

Geachte heer/ mevrouw,

We willen u graag informeren dat 5.1.2.e mede-oprichter van Fox-IT, per 1 januari 2018 zijn functie als directeur neer zal leggen. Meer gedetailleerde informatie vindt u in het persbericht hieronder. Het persbericht wordt zo dadelijk gepubliceerd.

Persbericht: Mede-oprichter 5.1.2.e vertrekt bij Fox-IT

5.1.2.e mede-oprichter van Fox-IT, legt per 1 januari 2018 zijn functie als directeur neer. 5.1.2.e heeft in 1999 samen met 5.1.2.e Fox-IT opgericht om op innovatieve wijze een waardevolle bijdrage te leveren aan het bestrijden van cybercriminaliteit. Fox-IT werd daarmee het eerste digitale forensisch onderzoeksbureau in Nederland. Onder de leiding van 5.1.2.e en 5.1.2.e groeide het bedrijf naar een omzet van 28,5 miljoen euro en werd het in 2015 overgenomen door NCC Group.

Fox-IT kiest er voor om de werkzaamheden van 5.1.2.e bij verschillende mensen binnen de organisatie neer te leggen. Een deel van zijn taken is de afgelopen periode reeds overgedragen binnen de organisatie. Na 1 januari 2018 blijft 5.1.2.e als adviseur verbonden aan Fox-IT.

5.1.2.e vindt dat het tijd is voor verandering. *"Ik ben er trots op dat Fox-IT een bepalende speler is geworden op gebied van cybersecurity. We zijn er tevens in geslaagd om mee te bewegen met de groei in de markt en door de overname door NCC Group zijn we ook in staat om internationaal verder uit te bouwen. Fox-IT is daarmee in een volgende fase gekomen, en voor mij wordt het tijd om verder te gaan. Cybersecurity is van een technisch issue een nationaal veiligheidsvraagstuk geworden. Bij andere instellingen zal ik mij dan ook blijven inzetten om Nederland digitaal veiliger te maken."*

5.1.2.e 5.1.2.e geeft aan dat hij 5.1.2.e ziet als de verpersoonlijking van het thema 'cybersecurity' in Nederland, een zeer bijzondere prestatie. *"Ik heb veel bewondering voor de wijze waarop hij cybersecurity op de kaart heeft gezet binnen de Nederlandse samenleving. Dit heeft er mede voor gezorgd dat Fox-IT als bedrijf is gegroeid naar de meest toonaangevende cybersecurity speler van Europa. Wat ooit begon als zijn persoonlijke missie wordt inmiddels gedragen door meer dan 300 medewerkers."*

De strategie is helder. Fox-IT breidt internationaal verder uit. Wij doen dit samen met NCC Group aan de hand van vier pijlers:

1. Wij doen de meest uitdagende en impactvolle opdrachten en doen zelfstandig onderzoek naar grote incidenten, zoals spionage door buitenlandse inlichtingendiensten.
2. Wij werken aan zeer hoogwaardige cryptografische oplossingen voor de bescherming van staatsgeheimen, waarbij deze oplossingen een steeds bredere toepassing krijgen.
3. Wij gebruiken onze kennis om te werken aan innovatieve en schaalbare cybersecurity oplossingen voor zowel klanten als partners.
4. Hierdoor zijn wij de meest aantrekkelijke werkgever voor hackers en security specialisten.

Als u vragen heeft naar aanleiding van deze mail, neem dan contact op met 5.1.2.e of uw contactpersoon bij Fox-IT.

Met vriendelijke groet,

5.1.2.e (5.1.2.e & 5.1.2.e 5.1.2.e

Verslag

Onderwerp

Concept-verslag Kiesraadvergadering 14 november 2022

KIESRAAD

Datum

14 november 2022

Blad

1 van 4

Bezoekadres

Zurichtoren, 14 etage
Muzenstraat 85
2511 WB Den Haag

Postadres

Postbus 20011
2500 EA Den Haag

Notulist

5.1.2.e

Locatie

Zurichtoren, Muzenstraat

Deelnemers

5.1.2.e ; 5.1.2.e 5.1.2.e 5.1.2.e
5.1.2.e ; 5.1.2.e ; 5.1.2.e 5.1.2.e 5.1.2.e
5.1.2.e 5.1.2.e ; 5.1.2.e
5.1.2.e 5.1.2.e en 5.1.2.e

1. Opening en vaststelling agenda

BR
5.1.2.e

2. Mededelingen

5.1.2.e deelt mee dat hij per 1 juli 2023 zijn werkzaamheden als lid van de Kiesraad vroegtijdig zal neerleggen in verband met langdurig verblijf in het buitenland.

BR

BR
5.1.2.e

5.1.2.e

BR 5.1.2.e

BR 5.1.2.e 5.1.2.e

3. 076 Verslag 10 oktober 2022 en actielijst

BR

BR

4. Hamerstukken

BR

BR

5. Advies, Kennis en Onderzoek

BR

BR

BR

BR [Redacted]

BR [Redacted]

5.1.2.e

BR [Redacted]

BR [Redacted]

6. BR [Redacted]

BR [Redacted]

BR



BR



BR



7. Rondvraag en sluiting

BR



KIESRAAD



Verslag

Onderwerp

Vastgesteld verslag van de Kiesraadvergadering van 15 januari 2018

SECRETARIAAT KIESRAAD

Datum

15 januari 2018

Blad

1 van 4

Notulist

5.1.2.e

Locatie

Muzenstraat 85

Aanwezigen

5.1.2.e, 5.1.2.e
5.1.2.e 5.1.2.e 5.1.2.e,
5.1.2.e 5.1.2.e, 5.1.2.e 5.1.2.e (bij agendapunten 1 en 2), 5.1.2.e (bij agendapunt 5), 5.1.2.e en 5.1.2.e (bij agendapunten 6 en 10).

Inlichtingen

Bezoekadres

Muzenstraat 85
2511 WB Den Haag

Postadres

Postbus 20011
2500 EA Den Haag

1. Opening en vaststelling agenda

BR

5.1.2.e

2. Mededelingen en actualiteiten

BR

5.1.2.e

5.1.2.e

BR

5.1.2.e

3. Conceptverslagen van de vergaderingen van 13 november 2017 en 11 december 2017

BR

4. BR

BR

5. BR

BR

5.1.2.e

5.1.2.e

BR

5.1.2.e

5.1.2.e

5.1.2.e

5.1.2.e

5.1.2.e

5.1.2.e

5.1.2.e

5.1.2.e

5.1.2.e

6. BR

BR

BR

7. BR

BR 5.1.2.e

8. Functieprofielen vacatures

De leden hebben kennisgenomen van de notitie en besluiten om één vacature specifiek te richten op personen met kennis van de verkiezingspraktijk en decentrale overheden. Voor de tweede vacature wordt in de vacaturetekst opgenomen dat kennis van ICT en cybersecurity een pré is. De aandachtsgebieden staan er volgens aanwezigen niet aan in de weg dat er ook nog andere factoren meespelen. Vanuit het secretariaat worden de functieomschrijvingen opgesteld. Hierin wordt niet speciaal gezocht naar een vice-voorzitter. De leden besluiten om binnen de Kiesraad in nieuwe samenstelling na te gaan wie als vice-voorzitter wordt aangewezen.

Besloten wordt om de selectiecommissie te laten bestaan uit de voorzitter, een vertegenwoordiger van BZK en 5.1.2.e als vertegenwoordiger van de Kiesraad. In adviserende rol wordt vanuit het secretariaat 5.1.2.e 5.1.2.e betrokken.

9. BR

BR

10. BR

BR

11. BR

BR

12. Ter informatie toegezonden stukken

BR

13. Media-artikelen

BR

14. Publicaties Staatscourant

BR

15. Rondvraag en sluiting

BR

KIESRAAD



Minister van Binnenlandse Zaken en Koninkrijksrelaties
t.a.v. 5.1.2.e
Postbus 20011
2500 EA Den Haag

KIESRAAD

Datum
25 mei 2018

Ons kenmerk
2018-0000299885

Inlichtingen
5.1.2.e
T 5.1.2.e

Onderwerp
Verslag sollicitatiecommissie vacatures Kiesraad

Uw kenmerk

Blad
1 van 3

Bezoekadres
Zurichtoren, 14 etage
Muzenstraat 85
2511 WB Den Haag

Postadres
Postbus 20011
2500 EA Den Haag

Internetadres
www.kiesraad.nl

E-mailadres
kiesraad@kiesraad.nl

Geachte minister Ollongren,

Per 1 oktober 2018 ontstaan, vanwege het bereiken van de maximale zittingstermijn van de leden 5.1.2.e en 5.1.2.e twee vacatures in de Kiesraad.

Met het oog op de vervulling van deze vacatures, heeft de Kiesraad functieprofielen opgesteld en met uw ministerie afgestemd. Verder is in overleg een sollicitatiecommissie samengesteld, bestaande uit:

- o 5.1.2.e voorzitter Kiesraad;
- o 5.1.2.e lid Kiesraad;
- o 5.1.2.e, 5.1.2.e ministerie Binnenlandse Zaken en Koninkrijksrelaties;
- o 5.1.2.e 5.1.2.e Kiesraad (adviserend lid).

In deze brief doet de sollicitatiecommissie verslag van de gevolgde procedure en onderbouwt zij haar keuze voor de twee kandidaten die door de commissie aan u voor benoeming worden voorgedragen.

Procedure

Op zaterdag 17 maart jl. is een advertentietekst over de vacatures gepubliceerd in drie landelijke dagbladen, te weten NRC Handelsblad, De Volkskrant en het Algemeen Dagblad, alsook op de website van de Kiesraad. Via de advertentietekst werd uitgenodigd tot het kenbaar maken van belangstelling tot vervulling van de vacatures. De sluitingstermijn voor het indienen van een brief en curriculum vitae was op 23 april jl.

Datum
25 mei 2018

Kenmerk
2018-0000299885

Onderdeel
Kiesraad

Blad
2 van 3

Tot en met 23 april 2018 zijn 79 sollicitatiebrieven (van 19 vrouwen en 60 mannen) ontvangen. Alle sollicitanten hebben een schriftelijke ontvangstbevestiging ontvangen van hun sollicitatiebrief.

Een preselectie van de 79 sollicitatiebrieven is gemaakt door de voorzitter en plv. secretaris-directeur van de Kiesraad. Op basis van deze beoordeling zijn 29 kandidaten (11 vrouwen en 18 mannen) voorgelegd aan alle leden van de selectiecommissie. De 29 brieven zijn vervolgens beoordeeld en besproken met de gehele sollicitatiecommissie.

Op basis van de gestelde criteria zijn 8 kandidaten (4 vrouwen en 4 mannen) geselecteerd en op gesprek uitgenodigd. Deze gesprekken hebben plaatsgevonden op 9 en 17 mei jl.

De sollicitatiecommissie komt op basis van de inhoud van de brieven en de gesprekken unaniem tot een (enkelvoudige) voordracht voor beide vacatures.

Beoordeling

Bij de beoordeling van de sollicitanten is gekeken naar de profielen zoals die eerder zijn opgesteld en afgestemd. Voor de twee vacatures zijn in het bijzonder uitgenodigd om te solliciteren personen die voldoen aan een of meer van de navolgende vereisten:

- (gemeentelijke) praktijkervaring met betrekking tot het verkiezingsproces;
- ervaring met ICT-processen en -toepassingen binnen de overheid.

Mede aan de hand van deze profielen zijn bij de beoordeling van de brieven de volgende criteria gehanteerd:

- Het kunnen leveren van een belangrijke bijdrage aan de onafhankelijke oordeelsvorming binnen de Raad;
- Een goed gevoel voor politiek-bestuurlijke verhoudingen;
- Kennis van het functioneren van de rijksoverheid en van de vertegenwoordigende organen;
- Affiniteit (en bij voorkeur ervaring) met het kiesrecht en verkiezingen.
- Het niet vervullen van een functie die onverenigbaar wordt geacht met het lidmaatschap van de Kiesraad. Het gaat dan om iedere functie die tot gereede twijfel zou kunnen leiden over de onafhankelijke en onpartijdige oordeelsvorming door de Kiesraad.

Bij de beoordeling is tot slot het streven naar evenredige participatie in de Raad van mannen en vrouwen en deelname van personen behorende tot minderheidsgroepen betrokken.

Voordracht

U zal op de hoogte worden gebracht van de namen van de twee kandidaten die de sollicitatiecommissie voor benoeming aan u wil voordragen door ^{5.1.2.e}

^{5.1.2.e} De sollicitatiecommissie is van mening dat beide voorgestelde

Datum
25 mei 2018

Kenmerk
2018-0000299885

Onderdeel
Kiesraad

Blad
3 van 3

kandidaten in voldoende mate, en zelfs op onderdelen in (zeer) ruime zin, aan de gestelde criteria voldoen.

De voorgestelde kandidaat voor het functieprofiel over (gemeentelijke) praktijkervaring met betrekking tot het verkiezingsproces voldoet in het bijzonder aan het opgestelde profiel omdat zij:

- mede door haar ervaring als Directeur Verkiezingen bij een grote gemeente, beschikt over relevante ervaring met en actuele kennis van de organisatie van verkiezingen, alsook de uitdagingen die het verkiezingsproces in de praktijk met zich meebrengt;
- mede vanwege haar analytische denkvermogen, in staat wordt geacht een bijdrage te leveren aan de onafhankelijke oordeelsvorming binnen de Raad.

De voorgestelde kandidaat voor het functieprofiel waarin gevraagd wordt naar ervaring met ICT-processen en toepassingen binnen de overheid voldoet in het bijzonder aan het opgestelde profiel omdat hij:

- mede vanuit zijn (vorige) functie als Non executive board member van een cybersecuritybedrijf als dé deskundige te boek staat op het gebied van veiligheidsvraagstukken op dat terrein.
- mede omdat hij over uitgebreide ervaring beschikt over het functioneren van de rijksoverheid in die gevallen waar grote belangen op het gebied van (de beveiliging van) ICT-processen en – toepassingen een rol spelen;
- mede door zijn lidmaatschap (c.q. voorzitterschap) van een drietal commissies over het gebruik van ICT in het verkiezingsproces, blijkt geeft van een groot affiniteit met het verkiezingsproces;
- mede vanwege zijn analytische denkvermogen, in staat wordt geacht een bijdrage te leveren aan de onafhankelijke oordeelsvorming binnen de Raad.

Hoogachtend,
mede namens de andere leden van de sollicitatiecommissie,

5.1.2.e



KIESRAAD



Notitie

Onderwerp

Functieprofielen vacatures Kiesraad

Datum

9 januari 2018

Kenmerk

2017-0000601499

Onderdeel

Kiesraad

Inlichtingen

5.1.2.e

T 5.1.2.e

Blad

1 van 3

Aan

Voorzitter en leden

Van

5.1.2.e

Inleiding

Per 1 oktober 2018 ontstaan, vanwege het bereiken van de maximale zittingstermijn van de leden 5.1.2.e en 5.1.2.e twee vacatures in de Kiesraad.

Aangezien het van belang is om tijdig nieuwe leden te kunnen benoemen, is het wenselijk vast stil te staan bij de te volgen procedure, de bijbehorende planning en de gewenste functieprofielen. In deze notitie worden daartoe enkele voorstellen gedaan.

Procedure

De volgende procedure wordt voorgesteld:

- Het vervullen van de vacatures Kiesraad begint met het vaststellen van het functieprofiel. Het secretariaat van de Kiesraad doet hiertoe een voorstel, dat vervolgens in de vergadering wordt besproken en vastgesteld.
- Het functieprofiel wordt vervolgens gedeeld met BZK.
- De desbetreffende vacatures wordt opengesteld door de voorzitter van de Kiesraad. In het geval de vacature van de voorzitter zelf betreft, dan wordt de vacature opengesteld door de vicevoorzitter.
- De vacatures worden gepubliceerd in een tweetal landelijke dagbladen (NRC en Volkskrant), in enkele vakbladen, alsook op de website van de Kiesraad.
- Het is vervolgens gebruikelijk dat een selectiecommissie bestaande uit enkele leden van de Kiesraad, de 5.1.2.e en een vertegenwoordiger van BZK zich buigen over de opengestelde vacatures en daarop binnengekomen reacties.

De huidige bij vacatures te volgen procedure is enige tijd geleden onderwerp van bespreking geweest met BZK. De huidige 5.1.2.e heeft uiteindelijk aangegeven geen behoefte te hebben om de procedure te wijzigen. Wij gaan er dus vanuit dat de twee vacatures worden vervuld op de gebruikelijke wijze, waarbij de Kiesraad 'in the lead' is en waarbij BZK participeert met één lid in de selectiecommissie. Wel gaan wij ervan uit dat het BZK lid van de selectiecommissie

de minister tussentijds zal informeren over de richting die het op gaat en over evt. gevoeligheden tijdig terugkoppelt naar de selectiecommissie.

Planning

Bij de meest recente vacaturevervulling is ervaring opgedaan met het eerder meelopen van nieuwe leden voorafgaande aan hun formele benoeming. Voorgesteld wordt om de twee nieuwe leden ook alvast per augustus 2018 voor de Kiesraadvergaderingen uit te nodigen.

Indien dit voorstel wordt overgenomen dan wordt de volgende planning voorgesteld:

februari	Bespreking advertentietekst in KR vergadering
medio maart	Publicatie advertentietekst
medio april	Laatste dag insturen reacties
eind april	Selectie uit te nodigen kandidaten
medio mei	Gesprekken met kandidaten
eind mei	Keuze kandidaten, informeren Kiesraad en minister BZK
juni	Voordracht aan Z.H. de Koning (via Ministerraad)
juni	Mededeling aan benoemde leden Kiesraad
v.a. augustus	Aanwezigheid nieuwe leden bij vergaderingen Kiesraad

Functieprofielen

Met het oog op het naderende vertrek van twee leden is het van belang in kaart te brengen welke kennis, deskundigheid en ervaring de Kiesraad voor zijn taakuitvoering nodig heeft.

