Plan van Aanpak TNO-ITSEF

Hugo Buitenhuis
Dirk-Jan Out
Versie 0.9

Dit is het Plan van Aanpak van TNO-ITSEF voor de aanvullende controles van stemmachines in opdracht van het Ministerie van BZK.

De versie is 0.9: na een commentaarronde van BZK zal de definitieve versie worden opgemaakt.

Dit plan begint met een analyse die duidelijk maakt:

- Wat de lifecycle is van stemmachines (Sectie 1)
- Hoe de beveiliging is geregeld voor iedere stap in de lifecycle (Sectie 2)
- Hoe deze beveiliging kan worden getoetst (Sectie 3), alsmede
    - Welke beveiliging door TNO zal worden getoetst
    - Welke beveiliging niet door TNO zal worden getoetst
- En, in Sectie 4, hoe TNO-ITSEF de toetsing zal uitvoerewn

1. Lifecycles

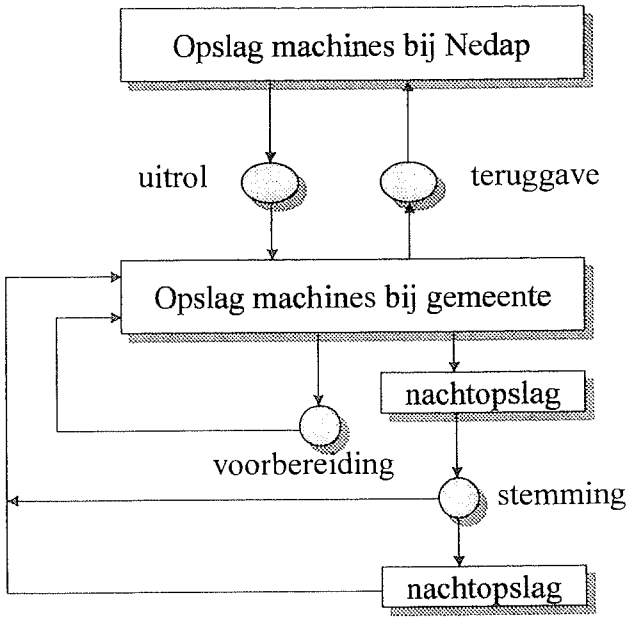
We beginnen dit rapport met de lifecycles van de verschillende stemmachines. Deze zijn grafisch weergegeven en geven aan wat er met een stemmachine gebeurt van fabricage tot gebruik in het stemlokaal en uiteindelijke opslag tot de volgende verkiezing. Gebruikte symbolen:

- rechthoek: fysieke opslag
- pijl: fysiek transport van een stemmachine
- rondje: een activiteit waarin iets met de machine gedaan wordt

We onderscheiden drie lifecycles:

- De lifecycle van NEDAP-apparatuur
- Twee lifecycles van SDU-apparatuur: een simpele en een complexere

