3.8 Eenduidige identificatiemethode bij gelijke naam en gelijk adres niet gedocumenteerd	Aanpassing	Zoals al in het rapport is aangegeven hebben de waterschappen hiertoe wel degelijk een mechanisme ontwikkeld.
3.9 Sporen van stem worden niet uitgewist	Aanpassing	BSN maakt geen onderdeel meer uit van de stemcodes. Dus uit de stemcodes en technische stem, valt niet op te maken van wie de stem is. Uit een kwitantie (ontvangstbevestiging) die bewaard wordt op een PC valt niet op te maken van wie die kwitantie is. De voorziening

Bevinding	Constatering/ Aanpassing	Toelichting
		vernietigd automatisch alle sporen en het is aan de kiezer of hij zijn kwitantie elektronische bewaard. Overigens is de gememoreerde bevinding 4.6 inmiddels hersteld.
3.10 Integriteit van logsysteem niet gewaarborgd	Aanpassing	Aanpassing houdt in dat op alle servers alles gelogd wordt naar blackbox loghost, machine waar de beheerders niet bij kunnen. De blackbox loghost ontvangt automatisch de logging alle andere machines. Wordt met audit functie gevuld, dit betekent dal elk commando wordt gelogd.
4.1 Stembureau kan afgebroken stemmen inzien	Aanpassing	Constatering terecht. Deze informatie moet niet worden meegestuurd. Oorzaak is het samenvoegen van 2 schermen A020 en A025, waarbij de reset van de parameters per abuis is weggevallen. Is opgelost in volgende versie VotingWindow.
4.2 Versienummer systeemsoftware leesbaar	Aanpassing	In de op te leveren productiesituatie is er geen versienummer meer zichtbaar.
4.3 Verouderde versie van systeemsoftware met bekende beveiligingsfouten	Aanpassing	Vanaf begin juli wordt gewerkt met een centraal provisoning-systeem, waardoor alle software op de verschillende systemen draaien met dezelfde en laatste (nieuwe) versies van de software. Systeemsoftware is dus volledige vernieuwd en actueel. Geconstateerde kwetsbaarheden kunnen niet meer voorkomen.
4.4 Servermappen zijn in te zien	Aanpassing	Is niet meer mogelijk en dit is ook opgelost door de upgrading van de software en de hardening van de systemen en de configuratie.
4.5 Kwitantie is manipuleerbaar	Aanpassing	Inmiddels is besloten deze manier van kwitantie tonen – via PDF - te laten vallen. De nieuwe manier van tonen (gebaseerd op scherm, gebruikt in 2004 en 2006) wordt meegenomen in de nieuwe versie van VotingWindow. Hierdoor wordt het scherm (ontvangstbevestiging) gegenereerd op de PC van de kiezer en wordt informatie (technische stem) lokaal uit het geheugen gehaald. Er is dan geen contact nodig met de stemserver, in tegenstelling met een kwitantie op basis van PDF.
4.6 Technische stemcodes in browsergeschiedenis	Aanpassing	Deze constatering vervalt bij de genoemde implementatie onder Bevinding 4.5.
4.7 Beheerschermen zichtbaar via het internet	Aanpassing	Dit is een direct gevolg van bevinding 4.3. Met het herstel van bevinding 4.3, is bevinding 4.7 niet meer mogelijk.
4.8 Beheerschermen kwetsbaar voor Cross-Site Scripting (XSS)	Aanpassing	Zie reactie op bevinding 4.7. Het gaat om de Stemserver Applicatie Beheerconsole, die alleen bereikbaar is via beheermachines van SURFnet beheerders. Staat niet (meer) in contact met het internet. Een Cross Site Scripting (XSS) aanval is onder de nieuwe configuratie onmogelijk. Bovendien is software extern nader onderzocht op XSS en wordt op de bevindingen aangepast.
4.9 Mogelijkheid om Denial-of-Service-aanval te versterken	Constatering	De gebruikte constructie om een Denial-of-Service-aanval te versterken, is vergelijkbaar wat kiezers doen om op de normale manier om bij de stemschermen te komen. De servers zijn daarop berekend en dat miljoenen aanvragen kunnen worden ingediend. Het systeem is daarop gedimensioneerd.
4.10 Beheerschermen geven informatie vrij	Aanpassing	Stemserver Applicatie Beheerconsole mag niet bereikbaar zijn. Het kunnen vinden is gevolg van bevinding 4.3 en 4.7. En is met de aangeven maatregelen opgelost.