In het verleden zijn de volgende – meer algemene – aandachtvelden benoemd:

1. *Kennis van het staatsrecht en in het bijzonder van het kiesrecht en het kiesproces.*
2. *Politiek-wetenschappelijke kennis en kennis van en ervaring met relevant politiek sociaal-wetenschappelijk onderzoek.*
3. *Kennis van en ervaring met betrekking tot de praktijk van verkiezingen.*
4. *Kennis van en ervaring met betrekking tot politiek-bestuurlijke verhoudingen en het functioneren van de rijksoverheid.*

Daarnaast zijn in het verleden enkele meer specifieke aandachtvelden benoemd:

5. *Kennis van en ervaring met betrekking tot ICT (en cybersecurity).*
6. *Kennis van overheidsfinanciën.*
7. *Kennis van en ervaring met internationaal kiesrecht en verkiezingen.*
8. *Kennis van en ervaring met toezicht(arrangementen).*

Gegeven het vertrek van ^{5.1.2.e} lijkt in ieder geval behoefte te bestaan aan versterking van kennis van en ervaring met betrekking tot de praktijk van verkiezingen. Met een dergelijk profiel is het aannemelijk dat ook mensen zullen reageren die verstand hebben van het kiesrecht en het kiesproces. Het secretariaat stelt om die reden dan ook voor deze punten (1 en 3) in een van de functieprofielen op te nemen.

Wat betreft de vervulling van de vacature die ontstaat vanwege het vertrek van 5.1.2.e

5.1.2.e zijn er verschillende opties.

- A. Volstaan zou kunnen worden met een verwijzing naar de meer algemenere functie-eisen (nrs. 1-4).

- B. Naast de meer algemenere eisen zou ook aanvullend kunnen worden gevraagd naar een meer specifiek functieprofiel. Bij de toenmalige benoeming van 5.1.2.e was bijvoorbeeld kennis van en ervaring met toezicht(arrangementen) een aandachtspunt i.v.m.de toezichtsrol die de Kiesraad zou krijgen bij de uitvoering van de Wet Financiering Politieke Partijen. Inmiddels is duidelijk dat de Kiesraad geen rol heeft gekregen bij de uitvoering van deze wet. Alhoewel toezicht ook in het verkiezingsproces een blijvende punt van aandacht is, is er alles afwegende wellicht minder noodzaak dit opnieuw als belangrijk aandachtspunt te benoemen. Ook een van de andere hierboven genoemde, meer specifieke, aandachtspunten zou kunnen worden benoemd, waarbij het secretariaat gezien de huidige samenstelling van de Kiesraad (zowel leden als secretariaat) en de huidige kwetsbaarheden, voorstelt om kennis van en ervaring met betrekking tot ICT en cybersecurity als aandachtsgebied te benoemen. Het benoemen van een specifiek aandachtsveld heeft echter alleen meerwaarde als dit criterium vervolgens bij de selectie ook (zwaar) meeweegt.

Naast de functieprofielen zou ervoor kunnen worden gekozen om wenselijke (kern)competenties te vermelden. Gedacht kan worden aan de kerncompetenties: integer, (onafhankelijke) oordeelsvorming, analytisch vermogen en samenwerken.

Vervolg

Met het aanstaande vertrek van 5.1.2.e wordt ook de functie van vicevoorzitter vacant. Het ligt naar het oordeel van het secretariaat voor de hand dat deze gezocht wordt onder de huidige leden en niet onder de nieuw te benoemen leden. Voorgesteld wordt hier in de februarivergadering op terug te komen. Tevens kan er dan bij worden stilgestaan welke leden deel gaan uitmaken van de selectiecommissie, gegeven ook de alsdan vastgestelde functieprofielen.

KIESRAAD



De minister van Binnenlandse Zaken en Koninkrijksrelaties
Postbus 20011
2500 EA Den Haag

KIESRAAD

Datum
4 mei 2022

Ons kenmerk
2022-0000201499

Inlichtingen
5.1.2.e
T 5.1.2.e

Uw kenmerk

Blad
1 van 1

Bezoekadres
Zurichtoren, 14 etage
Muzenstraat 85
2511 WB Den Haag

Postadres
Postbus 20011
2500 EA Den Haag

Internetadres
www.kiesraad.nl

E-mailadres
kiesraad@kiesraad.nl

Onderwerp
Herbenoeming leden Kiesraad

Geachte mevrouw Bruins Slot,

Op 1 oktober 2022 zal de termijn verstreken zijn waarvoor 5.1.2.e
5.1.2.e en 5.1.2.e als lid van de Kiesraad zijn
benoemd.¹ Beide leden hebben aangegeven graag voor herbenoeming in
aanmerking te komen. De Kiesraad beveelt aan zowel 5.1.2.e
als 5.1.2.e te herbenoemen voor een nieuwe periode van vier jaar. Deze
herbenoeming, die voor de eerste maal zal zijn, wordt volledig door de overige
leden van de Kiesraad ondersteund.

Indien u met de herbenoemingen instemt, verzoeken wij u te bevorderen dat deze
op kort termijn wordt gerealiseerd, zodat de continuïteit met ingang van 1 oktober
a.s. gewaarborgd is.

De Kiesraad,
voor deze,

5.1.2.e

W.J. Kuijken,
voorzitter

5.1.2.e

5.1.2.e

secretaris-directeur

¹ Koninklijk Besluit van 5 juli 2018, nrs. 2018001204 en 2018001205.

Bijlage 2 Strategiedag – onderdeel perscommunicatie (Leidraad externe contacten leden Kiesraad)

Leidraad externe contacten en nevenactiviteiten Kiesraad

In een recente vergadering van de Kiesraad werd gerefereerd aan een notitie waarin afspraken over persvragen richting Kiesraadleden zijn neergelegd. Gedoeld werd op een Leidraad externe contacten leden Kiesraad d.d. 10-05-2006. Deze leidraad, die overigens ook ingaat op nevenactiviteiten van Kiesraadleden, bleek inmiddels op punten verouderd en is hier om die reden en waar nodig geactualiseerd.

Perscontacten

1. Vragen van media over Kiesraad-gerelateerde kwesties worden in beginsel door de voorzitter of secretaris-directeur beantwoord, dan wel door de persvoorlichter (in overleg met de secretaris-directeur).
2. Bij vragen van media aan Kiesraadleden over politiek-gevoelige Kiesraadgerelateerde kwesties wordt doorverwezen naar de voorzitter of secretaris-directeur.
3. Bij vragen van media aan Kiesraadleden over kiesrechtelijke, verkiezingstechnische onderwerpen wordt doorverwezen naar de secretaris-directeur dan wel de persvoorlichter.
4. Namens de Kiesraad wordt in beginsel alleen door de voorzitter of secretaris-directeur gesproken, dan wel door de persvoorlichter (in overleg met de secretaris-directeur).
5. Bij het uitdragen van standpunten in de (vak)media geldt als algemene richtsnoer dat het aanzien en het gezag van de Kiesraad geen schade wordt toegebracht. Het uitgangspunt van collegiale advisering en besluitvorming is leidend.
6. Zo lang er niet een directe link is dan wel wordt gelegd met het Kiesraadlidmaatschap, zijn Kiesraadleden vrij in het uitdragen van wetenschappelijke, politieke etc. standpunten. Bij onderwerpen die recentelijk of op korte termijn in de Kiesraad aan de orde zijn (geweest) wordt extra terughoudendheid betracht.

Nevenactiviteiten

1. Bij het verrichten van nevenactiviteiten geldt als algemene richtsnoer dat het aanzien en gezag van de Kiesraad geen schade wordt toegebracht.
2. Leden verrichten geen werkzaamheden ten behoeve van dienstverlening door ondernemingen aan de Kiesraad of andere kieswettelijke instanties op decentraal niveau als onze dienstverlening in concurrentieverhouding wordt uitgeoefend.
3. Persoonlijke en directe dienstverlening aan publieke instellingen, ook als deze tegen betaling wordt verricht, bijvoorbeeld advisering of onderwijs, is toegestaan, mits deze niet wordt gepresenteerd als een activiteit van de Kiesraad of vanwege de Kiesraad door een lid.
4. (Nieuwe) hoofd- dan wel nevenactiviteiten worden gemeld aan de voorzitter.



FOX IT
part of nccgroup

Aan: De Kiesraad
Auteurs: 5.1.2.e en 5.1.2.e
Betreft: Overzicht bevindingen Rapport PR-180188,
Hertest OSV versie 2.24.1 en Hertest OSV versie 2.24.5
Ref. nr. PR-180188
Datum: 22 november 2019
Classificatie: PUBLIC
Status: Definitief
Versie: 1.0

Inleiding

De Kiesraad heeft Fox-IT in maart 2019 om een beveiligingsonderzoek van de OSV-programmatuur gevraagd, gevolgd door een hertest in april 2019 en november 2019. Dit document bevat een lijst met de huidige status van alle bevindingen uit het onderzoek en de hertests.

for a more secure society

FOX-IT BV
Olof Palmestraat 6, Delft
POSTBUS 638, 2600 AP Delft

T +31 (0)15 284 79 99
F +31 (0)15 284 79 90
ABN AMRO 554697041
KVK Haaglanden 27301624

FOX-IT.COM

Huidige status bevindingen

Onderstaande tabel geeft de status van de bevindingen uit alle voorgaande onderzoeken weer, waarbij de kleur geel aangeeft dat een bevinding gedeeltelijk is opgelost en groen dat een bevinding in zijn geheel is opgelost voor zover dit door Fox-IT vastgesteld kon worden. Een blauwe kleur geeft aan dat de bevinding zelf niet is opgelost, maar dat deze op een andere manier gemitigeerd is.

Bevinding	Huidig Risico	Status na hertest Q4 2019	Verwijzing
Niet ondersteunde software in gebruik / Unsupported and old Jboss and Java SE software used	GEMIDDELD	Deels opgelost	Onderzoek Fox-IT 2017, bevinding 2 Security-assessment-of-Dutch-election-software-OSV, par. 4.1.4 (p. 29)
HMAC-controle is te omzeilen	LAAG	Deels opgelost	RAP_Kiesraad_PR180188_Beveiligingsonderzoek OSV-PUBLIC
Stand-alone OSV installation is risky	LAAG	Deels opgelost	Security-assessment-of-Dutch-election-software-OSV, par. 4.1.7 (p. 35)
Transport door middel van USB-sticks	LAAG	Deels opgelost	Onderzoek Fox-IT 2017, bevinding 6
Incomplete source code and unsigned binary code	LAAG	Deels opgelost	Onderzoek VUsec, par. 6, issue 1
Improve protection against XSS (OSV P4 and P5)	LAAG	Deels opgelost	MEMO_Kiesraad_PR180188_Hertest_2019Q2_1.0
Unnecessary ports are opened by Java	LAAG	Gemitigeerd	Security-assessment-of-Dutch-election-software-OSV, par. 4.1.3 (p. 26)
Overige tekortkomingen OSV	LAAG	Gemitigeerd	Onderzoek Fox-IT 2017, bevinding 11, sub 4



Bevinding	Huidig Risico	Status na herrest Q4 2019	Verwijzing
Prevent showing stacktrace and server info to the user (OSV P4 and P5)	-	Opgelost	MEMO_Kiesraad_PR180188_Hertest_2019Q2_1.0,
Privilege escalation vulnerability (second HMAC bypass)	-	Opgelost	MEMO_Kiesraad_PR180188_Hertest_2019Q2_1.0
Onvoldoende autorisatiecontrole	-	Opgelost	RAP_Kiesraad_PR180188_Beveiligingsonderzoek OSV-PUBLIC, MEMO_Kiesraad_PR180188_Hertest_2019Q4_1.0
Persistent Cross-Site Scripting (XSS)	-	Opgelost	RAP_Kiesraad_PR180188_Beveiligingsonderzoek OSV-PUBLIC
Pagina's bereikbaar zonder authenticatie	-	Opgelost	RAP_Kiesraad_PR180188_Beveiligingsonderzoek OSV-PUBLIC, MEMO_Kiesraad_PR180188_Hertest_2019Q4_1.0
Gedetailleerde stack traces	-	Opgelost	RAP_Kiesraad_PR180188_Beveiligingsonderzoek OSV-PUBLIC
Verkiezingsleider is not allowed to enter polling station results (P4_PSB)	-	Opgelost	MEMO_Kiesraad_PR180188_Hertest_2019Q2_1.0
Verkiezingsleider is not allowed to enter municipality results (P4_HSB)	-	Opgelost	MEMO_Kiesraad_PR180188_Hertest_2019Q2_1.0
Verkiezingsleider is not allowed to enter kieskring results (P4_CSB)	-	Opgelost	MEMO_Kiesraad_PR180188_Hertest_2019Q2_1.0
OSV database isn't protected by a password		Opgelost	Security-assessment-of-Dutch-election-software-OSV, par. 4.1.3 (p. 41)
OSV database can be easily modified and votes can be changed		Opgelost	Security-assessment-of-Dutch-election-software-OSV, par. 4.1.3 (p. 22)



Bevinding	Huidig Risico	Status na herrest Q4 2019	Verwijzing
Modified EML files in archive directory on the server aren't detected		Opgelost	Security-assessment-of-Dutch-election-software-OSV, par. 4.1.3 (p. 43)
Willekeurige bestanden kunnen geüpload worden	-	Opgelost	RAP_Kiesraad_PR180188_Beveiligingsonderzoek OSV-PUBLIC
Gevoelige informatie in logbestand	-	Opgelost	RAP_Kiesraad_PR180188_Beveiligingsonderzoek OSV-PUBLIC
SHA256-hash controle kan omzeild worden	-	Opgelost	RAP_Kiesraad_PR180188_Beveiligingsonderzoek OSV-PUBLIC
SSL version 3.0 is detected	-	Opgelost	Security-assessment-of-Dutch-election-software-OSV, par. 4.1.14 (p. 40)
Password policy not enforced: one letter passwords possible	-	Opgelost	Security-assessment-of-Dutch-election-software-OSV, par. 4.1.22 (p. 51)
OSV can be run on an unencrypted HTTP connection on port 8080	-	Opgelost	Security-assessment-of-Dutch-election-software-OSV, par. 4.1.23 (p. 52)
jQuery security updates are missing	-	Opgelost	Security-assessment-of-Dutch-election-software-OSV, par. 4.1.29 (p. 59)
OSV database software Derby is missing security updates	-	Opgelost	Security-assessment-of-Dutch-election-software-OSV, par. 4.1.31 (p. 60)
Checking the integrity of the CD-ROM file is optional	-	Opgelost	Security-assessment-of-Dutch-election-software-OSV, par. 4.1.35 (p. 64)
Password hashing and login	-	Opgelost	Onderzoek VUsec, par. 6, issue 2



Bevinding	Huidig Risico	Status na herrest Q4 2019	Verwijzing
OSV-webapplicatie toegankelijk zonder verbodings-versleuteling	-	Opgelost	Onderzoek Fox-IT 2017, bevinding 1
Werkwijze wachtwoorden onveilig	-	Opgelost	Onderzoek Fox-IT 2017, bevinding 4
Verificatie integriteit EML-bestanden onvoldoende	-	Opgelost	Onderzoek Fox-IT 2017, bevinding 5
Integriteitscontrole OSV installatie-cd-rom kan omzeild worden	-	Opgelost	Onderzoek Fox-IT 2017, bevinding 7
XML External Entity Injection (XXE)	-	Opgelost	Onderzoek Fox-IT 2017, bevinding 8
Vier-ogen-principe wordt niet afgedwongen	-	Opgelost	Onderzoek Fox-IT 2017, bevinding 9
Niet geverifieerde externe software vereist	-	Opgelost	Onderzoek Fox-IT 2017, bevinding 10
Browser back button works even if user is logged out (HTML code can be cached)	-	Opgelost	Security-assessment-of-Dutch-election-software-OSV, par. 4.1.21 (p. 49)
No restriction on JavaScript usage via Content Security Policy	-	Opgelost	Security-assessment-of-Dutch-election-software-OSV, par. 4.1.27 (p. 52)
Integer overflow	-	Opgelost	Onderzoek VUsec, par. 5, issue 1
XML schema validation and application checks bypass	-	Opgelost	Onderzoek VUsec, par. 5, issue 2



Bevinding	Huidig Risico	Status na hertest Q4 2019	Verwijzing
Election definition and XSS	-	Opgelost	Onderzoek VUsec, par. 5, issue 4
Publication of e-mail addresses	-	Opgelost	Security-assessment-of-Dutch-election-software-OSV, par. 4.5.2 (p. 75)
Strict Transport Security isn't enabled	-	Opgelost	Security-assessment-of-Dutch-election-software-OSV, par. 4.1.24 (p. 54)
Prevent the access of other .jsp sites (OSV P4 and P5)	-	Opgelost	MEMO_Kiesraad_PR180188_Hertest_2019Q2_1.0
Control the authorization of a user if he/she opens a page or performs an action	-	Opgelost	MEMO_Kiesraad_PR180188_Hertest_2019Q2_1.0
Prevent access without authentication to pages	-	Opgelost	MEMO_Kiesraad_PR180188_Hertest_2019Q2_1.0
Prevent that result is set by single result file import in P4_HSB and P4_CSB	-	Opgelost	MEMO_Kiesraad_PR180188_Hertest_2019Q2_1.0
OSV-2121 Control the authorization of a user if he/she performs an action	-	Opgelost	MEMO_Kiesraad_PR180188_Hertest_2019Q2_1.0



FOX IT
part of nccgroup

Aan: De Kiesraad
Auteurs: 5.1.2.e en 5.1.2.e
Betreft: Hertest OSV versie 2.24.5 – Bijlage
Ref. nr. PR-180188
Datum: 11 november 2019
Classificatie: PUBLIC
Status: Definitief
Versie: 1.0

Inleiding

De Kiesraad heeft Fox-IT gevraagd om een hertest uit te voeren van de hieronder genoemde bevindingen. Dit document betreft een bijlage van het memorandum van 08-11-2019 versie 1.0 en bevat een lijst met de huidige status van alle bevindingen uit de voorgaande onderzoeken. De hertest was beperkt tot het testen van de genoemde bevindingen en het bepalen of deze als opgelost beschouwd kunnen worden. Tijdens de hertest is geen verder onderzoek verricht naar eventuele nieuwe kwetsbaarheden.

for a more secure society

FOX-IT BV
Olof Palmestraat 6, Delft
POSTBUS 638, 2600 AP Delft

T +31 (0)15 284 79 99
F +31 (0)15 284 79 90
ABN AMRO 554697041
KVK Haaglanden 27301624

FOX-IT.COM

Huidige status bevindingen

Onderstaande tabel geeft de status van de bevindingen uit alle voorgaande onderzoeken weer, waarbij de kleur geel aangeeft dat een bevinding gedeeltelijk is opgelost en groen dat een bevinding in zijn geheel is opgelost voor zover dit door Fox-IT vastgesteld kon worden. Een blauwe kleur geeft aan dat de bevinding zelf niet is opgelost, maar dat deze op een andere manier gemitigeerd is.