1.1 De NEDAP Lifecycle



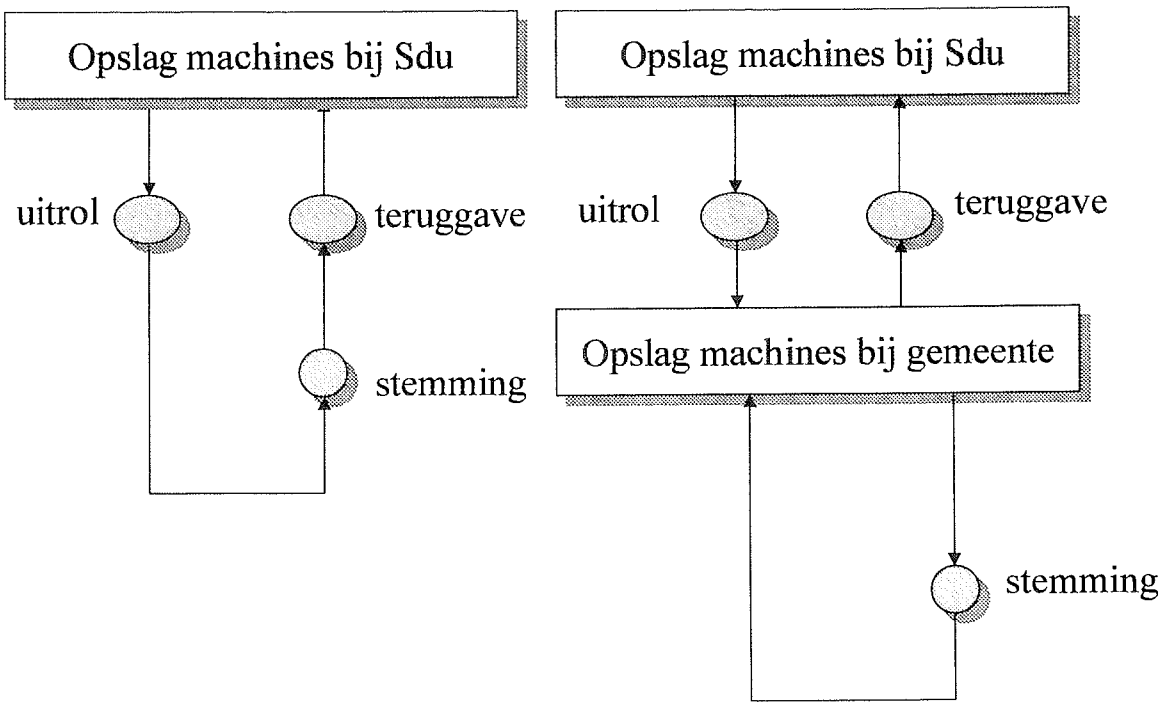
Lifecycle Nedap

In deze lifecycle worden stemmachines geproduceerd bij Nedap, en vandaar uit uitgerold naar een centrale opslag bij iedere gemeente, waar ze het grootste deel van hun actieve leven doorbrengen. Daarnaast wordt door Nedap zelf nog een relatief klein aantal machines opgeslagen die vlak voor de verkiezingen worden uitgerold en vlak daarna weer worden teruggeven.

Enige tijd voor de verkiezing vindt een voorbereiding plaats: hier worden de stemgeheugens voorzien van de lijst met partijen en kandidaten. Hiervoor wordt een pc met ISS software en een lees-/schrijfeenheid gebruikt.

De dag voor de verkiezing zal een gemeente de centraal opgeslagen stemmachines distribueren naar de stembureaus, waar ze in de zogeheten "nachtopslag" worden bewaard. Er vindt een stemming plaats, en dan zullen de stemmachines danwel meteen terug worden getransporteerd naar de centrale opslag, danwel eerst nog een nacht in de nachtopslag doorbrengen en dan naar de centrale opslag worden teruggebracht.

1.2 De SDU Lifecycles



SDU hanteert twee lifecycles: een simpele en een iets complexere.

In de simpele lifecycle rolt SDU de machine op de dag van de verkiezingen uit, de stemming vindt plaats, en SDU neemt hem dezelfde dag weer in.

In de complexere lifecycle worden de stemmachines enkele dagen voor de verkiezingen naar een centrale opslag locatie bij de gemeente gebracht. Op de dag van de verkiezing worden de stemmachines meegegeven aan een stembureaulid. Na de stemming brengt het stembureaulid de machine weer terug bij de centrale opslag. Daarna neemt Sdu de machines weer in.

1.3 Kwetsbaarheden in de lifecycle

Aan de hand van bovenstaande lifecycles kunnen we analyseren waar de machines kwetsbaar zijn, en of dit relevant is voor een lifecycle:

Locatie stemmachine	**Nedap**	**SDU-S**	**SDU-C**
I. Opslag bij fabrikant	X	X	X
II. Transport fabrikant <-> gemeente	X		X
III. Transport fabrikant <-> stemlocaal		X	
IV. Transport gemeente <-> stemlocaal	X		X
V. Opslag bij gemeente	X		X
VI. Opslag bij stemlocaal	X		X
VII. Gebruik in stemlocaal	X	X	X

Er bestaat een aantal dreigingen tegen stemmachines: in dit rapport wordt er maar 1 beschouwd:

Een aanvaller verkrijgt fysiek toegang tot een stemmachine en weet ongemerkt de functionaliteit hiervan te veranderen, resulterend in een andere stemverdeling.

