

E-mailbericht

-----Oorspronkelijk bericht-----

Van:

Verzonden: maandag 7 januari 2008 22:54

Aan: DAB-DIM Postbus

Onderwerp: Bericht via www.verkeerenwaterstaat.nl

Naam:

Organisatie:nvt

Adres:.

E-mailadres:

Vraag:

Beste L. S.,

Over niet al te lange tijd komen er nieuwe waterschapsverkiezingen. Bij deze verkiezingen is het op diverse manieren mogelijk een stem uit te brengen. Verschillende mogelijkheden om een stem uit te brengen zijn via brieven, telefoon en internet.

Bij verkiezingen zijn er een aantal zaken van het grootste belang. Het gaat hierbij met name om het stemgeheim en het kunnen verifiëren van de uitgebrachte stemmen. Hierover heeft U ondermeer op 19 december 2007 een brief gestuurd aan de tweede kamer.

Op basis van de informatie die ik tot op heden gevonden heb, heb ik niet kunnen concluderen dat het stemmen aan de hier voor genoemde voorwaarden voldoet, dit op meerdere vlakken.

Om te kunnen verifiëren of het systeem waterdicht en controleerbaar is zou de complete werking van het systeem, de specificaties en de implementatie openbaar moeten zijn. Onder implementatie versta ik naast beschrijvingen van de software ook de broncode.

Veel voorbeelden waarom dit van belang is zijn er te noemen, maar deze zijn al snel heel technisch. Wat wel te noemen is zijn bijvoorbeeld de programma onderdelen die willekeurige getallen maken. Een dergelijk systeem is hier qua beveiliging compleet van afhankelijk. Indien de distributie van de gegenereerde getallen ook maar fractioneel afwijkt van ideaal verdeelde getallen is fraude al eenvoudig mogelijk.

Het stemgeheim is een ander punt van zorg. Als ik de wetenschap van bewoners van hetzelfde huis en hun invloed buiten beschouwing laat (dit geldt even goed voor het via brief of telefoon stemmen en hoort daarom in een andere discussie thuis) zijn er hier nog aspecten die van grotere zorg zijn. Het is algemeen bekend dat zeer veel mensen computers hebben die feitelijk niet onder hun eigen controle staan, maar voorzien zijn van spyware of deel uit maken van een zogenaamd bot-net.

Op welke manier de waterschappen hun beveiliging ook organiseren, dit aspect van de beveiliging is zeer moeilijk onder controle te krijgen. Er zijn mogelijkheden om dit te realiseren maar die vereisen een vertrouwd platform (denk hierbij aan bijvoorbeeld een systeem zoals de random reader zoals de Rabo Bank die gebruikt, alleen dan nog verder doorgevoerd). Zolang kiesgerechtigden alleen via een kwetsbare, over het algemeen slecht beveiligde, PC kunnen stemmen is het fundamenteel onmogelijk om enige garantie af te geven over het stemmen.

Graag wil ik van U vragen of U er voor zorg wilt dragen dat alle ter zaken doende informatie beschikbaar komt. Dit bestaande uit bijvoorbeeld de broncode van alle gebruikte programma's. De procedures die de informatie beschermen en lekken kunnen bevatten. Bijvoorbeeld uitbested

drukwerk met geheime sleutels en backups die gemaakt worden van deze gegevens en hoe daar mee om gegaan wordt.

Bij voorbaad dank voor de informatie en transparantie.

Met vriendelijke groet,