Bevinding	Huidig Risico	Status na hertest Q4 2019	Verwijzing
HMAC-controle is te omzeilen	LAAG	Deels opgelost	RAP_Kiesraad_PR180188_Beveiligingsonderzoek OSV-PUBLIC
Stand-alone OSV installation is risky	LAAG	Deels opgelost	Security-assessment-of-Dutch-election-software-OSV, par. 4.1.7 (p. 35)
Niet ondersteunde software in gebruik / Unsupported and old Jboss and Java SE software used	GEMIDDELD	Deels opgelost	Onderzoek Fox-IT 2017, bevinding 2 Security-assessment-of-Dutch-election-software-OSV, par. 4.1.4 (p. 29)
Transport door middel van USB-sticks	LAAG	Deels opgelost	Onderzoek Fox-IT 2017, bevinding 6
Incomplete source code and unsigned binary code	LAAG	Deels opgelost	Onderzoek VUsec, par. 6, issue 1
Prevent showing stacktrace and server info to the user (OSV P4 and P5)	-	Opgelost	MEMO_Kiesraad_PR180272_Hertest_2019Q2_1.0
Improve protection against XSS (OSV P4 and P5)	-	Deels opgelost	MEMO_Kiesraad_PR180272_Hertest_2019Q2_1.0
Privilege escalation vulnerability (second HMAC bypass)	-	Opgelost	MEMO_Kiesraad_PR180272_Hertest_2019Q2_1.0



Bevinding	Huidig Risico	Status na herrest Q4 2019	Verwijzing
Unnecessary ports are opened by Java	LAAG	Gemitigeerd	Security-assessment-of-Dutch-election-software-OSV, par. 4.1.3 (p. 26)
Overige tekortkomingen OSV	LAAG	Gemitigeerd	Onderzoek Fox-IT 2017, bevinding 11, sub 4
Onvoldoende autorisatiecontrole	-	Opgelost	RAP_Kiesraad_PR180188_Beveiligingsonderzoek OSV-PUBLIC
Persistent Cross-Site Scripting (XSS)	-	Opgelost	RAP_Kiesraad_PR180188_Beveiligingsonderzoek OSV-PUBLIC
Pagina's bereikbaar zonder authenticatie	-	Opgelost	RAP_Kiesraad_PR180188_Beveiligingsonderzoek OSV-PUBLIC
Gedetailleerde stack traces	-	Opgelost	RAP_Kiesraad_PR180188_Beveiligingsonderzoek OSV-PUBLIC
Verkiezingsleider is not allowed to enter polling station results (P4_PSB)	-	Opgelost	MEMO_Kiesraad_PR180272_Hertest_2019Q2_1.0
Verkiezingsleider is not allowed to enter municipality results (P4_HSB)	-	Opgelost	MEMO_Kiesraad_PR180272_Hertest_2019Q2_1.0
Verkiezingsleider is not allowed to enter kieskring results (P4_CSB)	-	Opgelost	MEMO_Kiesraad_PR180272_Hertest_2019Q2_1.0
Willekeurige bestanden kunnen geüpload worden	-	Opgelost	RAP_Kiesraad_PR180188_Beveiligingsonderzoek OSV-PUBLIC
Gevoelige informatie in logbestand	-	Opgelost	RAP_Kiesraad_PR180188_Beveiligingsonderzoek OSV-PUBLIC



Bevinding	Huidig Risico	Status na herrest Q4 2019	Verwijzing
SHA256-hash controle kan omzeild worden	-	Opgelost	RAP_Kiesraad_PR180188_Beveiligingsonderzoek OSV-PUBLIC
SSL version 3.0 is detected	-	Opgelost	Security-assessment-of-Dutch-election-software-OSV, par. 4.1.14 (p. 40)
Password policy not enforced: one letter passwords possible	-	Opgelost	Security-assessment-of-Dutch-election-software-OSV, par. 4.1.22 (p. 51)
OSV can be run on an unencrypted HTTP connection on port 8080	-	Opgelost	Security-assessment-of-Dutch-election-software-OSV, par. 4.1.23 (p. 52)
jQuery security updates are missing	-	Opgelost	Security-assessment-of-Dutch-election-software-OSV, par. 4.1.29 (p. 59)
OSV database software Derby is missing security updates	-	Opgelost	Security-assessment-of-Dutch-election-software-OSV, par. 4.1.31 (p. 60)
Checking the integrity of the CD-ROM file is optional	-	Opgelost	Security-assessment-of-Dutch-election-software-OSV, par. 4.1.35 (p. 64)
Password hashing and login	-	Opgelost	Onderzoek VUsec, par. 6, issue 2
OSV-webapplicatie toegankelijk zonder verbindings-versleuteling	-	Opgelost	Onderzoek Fox-IT 2017, bevinding 1
Werkwijze wachtwoorden onveilig	-	Opgelost	Onderzoek Fox-IT 2017, bevinding 4
Verificatie integriteit EML-bestanden onvoldoende	-	Opgelost	Onderzoek Fox-IT 2017, bevinding 5



Bevinding	Huidig Risico	Status na herctest Q4 2019	Verwijzing
Integriteitscontrole OSV installatie-cd-rom kan omzeild worden	-	Opgelost	Onderzoek Fox-IT 2017, bevinding 7
XML External Entity Injection (XXE)	-	Opgelost	Onderzoek Fox-IT 2017, bevinding 8
Vier-ogen-principe wordt niet afgedwongen	-	Opgelost	Onderzoek Fox-IT 2017, bevinding 9
Niet geverifieerde externe software vereist	-	Opgelost	Onderzoek Fox-IT 2017, bevinding 10
Browser back button works even if user is logged out (HTML code can be cached)	-	Opgelost	Security-assessment-of-Dutch-election-software-OSV, par. 4.1.21 (p. 49)
No restriction on JavaScript usage via Content Security Policy	-	Opgelost	Security-assessment-of-Dutch-election-software-OSV, par. 4.1.27 (p. 52)
Integer overflow	-	Opgelost	Onderzoek VUsec, par. 5, issue 1
XML schema validation and application checks bypass	-	Opgelost	Onderzoek VUsec, par. 5, issue 2
Election definition and XSS	-	Opgelost	Onderzoek VUsec, par. 5, issue 4
Publication of e-mail addresses	-	Opgelost	Security-assessment-of-Dutch-election-software-OSV, par. 4.5.2 (p. 75)
Strict Transport Security isn't enabled	-	Opgelost	Security-assessment-of-Dutch-election-software-OSV, par. 4.1.24 (p. 54)



Bevinding	Huidig Risico	Status na herctest Q4 2019	Verwijzing
Prevent the access of other .jsp sites (OSV P4 and P5)	-	Opgelost	MEMO_Kiesraad_PR180272_Hertest_2019Q2_1.0
Control the authorization of a user if he/she opens a page or performs an action	-	Opgelost	MEMO_Kiesraad_PR180272_Hertest_2019Q2_1.0
Prevent access without authentication to pages	-	Opgelost	MEMO_Kiesraad_PR180272_Hertest_2019Q2_1.0
Prevent that result is set by single result file import in P4_HSB and P4_CSB	-	Opgelost	MEMO_Kiesraad_PR180272_Hertest_2019Q2_1.0
OSV-2121 Control the authorization of a user if he/she performs an action	-	Opgelost	MEMO_Kiesraad_PR180272_Hertest_2019Q2_1.0



FOX IT
part of nccgroup

Aan: De Kiesraad
Auteurs: 5.1.2.e en 5.1.2.e
Betreft: Overzicht bevindingen Rapport PR-180188,
Hertest OSV versie 2.24.1 en Hertest OSV versie 2.24.5
Ref. nr. PR-180188
Datum: 13 november 2019
Classificatie: PUBLIC
Status: Definitief
Versie: 1.0

Inleiding

De Kiesraad heeft Fox-IT in maart 2019 om een beveiligingsonderzoek van de OSV-programmatuur gevraagd, gevolgd door een hertest in april 2019 en november 2019. Dit document bevat een lijst met de huidige status van alle bevindingen uit de onderzoek en de hertests.

for a more secure society

FOX-IT BV
Olof Palmestraat 6, Delft
POSTBUS 638, 2600 AP Delft

T +31 (0)15 284 79 99
F +31 (0)15 284 79 90
ABN AMRO 554697041
KVK Haaglanden 27301624

FOX-IT.COM

Huidige status bevindingen

Onderstaande tabel geeft de status van de bevindingen uit alle voorgaande onderzoeken weer, waarbij de kleur geel aangeeft dat een bevinding gedeeltelijk is opgelost en groen dat een bevinding in zijn geheel is opgelost voor zover dit door Fox-IT vastgesteld kon worden. Een blauwe kleur geeft aan dat de bevinding zelf niet is opgelost, maar dat deze op een andere manier gemitigeerd is.

Bevinding	Huidig Risico	Status na hertest Q4 2019	Verwijzing
Niet ondersteunde software in gebruik / Unsupported and old Jboss and Java SE software used	GEMIDDELD	Deels opgelost	Onderzoek Fox-IT 2017, bevinding 2 Security-assessment-of-Dutch-election-software-OSV, par. 4.1.4 (p. 29)
HMAC-controle is te omzeilen	LAAG	Deels opgelost	RAP_Kiesraad_PR180188_Beveiligingsonderzoek OSV-PUBLIC
Stand-alone OSV installation is risky	LAAG	Deels opgelost	Security-assessment-of-Dutch-election-software-OSV, par. 4.1.7 (p. 35)
Transport door middel van USB-sticks	LAAG	Deels opgelost	Onderzoek Fox-IT 2017, bevinding 6
Incomplete source code and unsigned binary code	LAAG	Deels opgelost	Onderzoek VUsec, par. 6, issue 1
Improve protection against XSS (OSV P4 and P5)	LAAG	Deels opgelost	MEMO_Kiesraad_PR180188_Hertest_2019Q2_1.0
Unnecessary ports are opened by Java	LAAG	Gemitigeerd	Security-assessment-of-Dutch-election-software-OSV, par. 4.1.3 (p. 26)
Overige tekortkomingen OSV	LAAG	Gemitigeerd	Onderzoek Fox-IT 2017, bevinding 11, sub 4



Bevinding	Huidig Risico	Status na herctest Q4 2019	Verwijzing
Prevent showing stacktrace and server info to the user (OSV P4 and P5)	-	Opgelost	MEMO_Kiesraad_PR180188_Hertest_2019Q2_1.0
Privilege escalation vulnerability (second HMAC bypass)	-	Opgelost	MEMO_Kiesraad_PR180188_Hertest_2019Q2_1.0
Onvoldoende autorisatiecontrole	-	Opgelost	RAP_Kiesraad_PR180188_Beveiligingsonderzoek OSV-PUBLIC
Persistent Cross-Site Scripting (XSS)	-	Opgelost	RAP_Kiesraad_PR180188_Beveiligingsonderzoek OSV-PUBLIC
Pagina's bereikbaar zonder authenticatie	-	Opgelost	RAP_Kiesraad_PR180188_Beveiligingsonderzoek OSV-PUBLIC
Gedetailleerde stack traces	-	Opgelost	RAP_Kiesraad_PR180188_Beveiligingsonderzoek OSV-PUBLIC
Verkiezingsleider is not allowed to enter polling station results (P4_PSB)	-	Opgelost	MEMO_Kiesraad_PR180188_Hertest_2019Q2_1.0
Verkiezingsleider is not allowed to enter municipality results (P4_HSB)	-	Opgelost	MEMO_Kiesraad_PR180188_Hertest_2019Q2_1.0
Verkiezingsleider is not allowed to enter kieskring results (P4_CSB)	-	Opgelost	MEMO_Kiesraad_PR180188_Hertest_2019Q2_1.0
Willekeurige bestanden kunnen geüpload worden	-	Opgelost	RAP_Kiesraad_PR180188_Beveiligingsonderzoek OSV-PUBLIC
Gevoelige informatie in logbestand	-	Opgelost	RAP_Kiesraad_PR180188_Beveiligingsonderzoek OSV-PUBLIC



Bevinding	Huidig Risico	Status na herctest Q4 2019	Verwijzing
SHA256-hash controle kan omzeild worden	-	Opgelost	RAP_Kiesraad_PR180188_Beveiligingsonderzoek OSV-PUBLIC
SSL version 3.0 is detected	-	Opgelost	Security-assessment-of-Dutch-election-software-OSV, par. 4.1.14 (p. 40)
Password policy not enforced: one letter passwords possible	-	Opgelost	Security-assessment-of-Dutch-election-software-OSV, par. 4.1.22 (p. 51)
OSV can be run on an unencrypted HTTP connection on port 8080	-	Opgelost	Security-assessment-of-Dutch-election-software-OSV, par. 4.1.23 (p. 52)
jQuery security updates are missing	-	Opgelost	Security-assessment-of-Dutch-election-software-OSV, par. 4.1.29 (p. 59)
OSV database software Derby is missing security updates	-	Opgelost	Security-assessment-of-Dutch-election-software-OSV, par. 4.1.31 (p. 60)
Checking the integrity of the CD-ROM file is optional	-	Opgelost	Security-assessment-of-Dutch-election-software-OSV, par. 4.1.35 (p. 64)
Password hashing and login	-	Opgelost	Onderzoek VUsec, par. 6, issue 2
OSV-webapplicatie toegankelijk zonder verbindings-versleuteling	-	Opgelost	Onderzoek Fox-IT 2017, bevinding 1
Werkwijze wachtwoorden onveilig	-	Opgelost	Onderzoek Fox-IT 2017, bevinding 4
Verificatie integriteit EML-bestanden onvoldoende	-	Opgelost	Onderzoek Fox-IT 2017, bevinding 5



Bevinding	Huidig Risico	Status na herctest Q4 2019	Verwijzing
Integriteitscontrole OSV installatie-cd-rom kan omzeild worden	-	Opgelost	Onderzoek Fox-IT 2017, bevinding 7
XML External Entity Injection (XXE)	-	Opgelost	Onderzoek Fox-IT 2017, bevinding 8
Vier-ogen-principe wordt niet afgedwongen	-	Opgelost	Onderzoek Fox-IT 2017, bevinding 9
Niet geverifieerde externe software vereist	-	Opgelost	Onderzoek Fox-IT 2017, bevinding 10
Browser back button works even if user is logged out (HTML code can be cached)	-	Opgelost	Security-assessment-of-Dutch-election-software-OSV, par. 4.1.21 (p. 49)
No restriction on JavaScript usage via Content Security Policy	-	Opgelost	Security-assessment-of-Dutch-election-software-OSV, par. 4.1.27 (p. 52)
Integer overflow	-	Opgelost	Onderzoek VUsec, par. 5, issue 1
XML schema validation and application checks bypass	-	Opgelost	Onderzoek VUsec, par. 5, issue 2
Election definition and XSS	-	Opgelost	Onderzoek VUsec, par. 5, issue 4
Publication of e-mail addresses	-	Opgelost	Security-assessment-of-Dutch-election-software-OSV, par. 4.5.2 (p. 75)
Strict Transport Security isn't enabled	-	Opgelost	Security-assessment-of-Dutch-election-software-OSV, par. 4.1.24 (p. 54)



Bevinding	Huidig Risico	Status na herctest Q4 2019	Verwijzing
Prevent the access of other .jsp sites (OSV P4 and P5)	-	Opgelost	MEMO_Kiesraad_PR180188_Hertest_2019Q2_1.0
Control the authorization of a user if he/she opens a page or performs an action	-	Opgelost	MEMO_Kiesraad_PR180188_Hertest_2019Q2_1.0
Prevent access without authentication to pages	-	Opgelost	MEMO_Kiesraad_PR180188_Hertest_2019Q2_1.0
Prevent that result is set by single result file import in P4_HSB and P4_CSB	-	Opgelost	MEMO_Kiesraad_PR180188_Hertest_2019Q2_1.0
OSV-2121 Control the authorization of a user if he/she performs an action	-	Opgelost	MEMO_Kiesraad_PR180188_Hertest_2019Q2_1.0

Aan: De Kiesraad

Auteurs: Fox-IT

Betreft: Beantwoording vraag digitale overdracht – Memorandum

Ref. nr. PR-180152

Datum: 18 december 2018

Classificatie: PUBLIC

Status: Definitief

Versie: 1.1

Inleiding

De Kiesraad heeft Fox-IT gevraagd om onderstaande onderzoeksvraag te beantwoorden. Deze onderzoeksvraag zal doormiddel van een memorandum beantwoord worden. Bij de beantwoording van deze vraag heeft Fox-IT gekozen om niet alleen de technische aspecten van de vraag, maar ook de context en de omgeving waarbinnen de technische oplossing gebruikt wordt mee te wegen in het antwoord. De aan Fox-IT gestelde onderzoeksvraag luidt als volgt:

“Welke vorm van digitale overdracht, uitgaande van de huidige functionaliteit van OSV, is geschikt binnen de context van de huidige procedure waarlangs de uitslag formeel wordt vastgesteld en welke gegevensdrager past daarbij?”

for a more secure society

Contextualisatie Ondersteunende Software Verkiezingen (OSV)

Op dit moment wordt digitale overdracht met als doel het vaststellen van stemtotalen niet toegestaan en worden stemtotalen exclusief op basis van papier overgedragen. Ondersteunende Software Verkiezingen (OSV) wordt gebruikt ter ondersteuning van de verkiezingen, bij het berekenen van de stemtotalen (OSV Programma 4) alsook de zetelverdeling (OSV Programma 5). In OSV kunnen gegevens op een drietal manieren ingevoerd worden:

1. Handmatig, waarbij stemtotalen op basis van het N10 proces-verbaal (afkomstig van individuele stembureaus), als ook die op de N11 (de opgave van de burgemeester) en O3 (proces-verbaal hoofdstembureau) twee keer vanaf papier worden ingevoerd;
2. Automatisch, waarbij stemtotalen behorend bij de N11 en O3 in de vorm van een zogenaamd EML-bestand worden ingelezen;
3. Een combinatie waarbij eerst een bestand wordt ingelezen en daaropvolgend de stemtotalen handmatig worden ingevoerd.