Om deze dreiging te voorkomen, moet op iedere van de zeven locaties uit de tabel bescherming worden geboden. De beveiligingsmaatregelen zijn onder te verdelen in:

1. Tamper resistance: Voor zowel NEDAP als SDU is deze laag: [redacted] Deze zullen we dus verder verwaarlozen
2. Tamper evidence:
   - Bij NEDAP bestaat deze uit [redacted]
   - Bij SDU bestaat deze uit [redacted]
3. Organisatorische procedures: deuren, sloten, cameras, stembureauleden, bewakers etc.

2 Beveiling per lifecyle stap

We kunnen nu de tabel verder uitwerken, door te analyseren welke beveiliging waar plaatsvindt:

Locatie stemmachine	**Nedap**	**SDU-S**	**SDU-C**
I. Opslag bij fabrikant	A	B	B
II. Transport fabrikant <-> gemeente	C		D
III. Transport fabrikant <-> stemlocaal		D	
IV. Transport gemeente <-> stemlocaal	E		E
V. Opslag bij gemeente	F		F
VI. Opslag bij stemlocaal	G		G
VII. Gebruik in stemlocaal	H	H	H

A: Opslag bij NEDAP
NEDAP slaat een aantal stemmachines centraal op. NEDAP beveiligt deze met [redacted]
A1: De verantwoording voor de uitvoering van deze procedures ligt bij NEDAP.

B: Opslag bij SDU
SDU slaat al haar stemmachines centraal op. SDU beveiligt deze met [redacted]
B1: De verantwoording voor de uitvoering van deze procedures ligt bij SDU.

C: Transport van NEDAP naar gemeente en terug
NEDAP vervoert stemmachines naar de gemeente. NEDAP beveiligt deze met [redacted]
C1: De verantwoording voor de uitvoering van deze procedures ligt bij NEDAP.
C2: De kwaliteit van de NEDAP tamper-evidence is onbekend

D: Transport van SDU naar gemeente/stemlocaal en terug
SDU vervoert stemmachines naar de gemeente of direct naar het stemlocaal. SDU beveiligt deze met [redacted]
D1: De verantwoording voor de uitvoering van deze procedures ligt bij SDU.
D2: De kwaliteit van de SDU tamper-evidence is onbekend

E: Transport van gemeente naar stemlocaal en terug
Een gemeente moet stemmachines (SDU en Nedap) transporteren van gemeente naar een stemlocaal. Een gemeente beveiligt dit met [redacted] en gebruikt daarnaast [redacted]
E1: De verantwoording voor de uitvoering van deze procedures ligt bij de gemeente
E2: De kwaliteit van de NEDAP tamper-evidence is onbekend
E3: De kwaliteit van de SDU tamper-evidence is onbekend

F: Opslag bij gemeente
Een gemeente slaat stemmachines centraal op. Soms voor kortere tijd (SDU), soms voor langere tijd (NEDAP). Een gemeente beveiligt dit met [redacted] en gebruikt daarnaast [redacted]
F1: De verantwoording voor de uitvoering van deze procedures ligt bij de gemeente
F2: De kwaliteit van de NEDAP tamper-evidence is onbekend
F3: De kwaliteit van de SDU tamper-evidence is onbekend

G: Opslag bij stemlocaal
Een gemeente slaat stemmachines decentraal op in stemlokalen voor kortere tijd. .
Een gemeente beveiligt dit met [redacted] en gebruikt daarnaast [redacted].
G1: De verantwoording voor de uitvoering van deze procedures ligt bij de gemeente
G2: De kwaliteit van de NEDAP tamper-evidence is onbekend
G3: De kwaliteit van de SDU tamper-evidence is onbekend