Bevinding	Constatering/ Aanpassing	Toelichting
4.11 Beheerschermen kwetsbaar voor databasemanipulatie door middel van SQL Injection	Aanpassing	Stemserver Applicatie Beheerconsole mag niet bereikbaar zijn. Het kunnen vinden is gevolg van bevinding 4.3 en 4.7. En is met de aangeven maatregelen opgelost. Bovendien is software extern nader onderzocht op SQL Injection en wordt op de bevindingen aangepast.
4.12 Verouderde versie van database met bekende beveiligingsproblemen	Aanpassing	Het versie nummer geeft inderdaad een oude versie aan. Echter conform het beleid van de leverancier (RedHat (RELH4) backport policies). Database is derhalve bestand tegen de bekende kwetsbaarheden in de gebruikte versie.
4.13 Ondersteuning voor onveilige versleuteling als kiezer erom vraagt	Aanpassing	Minimale SSL protocol is vanaf juli versie 3.0. Conform vergelijkbare eisen die ook aan gebruikers van elektronisch bankieren worden gesteld.
5.1 Stemgeheim beperkt houdbaar	Aanpassing	Deze bevinding richt zich op de mogelijkheid om na verloop van tijd (na 2030) de in RIES gebruikte 3DES sleutels te kunnen kraken en daarmee het stemgeheim achteraf te kunnen doorbreken. Dat kan, omdat de stemsleutels voor de kiezers en daarvan afgeleide zaken in RIES worden berekend met het BSN van de kiezer. Inmiddels is in RIES deze aanpak veranderd. In de aan RIES door te geven kiezerbestanden komt geen BSN meer voor, maar in plaats daarvan een verder betekenisloos, uniek en willekeurig volgnummer voor iedere kiezer. Daarmee wordt voldaan aan de aanbeveling in de conclusie van deze bevinding.
5.2 Geldige stemcodes genereerbaar tijdens stemperiode	Aanpassing, juridische belemmering	De onderzoekers van Fox-IT hebben voor het eerst kunnen aantonen, dat het helaas mogelijk is tijdens de verkiezingen geldige codes te genereren en daarmee stemmen via internet uit te brengen. Door een wijziging in de huidige aanpak van de voorziening is een dergelijke aanval te voorkomen: het publiceren van het initiële referentiebestand van de verkiezing pas na sluiting van de verkiezing. De publicatie van het referentiebestand van een verkiezing bestaat uit het op Internet publiceren van statistische gegevens (over onder andere het aantal stemgerechtigden) en het referentiebestand zelf en in een gedrukt medium (de Staatscourant) een aantal hash-waarden ter garantie van de integriteit van de op Internet gepubliceerde data. Dit dient om een aantal controles door kiezers en derden mogelijk te maken. Een deel van die controles kan pas plaatsvinden na sluiting van de verkiezing, als opnieuw door publicatie van het (door uitgifte van vervangende stempakketten) aangepaste Referentiebestand kan worden vastgesteld wat er daadwerkelijk veranderd is. Verder speelt het Referentiebestand een rol bij het controleren door kiezers en derden van de uitslag en de afhandeling van klachten door de scheidsrechter, beide ook na sluiting van de verkiezing. Het Waterschapsbesluit waterschapsverkiezingen 2008 stelt echter als eis dat het referentiebestand ten minste vierentwintig uur voor het begin van de stemperiode wordt gepubliceerd. Reglementair is niet in de voorgestelde aanpassing voorzien en derhalve in 2008 niet mogelijk.
5.3 Referentiebestand niet gesorteerd	Aanpassing	BSN wordt niet meer gebruikt in RIES, zie reactie bevinding 5.1.

Bevinding	Constatering/ Aanpassing	Toelichting
5.4 "Umpire"-functie kan niet alle disputen oplossen; krijgt inzicht in de uitgebrachte stem	Constatering	Inherent aan de voorziening is dat bij een dispuut de kiezer zijn technische stemcode moet hebben opgeslagen en aan de scheidsrechter (umpire) geven. Anders kan de scheidsrechter geen oordeel vellen over het dispuut.
5.5 Drukker beschikt over geheime sleutels	Constatering	Er zijn procedurele en organisatorische maatregelen getroffen om het stemgeheim te waarborgen. Aanbeveling is niet alleen kostbaar, maar vergt ook een zeer lange ontwikkeltijd.
5.6 Logging-dilemma: veiligheid versus stemgeheim	Constatering	Zie bevinding 2.3.
5.7 Onduidelijkheid documentatie	Aanpassing	De gerefereerde documenten zijn op verschillende momenten, in de periode van 2003 tot heden geschreven. De reden dat door de waterschappen EiPSI is verzocht een beschrijving te maken (die inmiddels beschikbaar is) is om in de door Fox-IT gestelde behoefte te voorzien.
5.8 Digitale handtekening met publieke sleutel	Aanpassing	Is inmiddels hersteld.
5.9 Toevoeging geboortejaar (AbelPI) heeft geen functie	Constatering	Het gestelde over het gebruik van het geboortejaar bij internetstemmen (AbelPI) is in principe juist, maar niet van praktische betekenis. AbelPI is niet ontworpen om geavanceerde internet aanvallen tegen te gaan. Het is het maximaal haalbare om eenvoudige vormen van misbruik met gevonden stempakketten tegen te gaan.