Bij automatisch invoeren wordt het EML-bestand samen met de papieren processen-verbaal tussen de opeenvolgende stappen in het aggregatieproces overgedragen, zodat de uitvoer van de ene stap in het proces de invoer van de volgende stap in het proces wordt. Tijdens de overdracht van het EML-bestand is het cruciaal dat de integriteit van de stemtotalen gewaarborgd wordt. Het borgen van de integriteit dient tevens ter ondersteuning van de processen voor het detecteren van manipulaties van het papieren proces-verbaal. Bij het inlezen van een EML-bestand dwingt OSV een controle van de hash-waarde af. OSV voorziet in twee manieren van inlezen; alleen een EML-bestand inlezen of een EML-bestand inlezen aangevuld met handmatige invoer. Om manipulatie van stemtotalen in het EML-bestand op te kunnen merken, adviseert Fox-IT om de reeds bestaande controle van de hash-waarde van het EML-bestand te behouden alsook een aanvullende handmatige invoer uit te voeren.

Zonder automatische invoer vindt de invoer van stemtotalen op ieder niveau exclusief plaats door het handmatig overnemen van aantallen stemmen vanaf papier. Het gebrek aan een digitaal hulpmiddel (zoals bijvoorbeeld een OSV-oplossing) maakt het papieren proces potentieel kwetsbaar voor onbewuste invoerfouten en bewuste manipulaties. Bij de verwerking van stemtotalen is de confidentialiteit van de

stemtotalen van ondergeschikt belang, aangezien de stemtotalen publiek zijn in het kader van de transparantie van het democratische verkiezingsproces. Verder is het van belang dat in de huidige situatie het OSV beveiligingsconcept alsook de standaard componenten technisch *end-of-life* zijn, mede door verouderde standaard software componenten.

Voor de huidige wijze van inzet van OSV dient rekening gehouden te worden met het document 'Voorwaarden voor gebruik OSV'¹ zoals gepubliceerd door de Kiesraad. Dit document beschrijft onder andere dat partijen die verantwoordelijk zijn voor het stemtelproces en die gebruik maken van OSV in het verkiezingsproces worden geacht de software te gebruiken op computers die op geen enkel moment op enigerlei wijze verbonden worden met andersoortige netwerken, zoals het Internet.

Een strikte naleving van bovengenoemde vereisten door de in het verkiezingsproces verantwoordelijke partijen, resulteert in een significante beperking van het risico dat de aanwezigheid van kwetsbaarheden kan worden uitgebuit om de integriteit van de verkiezingsuitslag te compromitteren. De systemen die worden gebruikt voor het stemtelproces en die gebruik maken van OSV in het verkiezingsproces bevinden zich echter buiten de directe invloedssfeer van de Kiesraad. Strikte naleving van de vereisten kan alleen worden bereikt door de decentrale verantwoordelijke partijen, om daarmee het risico van het niet naleven van de vereisten uit te sluiten.

Mede gezien de door de Kieswet gestelde termijnen voor het tellen, aggregeren en vaststellen van deze uitkomsten wenst de Kiesraad te verkennen of digitale gegevensoverdracht mogelijk is en op welke wijze dit ingevuld zou kunnen worden. Daarnaast biedt digitale overdracht van de stemtotalen een verhoogde beveiliging van het gehele proces, waarbij het digitale proces en het papieren proces gebruikt kunnen worden om elkaar te controleren.

¹ <https://www.kiesraad.nl/binaries/kiesraad/documenten/formulieren/2016/osv/osv-bestanden/voorwaarden-voor-gebruik-osv/Voorwaarden+voor+gebruik+OSV+9-2-2018.pdf>

Advies met betrekking tot overdracht digitale OSV-bestanden

Het waarborgen van de integriteit van het stemtelproces alsook de berekening van de zetelverdeling kan niet geborgd worden door enkel technische maatregelen. Dit vereist een geïntegreerde combinatie van maatregelen die op technisch en procedureel vlak een sluitend geheel vormen en daarmee de weerbaarheid van het proces vergroten. Verdere toelichting op (het belang van) deze samenhang aan maatregelen kan gevonden worden in het rapport van Fox-IT uit 2017 inzake OSV².

Aangezien de Kiesraad reeds op de hoogte is van de beperkingen van de voorgaande procedurele (met gebruikmaking van USB-sticks voor digitale gegevensoverdracht), alsook van de huidige softwarematige oplossing, heeft Fox-IT onderzoek gedaan naar welke vorm van gegevensoverdracht geschikt en haalbaar is en tevens beperkte additionele risico's met zich meebrengt. Derhalve wordt de onderzoeksvraag geïnterpreteerd als gericht op de identificatie van de meest geschikte vorm van digitale gegevensoverdracht, gegeven de huidige functionaliteit van OSV en de daarbij behorende procedurele context. Om de weerbaarheid van de vaststelling van de verkiezingsuitslag tegen bewuste manipulaties in bredere zin te bereiken, moet, zoals beschreven, een balans gevonden worden tussen techniek, procedures en het menselijk aspect. In het navolgende advies wordt met alle drie deze aspecten rekening gehouden.

Bij de beantwoording van de onderzoeksvraag heeft Fox-IT de mogelijkheid van dataoverdracht door middel van beveiligde websites of soortgelijke mogelijkheden zoals e-mail, die een netwerkverbinding vereisen, buiten beschouwing gelaten. Dit besluit is genomen in het kader van de potentiële additionele risico's die hiermee geïntroduceerd worden, de complexiteit om dergelijke oplossingen in te passen in de vaststelling van de verkiezingsuitslag gegeven het vereiste van een gescheiden netwerkgeving en het beperkte tijdsbestek waarbinnen de Kiesraad de aanbevelingen wenst te effectueren bij de inzet van de huidige OSV-oplossing.

Oplossingen die betrekking hebben op media die meerdere malen beschreven kunnen worden zoals (beveiligde) USB-sticks zijn na een korte evaluatie minder geschikt bevonden. De aanwezigheid van software en/of firmware introduceert een additioneel risico waarmee de ontvanger van dergelijke media

² <https://www.kiesraad.nl/binaries/kiesraad/documenten/rapporten/2017/3/fox-it/fox-it/Rapport+Fox-IT+3-3-2017.pdf>

aangevallen kan worden. Daarnaast is de manipulatie van dergelijke software en/of firmware moeilijk detecteerbaar en zou dergelijke manipulatie forensisch mogelijk niet meer aan te tonen zijn. Het risico van het gebruik van een dergelijke technische oplossing kan beperkt worden door gebruik te maken van een combinatie aan procedurele maatregelen (vier ogen principe, sealbags, et cetera) zoals verder benoemd in dit advies. De resterende risico's zouden hierdoor beperkt kunnen worden, maar naar oordeel van Fox-IT niet tot een acceptabel niveau, mede doordat de firmware-aanvalsvector in dezen een aandachtspunt blijft en manipulatie forensisch moeilijk detecteerbaar is of zelfs niet aantoonbaar zou zijn.

Transparantie

Eén van de maatregelen die onderdeel behoort te zijn van het verkiezingsproces betreft de transparantie van de vaststelling van de uitslag door het uniform online publiek beschikbaar stellen van een kopie van zowel de papieren processen-verbaal als de digitale gegevens van de stembureaus. De mogelijkheid voor burgers om de uitslag te toetsen door middel van deze processen-verbaal vergroot de controlerende capaciteit die burgers alsook andere instanties kunnen uitvoeren en daarmee de weerbaarheid van het verkiezingsproces. Let wel, de door de Kieswet gehanteerde termijnen kunnen hier nog wel een uitdaging in vormen mede door de zeer beperkt beschikbare tijd waarin deze controle dient plaats te vinden, voordat de uitslag formeel worden vastgesteld.

Integriteit waarborgen

Wanneer een medium gekozen wordt voor het uitwisselen van EML-bestanden is het belangrijk om daarbij de volgende randvoorwaarden in acht te nemen:

- De integriteit van het EML-bestand dient gewaarborgd te worden;
- Het gebruikte medium voor uitwisseling dient zo min mogelijk extra risico's te introduceren voor zowel de verzender als de ontvanger;
- De integriteit van de personen welke betrokken zijn bij het transport wordt door de Kiesraad als een gegeven beschouwd. Desalniettemin dient rekening gehouden te worden met de mogelijkheid dat een transport onderschept of gemanipuleerd kan worden.

Om de integriteit van de EML-bestanden en de daarin aanwezige stemtotalen met de hoogste mate van zekerheid te kunnen waarborgen, heeft vanuit een informatiebeveiligingsperspectief het digitaal ondertekenen van bestanden met behulp van een cryptografische oplossing sterk de voorkeur. In het door de Kiesraad geschetste kader is het echter niet haalbaar om een dergelijke oplossing op de korte termijn (voor de komende verkiezingen) te implementeren. Deze onhaalbaarheid vloeit deels voort uit de complexiteit van een dergelijke oplossing waarbij niet alleen de technische vereisten correct geïmplementeerd dienen te worden, maar ook de organisatorische vereisten met betrekking tot het distribueren van het sleutelmateriaal en het verifiëren dat het sleutelmateriaal door de juiste persoon in ontvangst is genomen. Fox-IT adviseert verder onderzoek te doen naar deze mogelijkheid om te bepalen of, en zo ja op welke termijn, een dergelijke oplossing niet alleen technisch maar ook organisatorisch haalbaar is om de integriteit van de digitale overdracht van stemtotalen te borgen.

Gegeven de hiervoor beschreven omstandigheid wordt uitgegaan van de doelstelling om de integriteit van stemtotalen tijdens de gegevensoverdracht op de korte termijn, zoveel als redelijkerwijs mogelijk is, te waarborgen. In dat kader wordt aangeraden om gebruik te maken van een medium waarbij de kosten van een aanval om bestanden aan te passen zoveel mogelijk verhoogd worden en het zo mogelijk fysiek inzichtelijk wordt dat manipulatie heeft plaatsgevonden. Hiervoor wordt aangeraden om gebruik te maken van een Compact Disc Read-Only Memory (CD-ROM) welke eenmalig beschreven kan worden en softwarematig gesloten wordt na het beschrijven, zodat verdere beschrijving of aanpassing van gegevens redelijkerwijs niet mogelijk is.

Hierbij dient opgemerkt te worden dat niet uitgesloten kan worden dat de gegevens op een CD-ROM aangepast kunnen worden door een kwaadwillende (hoewel dit zeer onwaarschijnlijk is). Dit is gedeeltelijk te wijten aan het feit dat de controle voor de beschrijving van de CD-ROM uitgevoerd wordt in software en dit het in principe mogelijk maakt om de gegevens op de CD-ROM te beïnvloeden. Een dergelijke manipulatie zou niet direct zichtbaar zijn tijdens het normale gebruik van het medium, maar kan achteraf door middel van forensisch onderzoek vastgesteld worden.

Indien het risico dat bestanden toegevoegd kunnen worden door een aanvaller (ondanks dat dit achteraf door middel van forensisch onderzoek gedetecteerd kan worden) als onwenselijk beschouwd wordt, kan dit

verder gemitigeerd worden door het volledig beschrijven van alle beschikbare ruimte. Deze handeling vereist extra inspanning van de gebruiker in het beschikbaar hebben van een bestand dat minimaal gelijk is aan de resterende ruimte op de CD-ROM. Deze extra inspanning vereist additionele procedurele instructies en in potentie het introduceren van nieuwe software waardoor de moeilijkheidsgraad aanzienlijk toeneemt. De toename van de moeilijkheidsgraad vloeit voort uit de diversiteit aan digitale omgevingen bij de verschillende instanties waarbinnen deze handeling correct uitgevoerd dient te worden. Het (beperkt) aanpassen van bestanden kan niet volledig uitgesloten worden, maar vereist wel een significant hogere investering en kan bovendien gedetecteerd worden.

De reeds bestaande maatregel waarbij de hash-waarde van het digitaal medium op het papieren proces verbaal geprint wordt en bij verwerking door OSV gecontroleerd wordt, draagt bij aan de detectie van eventuele manipulatie van de bestanden (gewijzigde hash-waarde). Ook de verhoogde transparantie door het publiek beschikbaar maken van de processen-verbaal van de stembureaus draagt bij aan het detecteren van eventuele gemanipuleerde stemtotalen.

Fysiek vervoer

Voor het fysieke vervoer van het medium waarmee de gegevens overgedragen worden, is het van belang dat manipulatie alsook vervanging van het medium opgemerkt wordt en dat de integriteit, zoveel als redelijkerwijs mogelijk is, geborgd wordt. Hiervoor stelt Fox-IT de volgende aanvullende maatregelen voor, die op de juiste manier toegepast dienen te worden. Hierbij is voor het hoogst mogelijke beveiligingsniveau van belang dat alle maatregelen toegepast worden. Echter kan dit mogelijk niet in alle gevallen als haalbaar worden geacht:

- Maak gebruik van een fysieke handtekening op het medium en de veiligheidsenveloppe;
- Maak gebruik van een veiligheidsenveloppe (ook wel: *sealbag*) voor transport;
- Vervoer het medium en het papieren proces-verbaal in verschillende transporten;
- Maak gebruik van het vierogenprincipe gedurende het hele proces vanaf de uitvoer tot en met de invoer van de gegevens.

Een vereiste om bovenstaande maatregelen te combineren, om afdoende weerbaar te zijn tegen manipulatie van de gegevens, is de eis dat de juiste controles worden afgedwongen. Dit omvat wat OSV betreft het controleren van de hash-waarde. Wat de procedures betreft, omvat dit onder andere het controleren van de nummers van de veiligheidsenveloppen wanneer deze in ontvangst worden genomen.

Uitleg bij risico's van fysiek vervoer digitale OSV-bestanden

Tijdens het fysiek transport bestaat het risico van manipulatie van gegevens. Dit risico kan met de hierboven beschreven maatregelen verkleind worden. Hieronder volgt een uitleg van deze maatregelen in samenhang tot de risico's die met deze maatregelen verkleind worden.

Het in één transport vervoeren van de éénmalig beschrijfbare CD-ROM alsook het papieren proces-verbaal in aparte veiligheidsenveloppen resulteert in een gereduceerd risico ten aanzien van de mogelijkheid voor aanvallers om ongedetecteerd de bestanden op de CD-ROM tijdens het transport te manipuleren. Dit kan dan namelijk tijdens het transport alleen door (al dan niet met medeweten van de transporteur) de data op de CD-ROM te wijzigen of de CD-ROM in zijn geheel te vervangen, deze in een nieuwe –met het juiste nummer geprepareerde- veiligheidsenveloppe te stoppen en het papieren proces-verbaal te vervangen door een exemplaar met de frauduleuze hash-waarde. Het risico tijdens transport kan ook beperkt worden door zowel de CD-ROM als het papieren proces-verbaal in aparte transporten te vervoeren. Hiermee worden voor een aanvaller de kosten van een succesvolle aanval sterk verhoogd.

Tenslotte kan het risico tijdens transport beperkt worden door elk individueel transport uit te voeren door twee personen in plaats van een. Hiermee verkleint de kans dat een aanval succesvol kan worden uitgevoerd. Het bovenstaande laat onverlet de eerder benoemde adviezen ten aanzien van het detecteren van manipulatie van stemtotalen in EML-bestanden, door middel van de reeds bestaande hash-controle te behouden alsook een aanvullende handmatige invoer uit te voeren.

Conclusie met betrekking tot de overdracht van digitale OSV-bestanden

Het gebrek aan een digitaal hulpmiddel (zoals bijvoorbeeld een OSV-oplossing) maakt het papieren proces potentieel kwetsbaar voor onbewuste invoerfouten en bewuste manipulaties. Het gebruik maken van digitale hulpmiddelen aanvullend aan het papieren proces maakt het geheel weerbaarder tegen bewuste of onbewuste manipulatie. Gebruik voor het vervoer van de door het digitale hulpmiddel gegenereerde digitale bestanden een CD-ROM welke eenmalig beschreven kan worden waarbij de kosten van een aanval om bestanden aan te passen zoveel mogelijk verhoogd worden en het zo fysiek inzichtelijk wordt dat manipulatie heeft plaatsgevonden.

De risico's gerelateerd aan de hieronder beschreven subset van maatregelen voor fysiek vervoer kunnen worden geaccepteerd of gemitigeerd. De keuze voor het mitigeren of accepteren van risico's dient op een weloverwogen en gedocumenteerde wijze plaats te vinden. Hierbij dient namelijk een afweging gemaakt te worden tussen de impact die een succesvolle aanval zou kunnen veroorzaken en de kans dat een dergelijke aanval succesvol kan worden uitgevoerd. De juiste balans voor deze beslissing dient in overleg met betrokken organisaties plaats te vinden, alsook instanties die de dreiging van statelijke actoren kunnen duiden.

Op het vlak van fysiek vervoer zijn, zoals benoemd, meerdere maatregelen mogelijk die onafhankelijk van elkaar ingezet kunnen worden. Naar de mening van Fox-IT kan een minimale subset van maatregelen op dit vlak beschreven worden, bestaand uit die maatregelen die het risico van manipulatie tijdens het transport het meest reduceren in relatie tot de impact die een aanval in verschillende stadia van het transport kan hebben. De hieronder beschreven minimale subset aan maatregelen verhogen de kans dat een eventuele manipulatie voorkomen of gedetecteerd wordt, met name omdat zij de complexiteit en de kosten van een dergelijke aanval aanzienlijk verhogen.

Voor het vervoer van de digitale gegevens van de gemeente naar het hoofdstembureau dient het vervoer van het digitale medium gescheiden van het papieren medium plaats te vinden. Daarbij zijn overigens de eerder in deze memo genoemde³ maatregelen, aangaande transparantie en het waarborgen van de

³ De maatregelen worden in dit memorandum beschreven onder het kopje 'Advies met betrekking tot overdracht digitale OSV-bestanden'

integriteit onverlet van toepassing. Voor het vervoer van de digitale gegevens van het hoofdstembureau naar het centraal stembureau dienen, naast het gescheiden vervoeren van het digitale medium en het papier, beide vervoersstromen uitgevoerd te worden middels een vier ogen principe (het door twee personen vervoeren van de gegevens).