H: Gebruik bij stemlocaal
In een stemlocaal worden de verkiezingen gehouden en zijn de stemmachines toegankelijk voor het publiek. Een gemeente beveiligt dit met [redacted] en gebruikt daarnaast [redacted]
H1: De verantwoording voor de uitvoering van deze procedures ligt bij de gemeente
H2: De kwaliteit van de NEDAP tamper-evidence is onbekend
H3: De kwaliteit van de SDU tamper-evidence is onbekend

3 Toezicht en testen

In principe dient ieder van de genoemde maatregelen boven getest danwel gecontroleerd op uitvoering te worden. Dit toezicht en testen kan worden onderverdeeld in drie groepen:

- Testen van technische maatregelen
- Controleren van centrale procedures
- Controleren van decentrale procedures

Testen van technische maatregelen
Het betreft hier het toezien op de additionele beveiligingsmaatregelen van NEDAP[1] apparatuur: C2, E2, F2, G2, en H2.

Het betreft hier niet het toezien op tamper-evidence van SDU: D2 E3, F3, G3 en H3. Het aanvallen van de SDU machines is lastiger omdat:

- [redacted]
- [redacted]
- [redacted]

[redacted]. Het verdient de aanbeveling om hier voor de maart verkiezingen dieper op de SDU-problematiek in te gaan.

TNO-ITSEF zal een beoordeling uitvoeren van de effectiviteit van de NEDAP maatregelen. Daarnaast zal TNO-ITSEF een steekproef nemen bij gemeentes om te zien of het is uitgevoerd.

***Testen van centrale maatregelen**
Het betreft hier het beoordelen van en toezien op procedures die op een klein aantal plaatsen wordt uitgevoerd/geinitieerd:

- Centrale Opslag NEDAP (A1) en vervoer naar gemeentes (C1)
- Centrale Opslag SDU (B1) en vervoer naar gemeentes/stemlocalen (D1)

TNO-ITSEF zal een beoordeling uitvoeren van de effectiviteit van de organisatorische maatregelen en controleren of deze worden uitgevoerd:

Testen van decentrale maatregelen
Het betreft hier het beoordelen van en toezien op procedures die op een groot aantal plaatsen wordt uitgevoerd/geinitieerd. Het betreft hier:

- Vervoer binnen gemeentes (E1)
- Opslag binnen gemeentes (F1)
- Opslag binnen stemlocalen (G1)
- Gebruik tijdens verkiezingen (H1)

---

[1] Op de vergadering bij de SG begrepen we pas dat de SDU apparatuur ook niet 100% van de tijd wordt bewaakt. Hij wordt in sommige gevallen de dag van te voren afgeleverd (bij gemeente of stemlokaal) en is daar gedurende korte tijd kwetsbaar.

TNO-ITSEF zal de effectiviteit van deze maatregelen niet controleren, en er niet op toezien dat deze worden uitgevoerd.
Deze zijn in principe de verantwoordelijkheden van de gemeentes, en deze dienen er zelf op toe te zien (bijvoorbeeld in samenwerking met de politie) dat de maatregelen effectief zijn en worde uitgevoerd.

Emergency Response
Als laatste kan blijken dat er ondanks al het bovenstaande toch een verdenking op specifieke stemmachines komt te rusten.

- TNO-ITSEF zal op de dag voor de verkiezingen, de dag van de verkiezingen en de vier dagen erna teams standby houden om controles uit te voeren op "verdachte" stemmachines.

Kanttekening: tamperen met stemmachines is een strafbaar feit wat vervolgd kan worden. Als wij met spoed aan die machines iets moeten doen, vernietigen wij wel bewijs.
Het Ministerie zal uit moeten zoeken hoe dit juridisch zit.
Eigenlijk is het NFI hier de aangewezen partij.