De procedure voor het vervoer van de schriftelijke en eventueel digitale gegevens dient inzichtelijk en helder te zijn voor eenieder die betrokken is bij dit proces. Dit vereist het uniform informeren van betrokkenen met het oog op het correct handelen bij het vervoeren van de gegevens alsook het identificeren en signaleren van potentiële afwijkingen. Hiermee wordt het risico verkleind dat een potentieel (beveiligings)incident onopgemerkt blijft.



FOX IT
part of nccgroup

Aan: De Kiesraad

T.a.v. 5.1.2.e en 5.1.2.e

Auteurs: 5.1.2.e en 5.1.2.e

Betreft: Beantwoording vraag implementeren Java 1.8 – Memorandum

Ref. nr. PR-180152

Datum: 9 november 2018

Classificatie: **COMMERCIAL.RESTRICTED.KIESRAAD**

Status: Definitief

Versie: 1.1

Inleiding

De Kiesraad heeft Fox-IT gevraagd om onderstaande onderzoeksvraag te beantwoorden. Deze onderzoeksvraag zal doormiddel van een memorandum beantwoord worden. Bij de beantwoording van deze vraag heeft Fox-IT gekozen om niet alleen de technische aspecten van de vraag, maar ook de context en de omgeving waarbinnen de technische oplossing gebruikt wordt mee te wegen in het antwoord. De aan Fox-IT gestelde onderzoeksvraag luidt als volgt:

“Beveelt opdrachtnemer binnen de huidige context van OSV, aan, om Java 1.8 te implementeren rekening houdend met mogelijke compatibiliteitsproblemen in combinatie met andere softwarecomponenten (zoals Jboss versie 4.2.3 die niet ontworpen is voor Java 1.8), inclusief een toelichting waarom opdrachtnemer het wel of niet aanbeveelt?”

for a more secure society

FOX-IT BV
Olof Palmestraat 6, Delft
POSTBUS 638, 2600 AP Delft

T +31 (0)15 284 79 99
F +31 (0)15 284 79 90
ABN AMRO 554697041
KVK Haaglanden 27301624

FOX-IT.COM

Huidige situatie

Het Ondersteunende Software Verkiezingen (OSV)-softwarepakket maakt op dit moment gebruik van zowel een verouderde versie van de JBoss applicatieserver als van een verouderde versie van de Java Runtime Environment (JRE), respectievelijk de versies 4.2.3 en 1.6. Hoewel beide softwarepakketten al enkele jaren oud zijn, heeft Fox-IT uit de interviews met de Kiesraad begrepen dat het upgraden van Java en JBoss naar een nieuwere versie problematisch is. De leverancier van OSV heeft aangegeven dat de toegepaste versie van JBoss niet gegarandeerd geschikt is voor gebruik (*compatible*) met nieuwere Java versies. Daarnaast heeft de upgrade naar een nieuwe versie van JBoss een aanzienlijke impact op de technische code van OSV doordat de toegepaste EJB (Enterprise JavaBeans)-standaard is gewijzigd in nieuwere versies van JBoss. Hierdoor voorziet de leverancier risico's ten aanzien de correcte werking van OSV en adviseert om af te zien van het upgraden van bepaalde software-onderdelen. Verder heeft de Kiesraad te kennen gegeven dat OSV als zodanig als 'end-of-life' wordt beschouwd, hetgeen mede voorkomt uit voortschrijdend inzicht met betrekking tot de beveiliging van de software.

De Kiesraad heeft besloten om in het kader van het verbeteren van de beveiliging van het OSV-softwarepakket een experiment uit te voeren, ten behoeve van het upgraden van het Java component. Het doel van dit experiment was het verkrijgen van een indicatie over de werking van de OSV-programmatuur met een nieuwe versie van Java, alsook het onafhankelijk van de leverancier vaststellen van de haalbaarheid hiervan. Tijdens dit experiment heeft de Kiesraad vastgesteld dat de OSV software met een recentere versie van Java in ieder geval basaal werkt wanneer de Java Runtime Environment wordt geüpgradet naar versie 1.8. Echter is de functionaliteit van OSV nog niet in de volle omvang getest in de nieuwe samenstelling.

Tot slot dient voor de huidige wijze van inzet van OSV rekening gehouden te worden met het document 'Voorwaarden voor gebruik OSV'¹ zoals gepubliceerd door de Kiesraad. Dit document beschrijft onder andere dat partijen die gebruik maken van OSV voor de verkiezingsuitslag worden geacht de software te gebruiken op computers die op geen enkel moment op enigerlei wijze verbonden worden met andersoortige netwerken, zoals het Internet. De beantwoording van de onderzoeksvraag houdt derhalve rekening met de

¹ <https://www.kiesraad.nl/binaries/kiesraad/documenten/formulieren/2016/osv/osv-bestanden/voorwaarden-voor-gebruik-osv/Voorwaarden+voor+gebruik+OSV+9-2-2018.pdf>

manier waarop OSV ontsloten wordt aan de gebruikers, namelijk enkel via een volledig geïsoleerd netwerk in een fysieke ruimte die alleen toegankelijk is voor bevoegden. Een strikte naleving van deze vereisten door de in het verkiezingsproces verantwoordelijke partijen, resulteert in een significante beperking van het risico dat de aanwezigheid van kwetsbaarheden kunnen worden uitgebuit om de integriteit van de verkiezingsuitslag te compromitteren. Deze systemen bevinden zich echter buiten de directe invloedssfeer van de Kiesraad, waardoor de strikte naleving van de vereisten alleen kan worden bereikt door de decentrale verantwoordelijke partijen, om daarmee het risico van het niet naleven van de vereisten uit te sluiten.

Advies

Zoals beschreven in Fox-IT's eerdere advies uit 2017 kan de integriteit van het stemtelproces alsook de berekening van de zetelverdeling niet enkel door technische maatregelen geborgd worden. Deze borging vereist een geïntegreerde combinatie van maatregelen die op technisch en procedureel vlak een sluitend geheel vormen en daarmee de weerbaarheid van het proces vergroten.

Onderzoek alternatieve ondersteunende software

Vanwege het feit dat de OSV-software beschouwd wordt als 'end of life', verdient het de aanbeveling om onderzoek te doen naar de eisen, randvoorwaarden en mogelijkheden tot het ontwikkelen van een oplossing die ondersteunend kan worden gebruikt voor het aggregeren van de stemtotalen alsook het bepalen van de zetelverdeling, rekening houdend met de (digitale) dreigingen waar een modern verkiezingsproces aan onderhevig is (en in de toekomst zal zijn). Deze noodzaak wordt tevens onderkend door de Kiesraad en wordt als zodanig benoemd in het document 'Evaluatieadvies gemeenteraadsverkiezingen en raadgevend referendum 21 maart 2018'².

Eventuele technische verbeteringen en technische mitigerende maatregelen binnen de huidige oplossing kunnen niet leiden tot een oplossing die als sluitend beschouwd kan worden. Het OSV-softwarepakket is ontworpen op basis van verouderde security-concepten. Verbeteringen in het huidige softwarepakket kunnen resulteren in een veiliger softwarepakket, maar deze verbeteringen kunnen op zichzelf niet resulteren in een significante verbetering van het gehele proces.

Java upgraden

Gezien publiek bekend kwetsbaarheden welke aanwezig zijn in de Java Runtime Environment versie 1.6, zoals momenteel in gebruik binnen het OSV-softwarepakket, raadt Fox-IT aan te upgraden naar versie 1.8. Deze versie beperkt de risico's die voortvloeien uit het gebruik van de Java Runtime Environment, bijvoorbeeld doordat verschillende zogenaamde 'deserialization' kwetsbaarheden verholpen zijn. Deze kwetsbaarheden zouden ertoe kunnen leiden dat niet-vertrouwde code wordt uitgevoerd waarmee de integriteit van OSV en de daarmee verwerkte gegevens gecompromitteerd zouden kunnen worden. Het

² <https://www.kiesraad.nl/adviezen-en-publicaties/adviezen/2018/5/17/evaluatieadvies-gemeenteraadsverkiezingen-en-raadgevend-referendum-21-maart-2018>

risico op uitbuiting van eventuele kwetsbaarheden is echter beperkt vanwege de door de Kiesraad beschreven richtlijnen, waardoor het kwetsbare aanvalsoppervlakte niet direct wordt blootgesteld aan externe aanvallers.

Desalniettemin zijn vanuit technisch perspectief aanvalspaden voorzienbaar die een aanvaller de mogelijkheid kunnen bieden om de software uit te buiten, zoals het gebruik van kwaadaardige EML-bestanden. Fox-IT adviseert om verder onderzoek te verrichten naar het beveiligingsniveau van de broncode van de OSV-software alsook de verwerking van gegevens door OSV. Dit kan verdere indicaties opleveren over de aanwezigheid van eventuele kwetsbaarheden, bijvoorbeeld bij het importeren van EML-bestanden. Eventuele technische kwetsbaarheden zouden zelfs op kunnen treden wanneer de eerdergenoemde richtlijnen zoals 'airgapped' systemen strikt gevolgd zijn. Voorgenoemd advies dient ter verdere inperking van de restrisico's die vanuit technisch perspectief denkbaar zijn, maar vanuit een praktisch perspectief lastig uit te buiten zijn.

Vanzelfsprekend raadt Fox-IT aan uitvoerig te testen of de OSV-software nog naar behoren functioneert na de upgrade van Java. Dit verlaagt de kans dat de software tijdens de verkiezing niet correct functioneert, waardoor partijen mogelijk moeten uitwijken naar minder veilige alternatieven om het proces binnen de gestelde termijnen af te ronden. Daarbij moet met name gecontroleerd worden of de uitkomsten van het aggregatieproces kunnen verschillen bij gebruik van de verschillende versies van de Java Runtime Environment.

Fox-IT merkt op dat met het upgraden van de Java Runtime Environment enkel bekende kwetsbaarheden binnen dat specifieke softwarepakket worden opgelost. Additionele kwetsbaarheden die mogelijk aanwezig zijn in het sterk verouderde JBoss-platform of de gebruikte software 'libraries' blijven in dat geval onverminderd aanwezig met alle risico's, zoals het in potentie overnemen van het werkstation waarop de OSV-oplossing is geïnstalleerd. Ook hiervoor geldt dat het onwaarschijnlijk is dat deze kwetsbaarheden daadwerkelijk uitgebuit kunnen worden, vanwege het feit dat de systemen vanwege de door de Kiesraad beschreven richtlijnen zich in een geïsoleerd netwerk behoren te bevinden en daarbinnen ook voorzien moeten zijn van een firewall. Deze firewall verzekert dat enkel de benodigde 'web-interface' bereikbaar is voor gebruikers en dat overige diensten (*services*) die niet essentieel zijn voor de juiste werking van OSV

ook niet binnen het geïsoleerde netwerk benaderd kunnen worden. Overige diensten kunnen enkel bereikt worden vanaf de server waar OSV op geïnstalleerd is (*localhost*).

Restrisico's

De samenhang aan procedurele maatregelen en technische maatregelen beperken in sterke mate de risico's aangaande de uitbuiting van technisch denkbare kwetsbaarheden, zoals kwaadaardige EML-bestanden en kwetsbaarheden voortvloeiend van het gebruik van verouderde software. Hiermee kan het restrisico als acceptabel beschouwd worden. Wel verdient het nog steeds sterk de aanbeveling om zo spoedig mogelijk uitgebreid onderzoek te verrichten naar het vervangen van de huidige ondersteunende software en de daaraan ten grondslag liggende beveiligingsconcepten. Daarbij dient rekening gehouden te worden met het feit dat ook vernieuwde en beter beveiligde software zelfstandig niet weerbaar is tegen hedendaagse dreigingen. De nieuwe oplossing dient zowel technische alsook procedurele aspecten te combineren om tot een sluitend geheel te komen.

Tot slot

Ook indien alle eerder genoemde adviezen geïmplementeerd worden, is het belangrijk om te constateren dat het OSV-softwarepakket ontworpen is op basis van verouderde beveiligingsconcepten. Verbeteringen in het huidige softwarepakket kunnen resulteren in een veiliger softwarepakket, maar deze verbeteringen kunnen op zichzelf niet resulteren in een significante verbetering van het gehele proces. Wel bieden de context en de daarbinnen toepasselijke procedurele maatregelen een additionele beveiligingslaag, waarmee het risico van de eerder beschreven aanvallen aanzienlijk worden verlaagd op basis waarvan de restrisico's als acceptabel kunnen worden beschouwd.



FOX IT
part of nccgroup

Aan: De Kiesraad

T.a.v. 5.1.2.e en 5.1.2.e

Auteurs: 5.1.2.e en 5.1.2.e

Betreft: Hertest OSV versie 2.22.1 – Memorandum

Ref. nr. PR-180188

Datum: 15 november 2018

Classificatie: COMMERCIAL.RESTRICTED.KIESRAAD

Status: Concept

Versie: 0.4

Inleiding

De Kiesraad heeft Fox-IT gevraagd om een hertest uit te voeren van de hieronder genoemde bevindingen, een referentie naar de bron van de bevinding is opgenomen in bijlage A. De hertest heeft zich beperkt tot het testen van de genoemde bevindingen en het bepalen of deze als opgelost beschouwd kunnen worden. Tijdens de hertest is geen verder onderzoek verricht naar nieuwe kwetsbaarheden.

Daarnaast wordt opgemerkt dat onderstaande technische bevindingen niet een volledig beeld geven van de beveiliging van het gehele verkiezingsproces. Op basis van enkel deze technische bevindingen kunnen dus geen conclusies getrokken worden over de weerbaarheid van het gehele verkiezingsproces.

#	Bevinding	Referentie
1	Unnecessary ports are opened by Java	Bron 1, par. 4.1.3 (p. 26)
2	Stand-alone OSV installation is risky	Bron 1, par. 4.1.7 (p. 35)
3	SSL version 3.0 is detected	Bron 1, par. 4.1.14 (p. 40)
4	Password policy not enforced: one letter passwords possible	Bron 1, par. 4.1.22 (p. 51)
5	OSV can be run on an unencrypted HTTP connection on port 8080	Bron 1, par. 4.1.23 (p. 52)
6	jQuery security updates are missing	Bron 1, par. 4.1.29 (p. 59)
7	OSV database software Derby is missing security updates	Bron 1, par. 4.1.31 (p. 60)
8	Checking the integrity of the CD-ROM file is optional	Bron 1, par. 4.1.35 (p. 64)
9	Password hashing and login	Bron 2, par. 6, issue 2
10	OSV-webapplicatie toegankelijk zonder verbinding-versleuteling	Bron 3, bevinding 1
11	Niet ondersteunde software in gebruik	Bron 3, bevinding 2
12	Werkwijze wachtwoorden onveilig	Bron 3, bevinding 4
13	Verificatie integriteit EML-bestanden onvoldoende	Bron 3, bevinding 5
14	Transport door middel van USB-sticks	Bron 3, bevinding 6
15	Integriteitscontrole OSV installatie-cd-rom kan omzeild worden	Bron 3, bevinding 7
16	XML External Entity Injection (XXE)	Bron 3, bevinding 8
17	Vier-ogen-principe wordt niet afgedwongen	Bron 3, bevinding 9
18	Ongeverifieerde externe software vereist	Bron 3, bevinding 10
19	Overige tekortkomingen OSV	Bron 3, bevinding 11, sub 4

for a more secure society

FOX-IT BV

Olof Palmestraat 6, Delft

POSTBUS 638, 2600 AP Delft

T +31 (0)15 284 79 99

F +31 (0)15 284 79 90

ABN AMRO 554697041

KVK Haaglanden 27301624

FOX-IT.COM

Voor het uitvoeren van de hertest zijn de volgende bestanden door de Kiesraad aangeleverd:

#	Bestandsnaam	SHA256
1	osv_programma4en5_installer_v2.22.1.zip	E613B3BE5AF3299D0C24B8A8134B55B6 D5330BCFF86683224E8CA52FBA117355
2	OSV GR2018 voorbeeld bestanden.zip	889CCDB405EABBBF7B42EE26E223100A 5A0AD55F9F33F0F2677AD21FE196892E
3	Voorwaarden+voor+gebruik+OSV-2018-10-30.pdf	4FF6B8453E8508909D2061A28F28C80A BDFE29B0F3A8CF066D2796B9E4A8009F
4	Bijlagen+P4+en+5+voor+GRh2018+20181030.pdf	440001FEEAB9AF34FF4CF12C74BED504 088C68187FECEBC70BD562A87FF5CE4F
5	osv-broncode-programma-4-en-5-versie-2.22.1.zip	5A233068C6798E3AAE365345B9E4E6EB 36A8701B94A2D76A3A973E0AC7C047DD

Resultaten hertest

Onderstaande tabel geeft de status van de bevindingen weer ten tijde van de hertest, waarbij de kleur blauw aangeeft dat het risico van een bevinding is gemitigeerd, maar de oorzaak niet opgelost is. Verder geeft de kleur rood aan dat een bevinding niet is opgelost, geel dat een bevinding gedeeltelijk is opgelost en groen dat een bevinding in zijn geheel is opgelost voor zover dit door Fox-IT vastgesteld kon worden. Voor de bevindingen die niet zijn opgelost is een restrisico ingeschat, daarbij is in beperkte mate rekening gehouden met de meest relevantie niet-technische maatregelen die impact hebben op de betreffende bevinding.

#	Resultaat	Bevinding	Risico	Opmerking
1	Gemitigeerd	Unnecessary ports are opened by Java	LAAG	Java opent nog steeds onnodige poorten, maar deze worden afgeschermd door de Windows Firewall zoals beschreven in het document "Voorwaarden+voor+gebruik+OSV-2018-10-30".
2	Niet opgelost	Stand-alone OSV installation is risky	GEMIDDELD	De voorwaarden voor het gebruik van OSV geven aan dat gebruikersaccounts zo min mogelijk rechten dienen te bevatten. Tijdens de installatie worden de rechten van de OSV map niet juist ingesteld. Hierdoor is het afhankelijk van de gekozen locatie alsnog mogelijk om de bestanden te manipuleren vanaf een ander systeemaccount.
3	Niet opgelost	SSL version 3.0 is detected	LAAG	Het SSLv3 protocol is nog steeds beschikbaar, alleen het RC4 algoritme is uitgeschakeld.
4	Deels opgelost	Password policy not enforced: one letter passwords possible	LAAG	De wachtwoordeisen worden enkel afgedwongen door middel van JavaScript. De OSV applicatie accepteert alle wachtwoorden, indien deze zonder tussenkomst van JavaScript verzonden worden.
5	Opgelost	OSV can be run on an unencrypted HTTP connection on port 8080	-	-
6	Opgelost	jQuery security updates are missing	-	De software kan onverhoopt beveiligingsupdate missen, indien een nieuwe versie van jQuery beschikbaar gemaakt wordt ten tijde van de verkiezingen.
7	Opgelost	OSV database software Derby is missing security updates	-	De software kan onverhoopt beveiligingsupdate missen, indien een nieuwe versie van Derby beschikbaar gemaakt wordt ten tijde van de verkiezingen.
8	Opgelost	Checking the integrity of the CD-ROM file is optional	-	Procedureel wordt afgedwongen dat de integriteit van de CD-ROM gecontroleerd wordt.
9	Opgelost	Password hashing and login	-	-



10	Opgelost	OSV-webapplicatie toegankelijk zonder verbodings-versleuteling	-	-	
11	Deels opgelost	Niet ondersteunde software in gebruik	GEMIDDELD		Enkele componenten van de OSV applicatie zijn bijgewerkt.
12	Deels opgelost	Werkwijze wachtwoorden onveilig	LAAG		De wachtwoordeisen worden enkel afgedwongen door middel van JavaScript. De OSV applicatie accepteert alle wachtwoorden, indien deze zonder tussenkomst van JavaScript verzonden worden. Het MD5 hashing algoritme is vervangen met script.
13	Opgelost	Verificatie integriteit EML-bestanden onvoldoende	-	-	
14	Deels opgelost	Transport door middel van USB-sticks	LAAG		Volgens de procedure is het niet toegestaan om gebruik te maken van USB-sticks volgens de huidige richtlijnen.
15	Opgelost	Integriteitscontrole OSV installatie-cd-rom kan omzeild worden	-		Voor het linux commando wordt aanbevolen om '-b' als extra parameter mee te geven zodat het bestand in de juiste modus wordt ingelezen.
16	Deels opgelost	XML External Entity Injection (XXE)	GEMIDDELD		De broncode bevat wijzigingen om verschillende functionaliteiten gerelateerd aan XXE uit te zetten. Het is nog steeds mogelijk om de OSV applicatie te dwingen om onvoorziene HTTP en SMB verzoeken uit te voeren.
17	Opgelost	Vier-ogen-principe wordt niet afgedwongen	-	-	
18	Opgelost	Niet geverifieerde externe software vereist	-		Standaard functionaliteit van Windows wordt gebruikt.
19	Gemitigeerd	Overige tekortkomingen OSV	GEMIDDELD		Java opent nog steeds onnodige poorten, maar deze worden afgeschermd door de Windows Firewall zoals beschreven in het document "Voorwaarden+voor+gebruik+OSV-2018-10-30".

Bijlage A: Bronnen

Bron 1: Onderzoek RTL & Sijmen Ruwhof

- <https://sijmen.ruwhof.net/weblog/wp-content/uploads/2018/03/Security-assessment-of-Dutch-election-software-OSV.pdf>

Bron 2: Onderzoek VUsec

- <https://www.vusec.net/security-analysis-elections-software/>

Bron 3: Onderzoek Fox-IT

- <https://www.kiesraad.nl/adviezen-en-publicaties/rapporten/2017/3/fox-it/fox-it>



Aan: De Kiesraad
Auteurs: 5.1.2.e en 5.1.2.e
Betreft: Hertest OSV versie 2.24.1 – Memorandum
Ref. nr. PR-180188
Datum: 23 April 2019
Classificatie: PUBLIC
Status: Definitief
Versie: 1.0

Inleiding

De Kiesraad heeft Fox-IT gevraagd om een hertest uit te voeren van de hieronder genoemde bevindingen. Dit memorandum betreft een aanvulling op de bevindingen in paragraaf 4.3 en 4.4 van het rapport¹ van 12-03-2019. De hertest heeft zich beperkt tot het testen van de genoemde bevindingen en het bepalen of deze als opgelost beschouwd kunnen worden. Tijdens de hertest is geen verder onderzoek verricht naar nieuwe kwetsbaarheden.

Op basis van enkel deze technische bevindingen kunnen dus geen conclusies getrokken worden over de weerbaarheid van het gehele verkiezingsproces.

#	Kiesraad referentie	Kiesraad omschrijving
1	OSV-2009	Prevent showing stacktrace and server info to the user (OSV P4 and P5)
2	OSV-2013	Prevent the access of other .jsp sites (OSV P4 and P5)
3	OSV-2121	Control the authorization of a user if he/she opens a page or performs an action
4	OSV-2149	Prevent access without authentication to pages
5	OSV-2001	Improve protection against XSS (OSV P4 and P5)
6	OSV-2081	Verkiezingsleider is not allowed to enter polling station results (P4_PSB)
7	OSV-2082	Verkiezingsleider is not allowed to enter municipality results (P4_HSB)
8	OSV-2083	Verkiezingsleider is not allowed to enter kieskring results (P4_CSB)
9	OSV-2087	Prevent that result is set by single result file import in P4_HSB and P4_CSB
10	OSV-2122	Privilege escalation vulnerability (second HMAC bypass)
11	OSV-2159	OSV-2121 Control the authorization of a user if he/she performs an action

Voor het uitvoeren van de hertest zijn de volgende bestanden door de Kiesraad aangeleverd:

#	Bestandsnaam	SHA256
1	osv45_v2.24.1_source_for_review.zip	E2605FC018DA0A694BA2EB177CFB39C0 037B926FE469981A397A1625552C109F
2	osv_programma4en5_installer_v2.24.1.zip	DF311A8D5AF3F530AD3B4C1B56131BAF F3057B95848F8AA94B095378EF42F91B

¹ Rapport FOX-IT beveiligingsonderzoek OSV 14-3-2019.pdf

Resultaten hertest

Onderstaande tabel geeft de status van de bevindingen weer ten tijde van de hertest, waarbij de kleur rood aangeeft dat een bevinding niet is opgelost, geel dat een bevinding gedeeltelijk is opgelost en groen dat een bevinding in zijn geheel is opgelost voor zover dit door Fox-IT vastgesteld kon worden. Voor de bevindingen die niet zijn opgelost, is een restrisico ingeschat, waarbij in beperkte mate rekening gehouden is met de meest relevantie niet-technische maatregelen die impact hebben op de betreffende bevinding.

#	Resultaat	Kiesraad omschrijving	Opmerking
1	Deels opgelost	Prevent showing stacktrace and server info to the user (OSV P4 and P5)	Applicatie toont geen stack traces meer, Jboss wel.
2	Opgelost	Prevent the access of other .jsp sites (OSV P4 and P5)	-
3	Opgelost	Control the authorization of a user if he/she opens a page or performs an action	-
4	Opgelost	Prevent access without authentication to pages	-
5	Deels opgelost	Improve protection against XSS (OSV P4 and P5)	Eén specifieke XSS is opgelost, overige XSS bevindingen zijn nog aanwezig. Het is niet mogelijk om een uitputtende lijst aan te leveren, dit dient in de broncode opgelost te worden.
6	Niet opgelost	Verkiezingsleider is not allowed to enter polling station results (P4_PSB)	De verkiezingsleider kan deze rol opnieuw aan zichzelf toekennen of een gebruiker aanmaken met deze rechten. Beide acties zijn in de huidige logging herleidbaar.
7	Niet opgelost	Verkiezingsleider is not allowed to enter municipality results (P4_HSB)	De verkiezingsleider kan deze rol opnieuw aan zichzelf toekennen of een gebruiker aanmaken met deze rechten. Beide acties zijn in de huidige logging herleidbaar.
8	Niet opgelost	Verkiezingsleider is not allowed to enter kieskring results (P4_CSB)	De verkiezingsleider kan deze rol opnieuw aan zichzelf toekennen of een gebruiker aanmaken met deze rechten. Beide acties zijn in de huidige logging herleidbaar.
9	Opgelost	Prevent that result is set by single result file import in P4_HSB and P4_CSB	-
10	Deels opgelost	Privilege escalation vulnerability (second HMAC bypass)	Verhogen privileges is verholpen, het omzeilen van de HMAC controle is nog steeds van toepassing.
11	Opgelost	OSV-2121 Control the authorization of a user if he/she performs an action	-

Aan: De Kiesraad
Auteurs: 5.1.2.e en 5.1.2.e
Betreft: Hertest OSV versie 2.24.5 – Memorandum
Ref. nr. PR-180188
Datum: 11 november 2019
Classificatie: PUBLIC
Status: Definitief
Versie: 1.0
Bijlage: BIJLAGE_Kiesraad_PR-180188_Bevindingen voor Hertest 2019Q4

Inleiding

De Kiesraad heeft Fox-IT gevraagd om een hertest uit te voeren van de hieronder genoemde bevindingen. Dit memorandum betreft een aanvulling op de bevindingen genoemd in het memorandum van 23-04-2019 versie 1.0. De hertest was beperkt tot het testen van de genoemde bevindingen en het bepalen of deze als opgelost beschouwd kunnen worden. Tijdens de hertest is geen verder onderzoek verricht naar nieuwe kwetsbaarheden.

Op basis van enkel deze technische bevindingen kunnen dus geen conclusies getrokken worden over de weerbaarheid van het gehele verkiezingsproces.

#	Kiesraad referentie	Kiesraad omschrijving
1	OSV-2000	Modified EML files in archive directory on the server aren't detected
2	OSV-2001	Persistent Cross-Site Scripting (XSS)
3	OSV-2161 OSV-2009 OSV-1962	Gedetailleerde stack traces
4	OSV-1994	OSV database can be easily modified and votes can be changed
5	OSV-1994	OSV database isn't protected by a password
6	OSV-2081	Verkiezingsleider is not allowed to enter polling station results (P4_PSB)
7	OSV-2082	Verkiezingsleider is not allowed to enter municipality results (P4_HSB)
8	OSV-2083	Verkiezingsleider is not allowed to enter kieskring results (P4_CSB)
9	OSV-2122 OSV-2098	HMAC-controle is te omzeilen

Voor het uitvoeren van de hertest zijn de volgende bestanden door de Kiesraad aangeleverd:

# Bestandsnaam	SHA256
1 osv45_v2.24.5_source_for_review.zip	4BE47A0EC3B4AA323FD71C9950F2ACDC 2A8E3B31DB64BF8B8C2C2AE7E0A6A777
2 2019-09-19_P4_P5_v2.24.5.zip	648A2D9B62D401A154144A9D24CFFBBD EB6E8428279734C103AEBF3BC9C8EC6C

for a more secure society



Resultaten hertest

Onderstaande tabel geeft de status van de bevindingen weer ten tijde van de hertest, waarbij de kleur geel aangeeft dat een bevinding gedeeltelijk is opgelost en groen dat een bevinding in zijn geheel is opgelost voor zover dit door Fox-IT vastgesteld kon worden.

#	Resultaat	Kiesraad omschrijving ¹	Opmerking
1	Opgelost	Modified EML files in archive directory on the server aren't detected	Opgelost. Let wel, dit kan door een aanvaller met de juiste voorbereiding omzeild worden, dit is inherent aan de opzet van de software.
2	Opgelost	Persistent Cross-Site Scripting (XSS)	HTML-bestanden in de export map kunnen niet meer aangeroepen worden.
3	Opgelost	Gedetailleerde stack traces	Enkel generieke meldingen worden getoond.
4	Opgelost	OSV database can be easily modified and votes can be changed	Opgelost, database is voorzien van wachtwoord. Let wel, dit kan door een aanvaller met de juiste voorbereiding omzeild worden, dit is inherent aan de opzet van de software.
5	Opgelost	OSV database isn't protected by a password	Opgelost, database is voorzien van wachtwoord. Let wel, dit kan door een aanvaller met de juiste voorbereiding omzeild worden, dit is inherent aan de opzet van de software.
6	Opgelost	Verkiezingsleider is not allowed to enter polling station results (P4_PSB)	Strikt genomen opgelost, maar een verkiezingsleider kan altijd een extra account voor zichzelf aanmaken zodat de resultaten alsnog ingevuld kunnen worden. Kan gemitigeerd worden door audit logs te controleren.
7	Opgelost	Verkiezingsleider is not allowed to enter municipality results (P4_HSB)	Strikt genomen opgelost, maar een verkiezingsleider kan altijd een extra account voor zichzelf aanmaken. Kan gemitigeerd worden door audit logs te controleren.
8	Opgelost	Verkiezingsleider is not allowed to enter kieskring results (P4_CSB)	Strikt genomen opgelost, maar een verkiezingsleider kan altijd een extra account voor zichzelf aanmaken. Kan gemitigeerd worden door audit logs te controleren.
9	Deels opgelost	HMAC-controle is te omzeilen	Kan nog steeds omzeild worden. Let wel, de implementatie van additionele autorisatiecontroles maakt deze maatregel minder relevant en mitigeert een groot deel van de gevolgen. Technisch blijft het mogelijk om parameters in de URL te manipuleren, echter de gevolgen hiervan zijn beperkt.

¹ Originale omschrijving uit brondocumenten.



Aan: De Kiesraad
Auteurs: 5.1.2.e en 5.1.2.e
Betreft: Hertest OSV versie 2.24.5 – Memorandum
Ref. nr. PR-180188
Datum: 13 november 2019
Classificatie: PUBLIC
Status: Definitief
Versie: 1.0
Bijlage: BIJLAGE_Kiesraad_PR-180188_Bevindingen voor Hertest 2019Q4

Inleiding

De Kiesraad heeft Fox-IT gevraagd om een hertest uit te voeren van de hieronder genoemde bevindingen. Dit memorandum betreft een aanvulling op de bevindingen genoemd in het memorandum van 23-04-2019 versie 1.0. De hertest was beperkt tot het testen van de genoemde bevindingen en het bepalen of deze als opgelost beschouwd kunnen worden. Tijdens de hertest is geen verder onderzoek verricht naar nieuwe kwetsbaarheden.

Op basis van enkel deze technische bevindingen kunnen dus geen conclusies getrokken worden over de weerbaarheid van het gehele verkiezingsproces.

#	Kiesraad referentie	Kiesraad omschrijving
1	OSV-2000	Modified EML files in archive directory on the server aren't detected
2	OSV-2001	Persistent Cross-Site Scripting (XSS)
3	OSV-2161 OSV-2009 OSV-1962	Gedetailleerde stack traces
4	OSV-1994	OSV database can be easily modified and votes can be changed
5	OSV-1994	OSV database isn't protected by a password
6	OSV-2081	Verkiezingsleider is not allowed to enter polling station results (P4_PSB)
7	OSV-2082	Verkiezingsleider is not allowed to enter municipality results (P4_HSB)
8	OSV-2083	Verkiezingsleider is not allowed to enter kieskring results (P4_CSB)
9	OSV-2122 OSV-2098	HMAC-controle is te omzeilen

Voor het uitvoeren van de hertest zijn de volgende bestanden door de Kiesraad aangeleverd:

# Bestandsnaam	SHA256
1 osv45_v2.24.5_source_for_review.zip	4BE47A0EC3B4AA323FD71C9950F2ACDC 2A8E3B31DB64BF8B8C2C2AE7E0A6A777
2 2019-09-19_P4_P5_v2.24.5.zip	648A2D9B62D401A154144A9D24CFFBBD EB6E8428279734C103AEBF3BC9C8EC6C

for a more secure society



Resultaten hertest

Onderstaande tabel geeft de status van de bevindingen weer ten tijde van de hertest, waarbij de kleur geel aangeeft dat een bevinding gedeeltelijk is opgelost en groen dat een bevinding in zijn geheel is opgelost voor zover dit door Fox-IT vastgesteld kon worden.

#	Resultaat	Kiesraad omschrijving ¹	Opmerking
1	Opgelost	Modified EML files in archive directory on the server aren't detected	Opgelost. Let wel, dit kan door een aanvaller met de juiste voorbereiding omzeild worden, dit is inherent aan de opzet van de software.
2	Opgelost	Persistent Cross-Site Scripting (XSS)	HTML-bestanden in de export map kunnen niet meer aangeroepen worden.
3	Opgelost	Gedetailleerde stack traces	Enkel generieke meldingen worden getoond.
4	Opgelost	OSV database can be easily modified and votes can be changed	Opgelost, database is voorzien van wachtwoord. Let wel, dit kan door een aanvaller met de juiste voorbereiding omzeild worden, dit is inherent aan de opzet van de software.
5	Opgelost	OSV database isn't protected by a password	Opgelost, database is voorzien van wachtwoord. Let wel, dit kan door een aanvaller met de juiste voorbereiding omzeild worden, dit is inherent aan de opzet van de software.
6	Opgelost	Verkiezingsleider is not allowed to enter polling station results (P4_PSB)	Strikt genomen opgelost, maar een verkiezingsleider kan altijd een extra account voor zichzelf aanmaken zodat de resultaten alsnog ingevuld kunnen worden. Kan gemitigeerd worden door audit logs te controleren.
7	Opgelost	Verkiezingsleider is not allowed to enter municipality results (P4_HSB)	Strikt genomen opgelost, maar een verkiezingsleider kan altijd een extra account voor zichzelf aanmaken. Kan gemitigeerd worden door audit logs te controleren.
8	Opgelost	Verkiezingsleider is not allowed to enter kieskring results (P4_CSB)	Strikt genomen opgelost, maar een verkiezingsleider kan altijd een extra account voor zichzelf aanmaken. Kan gemitigeerd worden door audit logs te controleren.
9	Deels opgelost	HMAC-controle is te omzeilen	Kan nog steeds omzeild worden. Let wel, de implementatie van additionele autorisatiecontroles maakt deze maatregel minder relevant en mitigeert een groot deel van de gevolgen. Technisch blijft het mogelijk om parameters in de URL te manipuleren, echter de gevolgen hiervan zijn beperkt.

¹ Originale omschrijving uit brondocumenten.