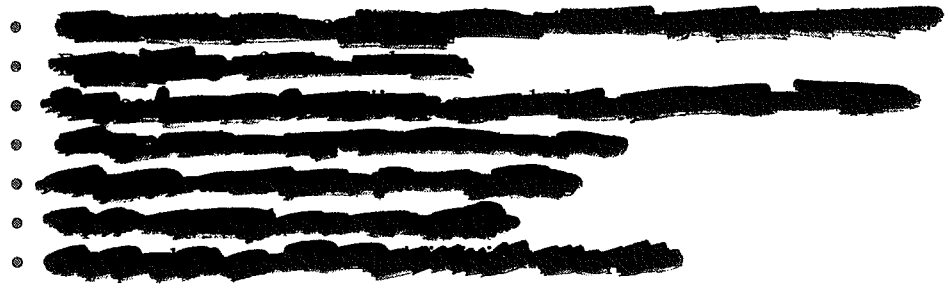
4 Activiteiten

Activiteit #1: Onderzoek effectiviteit NEDAP maatregelen

TNO-ITSEF zal een beoordeling uitvoeren van de effectiviteit van de NEDAP maatregelen. Daarnaast zal TNO-ITSEF een steekproef nemen bij gemeentes om te zien of het is uitgevoerd.

Activiteit #1A
Allereerst zal TNO-ITSEF een onderzoek uitvoeren naar de verzegelingsmaatregelen van NEDAP.

Aanvang: zodra de zaken van NEDAP bij TNO-ITSEF arriveren
Afronding: binnen drie weken daarna
Activiteiten:



Activiteit #1B
Daarnaast zal TNO een steekproef nemen bij 30 gemeenten of NEDAP de verzegeling inderdaad heeft uitgevoerd.

Aanvang: zodra NEDAP aangeeft dat verzegeling is afgerond
Afronding: afhankelijk van gemeentes
Activiteiten: BZK stuurt brief naar 30 (door ons willekeurig gekozen) gemeentes met dringend verzoek om:

- Foto van verzegeld apparaat (om te garanderen dat ze er echt naar kijken)
- Lijst van serienummers die die gemeente denkt in bezit te hebben
- Verklaring dat ze gecontroleerd hebben dat alle apparaten zijn verzegeld

naar TNO te sturen.

Activiteit #2: Centrale opslag NEDAP en vervoer NEDAP

TNO-ITSEF zal een beoordeling uitvoeren van de maatregelen die NEDAP heeft genomen voor de opslag en het vervoer van en naar gemeentes

Aanvang: in overleg met NEDAP
Afronding: binnen twee weken daarna
Activiteiten:

- Beoordelen relevantie documentatie processen NEDAP
- Audit bij NEDAP of deze processen worden uitgevoerd
- Eindoordeel in kort rapport

Activiteit #3: Centrale opslag SDU en vervoer SDU

TNO-ITSEF zal een beoordeling uitvoeren van de maatregelen die SDU heeft genomen voor de opslag en het vervoer van en naar gemeentes

Aanvang: in overleg met SDU
Afronding: binnen twee weken daarna
Activiteiten:

- Beoordelen relevantie documentatie processen SDU
- Audit bij SDU of deze processen worden uitgevoerd
- Eindoordeel in kort rapport

Activiteit #4: Onderzoek effectiveit NEDAP maatregelen

TNO-ITSEF zal op de dag voor de verkiezingen, de dag van de verkiezingen en de vier dagen erna teams standby houden om controles uit te voeren op "verdachte" stemmachines..

Aanvang: 21 november
Afronding: 26 november
Activiteiten:

- Team standby houden dat verdachte stemmachines controleert
- Indien er onvoldoende verdachte machines zijn, steekproeven uitvoeren.
- Tijdige mondelinge rapportage voor deze activiteit aan Kiesraad
- Schriftelijke eindrapportage (zal einge dagen erna komen)

Activiteit #5: Diversen

Deze activiteit bevat de omlijstende zaken die TNO-ITSEF in dit kader voor MinBZK verricht

Aanvang: reeds geruime tijd
Afronding: 30 november
Activiteiten:

- Overleg met Ministerie
- Schrijven van projectplannen
- Overige activiteiten
- Schrijven eindrapport