Aan: De Kiesraad

T.a.v. 5.1.2.e en 5.1.2.e

Auteurs: 5.1.2.e en 5.1.2.e

Betreft: Hertest OSV versie 2.24.1 – Memorandum

Ref. nr. PR-180188

Datum: 23 april 2019

Classificatie: COMMERCIAL.RESTRICTED.KIESRAAD

Status: Concept

Versie: 0.1

Inleiding

De Kiesraad heeft Fox-IT gevraagd om een hertest uit te voeren van de hieronder genoemde bevindingen. De hertest heeft zich beperkt tot het testen van de genoemde bevindingen en het bepalen of deze als opgelost beschouwd kunnen worden. Tijdens de hertest is geen verder onderzoek verricht naar nieuwe kwetsbaarheden.

Daarnaast wordt opgemerkt dat onderstaande technische bevindingen niet een volledig beeld geven van de beveiliging van het gehele verkiezingsproces. Op basis van enkel deze technische bevindingen kunnen dus geen conclusies getrokken worden over de weerbaarheid van het gehele verkiezingsproces.

#	Kiesraad referentie	Kiesraad omschrijving
1	OSV-2009	Prevent showing stacktrace and server info to the user (OSV P4 and P5)
2	OSV-2013	Prevent the access of other .jsp sites (OSV P4 and P5)
3	OSV-2121	Control the authorization of a user if he/she opens a page or performs an action
4	OSV-2149	Prevent access without authentication to pages
5	OSV-2001	Improve protection against XSS (OSV P4 and P5)
6	OSV-2081	Verkiezingsleider is not allowed to enter polling station results (P4_PSB)
7	OSV-2082	Verkiezingsleider is not allowed to enter municipality results (P4_HSB)
8	OSV-2083	Verkiezingsleider is not allowed to enter kieskring results (P4_CSB)
9	OSV-2087	Prevent that result is set by single result file import in P4_HSB and P4_CSB
10	OSV-2122	Privilege escalation vulnerability (second HMAC bypass)
11	OSV-2159	OSV-2121 Control the authorization of a user if he/she performs an action

Voor het uitvoeren van de hertest zijn de volgende bestanden door de Kiesraad aangeleverd:

#	Bestandsnaam	SHA256
1	osv45_v2.24.1_source_for_review.zip	E2605FC018DA0A694BA2EB177CFB39C0 037B926FE469981A397A1625552C109F
2	osv_programma4en5_installer_v2.24.1.zip	DF311A8D5AF3F530AD3B4C1B56131BAF F3057B95848F8AA94B095378EF42F91B

for a more secure society

Resultaten hertest

Onderstaande tabel geeft de status van de bevindingen weer ten tijde van de hertest, waarbij de de kleur rood aangeeft dat een bevinding niet is opgelost, geel dat een bevinding gedeeltelijk is opgelost en groen dat een bevinding in zijn geheel is opgelost voor zover dit door Fox-IT vastgesteld kon worden. Voor de bevindingen die niet zijn opgelost is een restrisiko ingeschat, daarbij is in beperkte mate rekening gehouden met de meest relevantie niet-technische maatregelen die impact hebben op de betreffende bevinding.

#	Resultaat	Kiesraad omschrijving	Opmerking
1	Deels opgelost	Prevent showing stacktrace and server info to the user (OSV P4 and P5)	Applicatie toont geen stack traces meer, Jboss wel.
2	Opgelost	Prevent the access of other .jsp sites (OSV P4 and P5)	-
3	Opgelost	Control the authorization of a user if he/she opens a page or performs an action	-
4	Opgelost	Prevent access without authentication to pages	-
5	Deels opgelost	Improve protection against XSS (OSV P4 and P5)	Één specifieke XSS is opgelost, overige XSS bevindingen zijn nog aanwezig. Het is niet mogelijk om een uitputtende lijst aan te leveren, dit dient in de broncode opgelost te worden.
6	Niet opgelost	Verkiezingsleider is not allowed to enter polling station results (P4_PSB)	De verkiezingsleider kan deze rol opnieuw aan zichzelf toekennen of een gebruiker aanmaken met deze rechten. Beide acties zijn in de huidige logging herleidbaar.
7	Niet opgelost	Verkiezingsleider is not allowed to enter municipality results (P4_HSB)	De verkiezingsleider kan deze rol opnieuw aan zichzelf toekennen of een gebruiker aanmaken met deze rechten. Beide acties zijn in de huidige logging herleidbaar.
8	Niet opgelost	Verkiezingsleider is not allowed to enter kieskring results (P4_CSB)	De verkiezingsleider kan deze rol opnieuw aan zichzelf toekennen of een gebruiker aanmaken met deze rechten. Beide acties zijn in de huidige logging herleidbaar.
9	Opgelost	Prevent that result is set by single result file import in P4_HSB and P4_CSB	-
10	Deels opgelost	Privilege escalation vulnerability (second HMAC bypass)	Verhogen privileges is verholpen het omzeilen van de HMAC controle is nog steeds van toepassing.
11	Opgelost	OSV-2121 Control the authorization of a user if he/she performs an action	-

Aan: De Kiesraad
Auteurs: 5.1.2.e en 5.1.2.e
Betreft: Hertest OSV versie 2.24.1 – Memorandum
Ref. nr. PR-180272
Datum: 23 April 2019
Classificatie: PUBLIC
Status: Definitief
Versie: 1.0

Inleiding

De Kiesraad heeft Fox-IT gevraagd om een hertest uit te voeren van de hieronder genoemde bevindingen. Dit memorandum betreft een aanvulling op de bevindingen in paragraaf 4.3 en 4.4 van het rapport¹ van 12-03-2019. De hertest heeft zich beperkt tot het testen van de genoemde bevindingen en het bepalen of deze als opgelost beschouwd kunnen worden. Tijdens de hertest is geen verder onderzoek verricht naar nieuwe kwetsbaarheden.

Op basis van enkel deze technische bevindingen kunnen dus geen conclusies getrokken worden over de weerbaarheid van het gehele verkiezingsproces.

#	Kiesraad referentie	Kiesraad omschrijving
1	OSV-2009	Prevent showing stacktrace and server info to the user (OSV P4 and P5)
2	OSV-2013	Prevent the access of other .jsp sites (OSV P4 and P5)
3	OSV-2121	Control the authorization of a user if he/she opens a page or performs an action
4	OSV-2149	Prevent access without authentication to pages
5	OSV-2001	Improve protection against XSS (OSV P4 and P5)
6	OSV-2081	Verkiezingsleider is not allowed to enter polling station results (P4_PSB)
7	OSV-2082	Verkiezingsleider is not allowed to enter municipality results (P4_HSB)
8	OSV-2083	Verkiezingsleider is not allowed to enter kieskring results (P4_CSB)
9	OSV-2087	Prevent that result is set by single result file import in P4_HSB and P4_CSB
10	OSV-2122	Privilege escalation vulnerability (second HMAC bypass)
11	OSV-2159	OSV-2121 Control the authorization of a user if he/she performs an action

Voor het uitvoeren van de hertest zijn de volgende bestanden door de Kiesraad aangeleverd:

#	Bestandsnaam	SHA256
1	osv45_v2.24.1_source_for_review.zip	E2605FC018DA0A694BA2EB177CFB39C0 037B926FE469981A397A1625552C109F
2	osv_programma4en5_installer_v2.24.1.zip	DF311A8D5AF3F530AD3B4C1B56131BAF F3057B95848F8AA94B095378EF42F91B

¹ Rapport FOX-IT beveiligingsonderzoek OSV 14-3-2019.pdf

Resultaten hertest

Onderstaande tabel geeft de status van de bevindingen weer ten tijde van de hertest, waarbij de kleur rood aangeeft dat een bevinding niet is opgelost, geel dat een bevinding gedeeltelijk is opgelost en groen dat een bevinding in zijn geheel is opgelost voor zover dit door Fox-IT vastgesteld kon worden. Voor de bevindingen die niet zijn opgelost, is een restrisico ingeschat, waarbij in beperkte mate rekening gehouden is met de meest relevantie niet-technische maatregelen die impact hebben op de betreffende bevinding.

#	Resultaat	Kiesraad omschrijving	Opmerking
1	Deels opgelost	Prevent showing stacktrace and server info to the user (OSV P4 and P5)	Applicatie toont geen stack traces meer, Jboss wel.
2	Opgelost	Prevent the access of other .jsp sites (OSV P4 and P5)	-
3	Opgelost	Control the authorization of a user if he/she opens a page or performs an action	-
4	Opgelost	Prevent access without authentication to pages	-
5	Deels opgelost	Improve protection against XSS (OSV P4 and P5)	Eén specifieke XSS is opgelost, overige XSS bevindingen zijn nog aanwezig. Het is niet mogelijk om een uitputtende lijst aan te leveren, dit dient in de broncode opgelost te worden.
6	Niet opgelost	Verkiezingsleider is not allowed to enter polling station results (P4_PSB)	De verkiezingsleider kan deze rol opnieuw aan zichzelf toekennen of een gebruiker aanmaken met deze rechten. Beide acties zijn in de huidige logging herleidbaar.
7	Niet opgelost	Verkiezingsleider is not allowed to enter municipality results (P4_HSB)	De verkiezingsleider kan deze rol opnieuw aan zichzelf toekennen of een gebruiker aanmaken met deze rechten. Beide acties zijn in de huidige logging herleidbaar.
8	Niet opgelost	Verkiezingsleider is not allowed to enter kieskring results (P4_CSB)	De verkiezingsleider kan deze rol opnieuw aan zichzelf toekennen of een gebruiker aanmaken met deze rechten. Beide acties zijn in de huidige logging herleidbaar.
9	Opgelost	Prevent that result is set by single result file import in P4_HSB and P4_CSB	-
10	Deels opgelost	Privilege escalation vulnerability (second HMAC bypass)	Verhogen privileges is verholpen, het omzeilen van de HMAC controle is nog steeds van toepassing.
11	Opgelost	OSV-2121 Control the authorization of a user if he/she performs an action	-

QM MANUAL

RELEASE REPORT

Project:	OSV		
Created on:	17 May 19	by:	5.1.2.e
Last change:	17 May 19	by:	5.1.2.e
Release date:	17 May 19	by:	5.1.2.e
Version	P4/P5 v2.24.4		
Status:	released		

RELEASE REPORT

Release	P4/P5 v2.24.4		
QS-Manager	5.1.2.e	Release date	17 May 19

All named issues can be found on JIRA (<http://confluence.ivu.de/jira>).

SOFTWARE COMPONENTS

Component title	Version	OK	Comment
Program 0		n.r.	
Program 1		n.r.	
Program 2-3		n.r.	
Program 4	2.24.4	☒	Issues see below
Program 5	2.24.4	☒	Issues see below

Legend:

n.r.: not released

red: critical error (prevents functionality)

SOLVED ISSUES

ID	Prg	Description	Solution
OSV-2001	P4, P5	Improve protection against XSS (OSV P4 and P5)	It is no longer possible to upload an .html file to werkmap of the OSV server and use it for a XSS attack. It is no longer possible to inject JavaScript in the 'Veranderen instellingen' page. It is no longer possible to inject JavaScript in the 'view' parameter that is executed on the 'Ongewoon URL-manipulatie' page.
OSV-2161	P4, P5	Calling JSP pages directly may cause error page with stack trace	The error page for a "HTTP Status 500" error now no longer contains the stack trace.
OSV-2171	P4	Error when opening "Mutatieoverzicht" for area on "Status" page PSB, HSB and CSB	<p>"If a jsp page is opened directly without being logged into the OSV application and the authorization check can detect that the user is not logged in, now the correct error message "U bent niet (meer) ingelogd." (instead of "!ERROR_NotLoggedIn!") is shown.</p> <p>On the status page "Statusoverzicht stembureaus" the links under the region names in the "Gebied" column now lead to the corresponding "Mutatieoverzicht". This "Mutatieoverzicht" is no longer shown in a pop-up-window but in the regular application window instead."</p>
OSV-2172	P4	User get message "U heeft niet de juiste rechten.." go to "Beheer" menu	When a user without the right to view the users that are logged on to OSV opens the 'Beheer' menu, now the page 'change password' opens. In this case the message that rights are missing is no longer shown.

Overzicht verbeteringen OSV na GR2018 en voor PS/EP2019

De papieren uitslagen van het stembureau zijn toegankelijker geworden

Het proces-verbaal van het stembureau en de opgave van de totalen van de gemeenten worden op internet beschikbaar gesteld. Voorheen lagen deze documenten enkel ter inzage. Hierdoor wordt het voor burgers beter mogelijk om de uitslagen vanaf het laagste niveau na te rekenen en te vergelijken met de resultaten uit OSV. Documenten ten behoeve van de vaststelling van de uitslagen worden met OSV opgesteld. Met de aanpassing in de wetgeving is het, meer dan voorheen, mogelijk om de optellingen in de documenten uit OSV te controleren met de gegevens die niet met de software tot stand zijn gekomen.

Bijwerken van standaardsoftwarecomponenten en technische verbeteringen

Een aantal standaardsoftwarecomponenten die in de OSV-software wordt toegepast zijn bijgewerkt. Het gaat hierbij met name om Java, Derby en jQuery. Door het bijwerken van deze componenten kunnen de kwetsbaarheden die in de oudere versies van deze componenten aanwezig zijn niet meer worden uitgebuit in relatie tot de OSV-software. In relatie tot het bijwerken van met name Java naar versie 1.8 zijn ook enkele andere technische kwetsbaarheden weggenomen. Het gaat daarbij om de ondersteuning van TLS (in plaats van SSL 3.0) en elementen als het toepassen van HTTP Strict Transport Security, Content Security Policy, Integer overflow protection, XML schema validation en XML External Entity Injection.

Afschermen van de communicatiepoorten op de OSV-computer

De afscherming van de communicatiepoorten in relatie tot de OSV-computer is verbeterd. Dit is deels gedaan door betere instructies te geven over het instellen van de systeem firewall, waarbij de toegangspoort wordt beperkt tot de noodzakelijke communicatiepoort. Naast de aanvullende instructie is de technische configuratie van OSV aangepast, waarmee ook in technische zin bepaalde communicatiepoorten niet meer voor externe toegang beschikbaar zijn.

Het wachtwoord beleid binnen OSV is aangescherpt

Een minimale wachtwoordlengte van 9 karakters wordt door de OSV-software afgedwongen. Daarnaast wordt in de voorwaarden die de gebruikers krijgen aangegeven dat bij de rol van verkiezingsleider een wachtwoord van minimaal 12 karakters dient te worden toegepast. Hierbij wordt als advies meegegeven om een wachtwoordzin te gebruiken. De codering (Base64) voor hashing van het wachtwoord is aangepast zodat volledige set van karakters voor het wachtwoord mogelijk is.

Autorisatie

Gebruikers dienen op basis van de ingestelde autorisatieprofielen geautoriseerd te zijn om gebruik te kunnen maken van bepaalde functionaliteit in OSV. Door aanvullende autorisatiecontrole op te nemen in de JavaServer Pages (JSP) vindt er een striktere controle plaats of een gebruiker geautoriseerd is voor een bepaalde functionaliteit. Ook de mogelijkheden om de Hashed Message Authentication Code (HMAC) controle te omzeilen zijn ingeperkt. Het is echter nog niet gelukt om alle varianten van een HMAC-bypass uit te sluiten.

Het vier-ogen-principe wordt meer afgedwongen

Er zijn aanpassingen in OSV doorgevoerd die technisch voorkomen dat dezelfde gebruiker zowel de eerste als de tweede invoer uitvoert. Daarnaast is het niet meer mogelijk dat de verkiezingsleider

uitslagen invoert. Hiermee wordt de rol van verkiezingsleider beter gescheiden van de gebruiker die de invoer doet.

Andere technische opgeloste constatering

Naar aanleiding van het recent uitgevoerde beveiligingsonderzoek zijn de volgende kwetsbaarheden naar voren gekomen die in de uiteindelijke versie zijn verholpen. Het gaat daarbij om de mogelijkheid willekeurige bestandstypen te uploaden naar de OSV-server computer. Een ander punt dat is verholpen is de mogelijkheid om de hashcode-controle die wordt uitgevoerd bij het inlezen van gegevensbestanden te omzeilen. Tevens wordt bepaalde beveiligingsgevoelige informatie (zoals session id en wachtwoord-hash) niet meer volledig in het log-bestand vermeld. Er worden bij foutmeldingen geen stacktraces meer getoond en er wordt bij de installatie op de door OSV gebruikte database een wachtwoord ingesteld. Tot slot is het niet meer mogelijk om via de "back" optie van de browser web-pagina's van eerdere gebruikers te bekijken.

Niet opgeloste bevindingen

Er zijn ook bevindingen die nog niet (volledig) zijn opgelost en er zijn een aantal nieuwe bevindingen naar voren gekomen naar aanleiding van het recent uitgevoerde beveiligingsonderzoek.

Een van de onderdelen waarvan het bijwerken tot op heden niet mogelijk was is het verouderde JBoss onderdeel dat met OSV wordt gebruikt. Het veranderen van de huidige gebruikte JBoss versie naar een nieuwere versie is niet zondermeer mogelijk aangezien dat tevens een nieuwe JBoss standaard (EJB) inhoudt. Het wijzigen van de standaard heeft gevolgen voor meerdere onderdelen van de OSV-software en daarmee een grote impact op het goed functioneren van OSV.

Ten aanzien van kwetsbaarheden die verband hebben met de mogelijkheden van Cross-Site Scripting (XSS) zijn er verscheidene verholpen. Er zijn echter nog XSS-mogelijkheden aanwezig die nog niet verholpen zijn. Met betrekking tot de mogelijkheid om de Hashed Message Authentication Code (HMAC) controle te omzeilen is gebleken dat deze nog niet voor alle situaties verholpen is. Echter, door de nieuwe autorisatiecontrole op de pagina's is het niet meer mogelijk om pagina's te openen met functionaliteit waarvoor men niet geautoriseerd is. Tot slot is gebleken dat de een striktere autorisatiecontrole met betrekking tot de "Werkmap" binnen OSV niet zonder meer mogelijk is. De aanpassing in JSP, zoals dat voor andere functionaliteiten is gedaan, blijkt voor de Werkmap niet mogelijk te zijn.

Relevante aanpassingen OSV v2.24.1

ID	Prg	Description	Solution
OSV-2009	P4, P5	Prevent showing stacktrace and server info to the user (OSV P4 and P5)	The error page of programs P4 and P5 no longer shows the exception stack trace in case an unexpected error (exception) occurs.
OSV-2013	P4, P5	Prevent the access of other .jsp sites (OSV P4 and P5)	See OSV-2121.
OSV-2121	P4, P5	Control the authorization of a user if he/she opens a page or performs an action	All jsp pages now have an authorisation check. If the page is opened by a user who is not logged in or does not have the necessary rights, an error message is shown.
OSV-2149	P4, P5	Prevent access without authentication to pages	See OSV-2121.
OSV-2001	P4, P5	Improve protection against XSS (OSV P4 and P5)	It is no longer possible to upload an .html file to werkmap of the OSV server and use it for a XSS attack.
OSV-2081	P4	Verkiezingsleider is not allowed to enter polling station results (P4_PSB)	In P4_PSB the user with the role 'Verkiezingsleider' is no longer allowed to manually enter results. The top-menu option 'Invoeren stemtotalen' and the input page are no longer available for user which this role.
OSV-2082	P4	Verkiezingsleider is not allowed to enter municipality results (P4_HSB)	In P4_HSB the user with the role 'Verkiezingsleider' is no longer allowed to manually enter results. The top-menu option 'Invoeren stemtotalen' and the input page are no longer available for user which this role.
OSV-2083	P4	Verkiezingsleider is not allowed to enter kieskring results (P4_CSB)	In P4_CSB the user with the role 'Verkiezingsleider' is no longer allowed to manually enter results. The top-menu option 'Invoeren stemtotalen' and the input page are no longer available for user which this role.
OSV-2087	P4	Prevent that result is set by single result file import in P4_HSB and P4_CSB	When in program P4_HSB or P4_CSB the input mode "2 = dubbele invoer" is active and an EML telling file is imported, then another user still needs to enter the result manually to confirm the input in the same way as this is required when the input mode "3 = inlezen plus invoer" is active.
OSV-2122	P4, P5	Privilege escalation vulnerability (second HMAC bypass)	The HMAC test of OSV now considers all requests that do not contain any parameters (except for the request to open the login page) as manipulated and shows the corresponding error page. Bypassing the HMAC check now can no longer be used to open a page or perform an action without authorization.

ID	Prg	Description	Solution
OSV-2159	P4, P5	OSV-2121 Control the authorization of a user if he/she performs an action	All actions now have an authorisation check. If the action is performed by a user who is not logged in or does not have the necessary rights, the action is not executed.

Fox rapport 14-3-19	Fox memo 23-4-19	Bevinding	Verwijzing	Omschrijving + Opmerkingen	Description	OSV JIRA
		Modified EML files in archive directory on the server aren't detected	5.1.2.e par. 4.1.18 (p. 43)	OSV software controleert niet of gegenereerde EML files nadien op de server worden aangepast door een hacker. Laat OSV continu controleren of de inhoud van de op de server opgeslagen EML bestanden buiten OSV om wordt gewijzigd.	"OSV software does not check whether generated EML files on the server are subsequently modified by a hacker. Let OSV continuously check if the content of the EML files stored on the server is changed outside of OSV. "	OSV-2000
bevinding 3. nieuw	5. Deels opgelost	Persistent Cross-Site Scripting (XSS)	Rapport Fox-IT 2019, bevinding 3	XSS kan gebruikt worden om de bij een gebruiker getoonde website te veranderen of Javascript code uit te voeren op de computer van een gebruiker. Het gevolg daarvan is dat het lijkt alsof deze code afkomstig is van OSV. In tegenstelling tot een niet persistent Cross-Site Scripting (XSS) aanval wordt bij deze aanval de code op de server opgeslagen. Het risico is dat de code elke keer opnieuw aan de betreffende gebruiker getoond wordt. Mogelijk wordt de betreffende code ook getoond en uitgevoerd door andere gebruikers, bijvoorbeeld door een verkiezingsleider.	XSS can be used to change the website displayed by a user or to execute JavaScript code on a user's computer. As a result, it appears that this code is from OSV. Unlike a non-persistent Cross-Site Scripting (XSS) attack, the code stores the code on the server. The risk is that the code is shown to the relevant user every time. The relevant code may also be displayed and executed by other users, for example by an election leader.	OSV-2001
bevinding 4. nieuw	1. Deels opgelost	Gedetailleerde stack traces	Rapport Fox-IT 2019, bevinding 4	Kennis van de achterliggende structuur van de webapplicatie kan een aanvaller helpen om de webapplicatie en de systemen in kaart te brengen en zo een verdere aanval voor te bereiden.		OSV-2161 OSV-2009 OSV-1962
		OSV database can be easily modified and votes can be changed	5.1.2.e par. 4.1.2 (p. 22)	De door OSV gebruikte database is niet voorzien van een wachtwoord. Een persoon die toegang heeft tot de OSV programma bestanden op de OSV server computer kan als 'relatie' eenvoudig toegang krijgen tot de database, met als mogelijk gevolg het aanpassen van (uitslag)gegevens in de database.	The database used by OSV is not provided with a password. A person who has access to the OSV program files on the OSV server computer can easily gain access to the database as a "relation", with the possible consequence of adjusting (result) data in the database.	OSV-1994

Zie ook nummer 53

		OSV database isn't protected by a password	5.1.2.e par. 4.1.16 (p. 41)	OSV database is niet beveiligd met wachtwoord	OSV database is not protected with password	OSV-1994
	6. Niet opgelost	Verkiezingsleider is not allowed to enter polling station results (P4_PSB)				OSV-2081
	7. Niet opgelost	Verkiezingsleider is not allowed to enter municipality results (P4_HSB)				OSV-2082
	8. Niet opgelost	Verkiezingsleider is not allowed to enter kieskring results (P4_CSB)				OSV-2083
bevinding 5. nieuw	10. deels opgelost	HMAC-controle is te omzeilen	Rapport Fox-IT 2019, bevinding 5	De HMAC is een beveiligingsmethode in OSV. Door deze te omzeilen wordt een belangrijke beveiligingsmaatregel onklaar gemaakt waarmee het voor aanvallers mogelijk wordt andere aanvallen uit te voeren of om bepaalde processen te negeren.	The HMAC is a security method in OSV. Bypassing this, an important security measure is disabled, making it possible for attackers to perform other attacks or to ignore certain processes.	OSV-2122 OSV-2098

KIESRAAD



Onderwerp	Eerste verkenning routes ontwikkeling verkiezingssoftware
Datum	23 maart 2023
Opstellers	5.1.2.e 5.1.2.e
Kenmerk	2023-0000086689

Aan: Kiesraad

1. Inleiding

De huidige stand van zaken in het DHV-traject is aanleiding voor de Kiesraad om na te denken over eventuele scenario's waarbij in een nieuw traject tot ontwikkeling van nieuwe verkiezingssoftware wordt gekomen.

Hiertoe is op 27 februari jl. in de Kiesraad – mede op basis van een advies van de Landsadvocaat – afgesproken dat er een eerste verkenning wordt uitgewerkt van drie opties:

- (A) Interimoplossing: continuering dienstverlening en doorontwikkeling OSV2020 na 13 juli 2025
- (B) Europees aanbesteden (openbaar) - Ontwikkeling van een nieuw DHV
- (C) Ontwikkeling van een nieuwe verkiezingssoftware door dit (gedeeltelijk zelf) modulair te ontwikkelen.

De opties zijn onder te brengen in twee routes. De Interim oplossing maakt - gezien de benodigde doorlooptijd voor ontwikkeling van nieuwe verkiezingssoftware - logischerwijs onderdeel uit van beide routes.

Route 1: (A) Interim oplossing - continuering OSV2020 en (B) Aanbesteding nieuw DHV

Route 2: (A) Interim oplossing - continuering OSV2020 en (C) Modulair ontwikkelen nieuwe verkiezingssoftware

Een eerste verkenning van deze routes is in deze notitie uitgewerkt. Daarop is input ontvangen van BZK-collega's van CIO Office, CDI Office, CZW, D&B en RIS. Het vergt komende periode nadere uitwerking om tot besluitvorming te kunnen komen.

2. Gevraagd besluit

De Kiesraad wordt gevraagd:

1. Kennis te nemen van de notitie *Eerste verkenning routes ontwikkeling verkiezingssoftware*;
2. In te stemmen met het advies om beide routes nader uit te werken: inhoudelijk, qua doorlooptijd en in financiële termen;
3. In te stemmen om hiertoe externe expertise te betrekken voor het analyseren van het lopende traject, hieruit lessons learned te trekken en deze te betrekken bij de uitwerking van beide routes;
4. Hiertoe binnen de bestedingsmiddelen van de Kiesraad middelen te vinden.

3. Evaluatie - Lessons learned

Interne lessen

Op basis van een eerste inventarisatie hebben we – intern Kiesraad – een aantal lessons learned geïdentificeerd uit de aanbesteding en de lopende implementatie van DHV:

Aanbestedingsexpertise

De Kiesraad dient ruime expertise en ervaring binnen het bureau te hebben of te organiseren op:

- Aanbestedingstrajecten, in het bijzonder IT-aanbestedingen
- Kennis en ervaring te hebben op het aansturen van een (bestuurlijke) governance)
- Oog te hebben voor het maatschappelijke belang en risico's

Dit kan worden gevonden in een (extern) projectleider, directeur, of vergelijkbare functie

Kennis en ervaring van verkiezingssoftware

Kennis van en ervaring met verkiezingssoftware – in alle facetten – vanuit bureau betrekken bij de ontwikkeling van nieuwe verkiezingssoftware:

- Betrokkenheid vanuit het bureau van business analisten tot testers is van belang om een ontwikkeltraject goed te kunnen uittekenen, en vervolgens te begeleiden.
- Deze kennis dient bij het bureau Kiesraad intern aanwezig te zijn, omdat deze na de ontwikkeling van de nieuwe verkiezingssoftware ook beheer, onderhoud en ontwikkeling inhoudelijk moet kunnen begeleiden.

Helderheid over diepgang en 'completeheid'

Het programma van eisen alsmede de kwaliteitstandaard op basis waarvan de kwaliteit van de te ontwikkelen software wordt beoordeeld dient helder te zijn. Dit geldt ook voor de mate van diepgang en 'completeheid' van zowel de specificaties van nieuwe verkiezingssoftware als voor de te ontwikkelen software.

Heldere governance

De governance dient – net als in het huidige DHV-traject – helder te zijn. Dit maakt dat zowel in- als extern goed en snel kan worden geschakeld in geval dit noodzakelijk is, bijvoorbeeld bij escalatie.

Projectmanagement, sturing, samenwerking en documentatie

Het interne projectmanagement en dossiervorming (documentatie) verdient vanaf het moment dat een aanbestedings- en ontwikkeltraject start zorgvuldige aandacht. Hierbij is een aantal zaken van belang:

- Heldere sturing op deadlines en planning
- Escalatie bij niet nakomen afspraken
- Geen rolvermenging tussen opdrachtgever en opdrachtnemer

- Dossievorming vanaf het moment dat de start van het traject
- Alle communicatie en interactie in de Nederlandse taal

Ontwikkelmethode

Door leverancier gekozen waterval-ontwikkelmethode maakt kwetsbaar en kent in ieder geval de volgende aandachtspunten en risico's:

- Een klant-leveranciersrelatie in plaats van partnership
- Zicht op voortgang traject
- Aantal mogelijkheden om tussentijds te kunnen bijsturen

Een andere ontwikkelmethode dan de watervalmethode, waarbij iteratief of agile wordt ontwikkeld mitigeert deze aandachtspunten en risico's.

Contractuele zaken

Het is van belang in het contract de juiste artikelen op te nemen die zie op een situatie waarin het ontwikkeltraject met een leverancier/samenwerkingspartner niet goed verloopt. Hierbij moet worden gedacht aan de volgende zaken:

- Opnemen van een boetebeding bij niet nakoming van de overeenkomst
- Het koppelen van betalingen aan te leveren (en geleverde) prestaties
- Heldere afspraken over kosten voor onderhoud en ontwikkeling
- Wanneer en voor welke zaken er bijvoorbeeld een RfC wordt afgesproken

Continuïteit reguliere werkzaamheden

Uit de voorbije aanbestedingsprocedure en het huidige bouw- en implementatieproces is gebleken dat dit een grote wissel trekt op de capaciteit van het bureau van de Kiesraad en de ruimte die resteert voor reguliere werkzaamheden. De draagkracht van het bureau om bij de reguliere werkzaamheden een Europese aanbesteding uit te voeren (en bouw- en implementatie te begeleiden) is echt beperkt in het licht van de benodigde organisatieontwikkeling. Dit vraagt met oog op een mogelijk nieuw proces om tot verkiezingssoftware te komen extra aandacht.

De komende periode werken we deze lessons learned nader uit en vertalen we deze waar mogelijk ook in eisen of voorwaarden in een mogelijk nieuw traject.

Externe blik

Om te voorkomen dat we gekleurd kijken naar de afgelopen aanbestedingsprocedure en het lopende ontwikkeltraject, en onze eigen rol hierin, stellen we voor dat we op basis van het dossier een externe toets laten doen om van te kunnen leren. Deze lessen kunnen we betrekken bij een eventueel nieuw traject. Daarbij willen we in ieder geval laten kijken naar lessen die we kunnen trekken uit en rondom de gevolgde aanbestedingsprocedure

- de gesloten overeenkomst (in relatie tot de aanpak van de leverancier)
- de ingerichte en uitgevoerde projectaanpak en governance van/door de Kiesraad

Voor het evalueren van de aanbestedings- en ontwikkeltraject van DHV, als ook voor het toetsen van de door ons voorgestelde weg voorwaarts, wil de Kiesraad het Adviescollege ICT-toetsing (AcICT) om advies vragen¹.

¹ bij een evaluatie van een complex aanbesteding- en implementatietraject bij V&J, AcICT een advies voor vervolgetraject heeft gegeven dat nauw aansluit bij de in deze notitie door de Kiesraad voorgestelde aanpak (zie [hier](#)).

4. Eerste uitwerking van opties A, B, C

Deze paragraaf bevat een eerste uitwerking van de opties:

(A) Interimoplossing: continuering dienstverlening en doorontwikkeling OSV2020 na 13 juli 2025 (hierna: continuering OSV2020)

(B) Europees aanbesteden (openbaar) - Ontwikkeling van een nieuw DHV

(C) Ontwikkeling van een nieuwe verkiezingssoftware door dit (gedeeltelijk zelf) modulair te ontwikkelen

Hierbij beschrijven we steeds de volgende elementen:

- i. Wat betekent dit voor de Kiesraad
- ii. Wat hebben we hiervoor nodig (capaciteit/tijd/prioriteit)
- iii. Wat betekent dit voor gebruikers/afnemers

(A) Interimoplossing: continuering dienstverlening en doorontwikkeling OSV2020 na 13 juli 2025

i. Wat betekent dit voor de Kiesraad

Hoewel de periode tot 13 juli 2025 nog ruim 2 jaar duurt, is het niet realistisch om te verwachten dat er in die periode een geheel nieuwe DHV applicatie, (aanbesteed) gebouwd en in gebruik genomen is. Naar verwachting zal de ontwikkeling van nieuwe verkiezingssoftware ten minste twee jaar duren vanaf het moment dat de Kiesraad na het doorlopen van een her-aanbesteding een nieuwe opdrachtnemer heeft geselecteerd.

Bovendien geldt dat ook dat na de ontwikkeling en de oplevering van nieuwe verkiezingssoftware, OSV2020 nog enige tijd als backup in gebruik dient te blijven. Dit van belang om te voorkomen dat – indien blijkt er onverhoopte tekortkomingen blijken bij een eerste gebruik van nieuwe functionaliteit gebruikers van de software een alternatief kan worden geboden in de vorm van OSV2020.

Al met al betekent dit dat de Kiesraad ten minste nog tot eind 2027 OSV2020 dienstverlening dient af te nemen, onder de nieuw af te sluiten (interim) overeenkomst.

Bovendien is het daarbij van belang - om te voorkomen dat eind 2027 een situatie ontstaat van tijdsdruk en mogelijk onrechtmatige verlengingen – dat bij een nieuwe (interim) overeenkomst voldoende verlengmogelijkheden worden overeengekomen voor het gebruik van OSV2020.

Hoe te komen tot een nieuwe overeenkomst

De landsadvocaat heeft geadviseerd om de continuering van de dienstverlening van OSV2020 via een openbare Europese aanbesteding te realiseren. Dit is te verkiezen boven het kiezen voor een uitzonderingsgrond waarop de huidige overeenkomst nog zou kunnen worden verlengd.

Vanzelfsprekend gevolg van het uitschrijven van een Europese aanbesteding is dat ook andere opdrachtnemers dan de huidige leverancier (Elect-iT) als nieuwe contractpartij uit de Europese aanbesteding kunnen komen. Deze manier van continuering van de dienstverlening van OSV2020 biedt concurrentiedruk, al is het de verwachting dat het aantal partijen dat geïnteresseerd is in deze aanbesteding minimaal zal zijn.

De OSV2020 programmatuur is opgebouwd uit drie modules die separaat afgenomen kunnen worden, dit kan relevant zijn voor de combinatie route 1 maar met name ook voor route 2. Zo kan bij route 2 de modules één voor één gemoderniseerd worden, en indien gewenst, gecentraliseerd worden ingericht. In dit traject kunnen we het aantal afgenomen OSV2020 modules gradueel afbouwen en vervangen door nieuwe componenten.

ii. Wat heeft de Kiesraad nodig

Het uitvoeren van een Europese aanbesteding vraagt de nodige voorbereidingen. Op hoofdlijnen zien deze voorbereidingen op:

Samenstellen aanbestedingsteam

De Rijks Inkoop Samenwerking (RIS) heeft een overzicht van de benodigde functionarissen (bijlage 2) waarin de functiebenamingen en verantwoordelijkheden staan beschreven voor de teamleden bij een aanbesteding. Duidelijk is dat de Kiesraad verantwoordelijk is voor het leveren van input op de benodigde dienstverlening en contractuele afhandeling. Binnen het bureau van de Kiesraad is geen expertise aanwezig in het leiden van een ICT-aanbestedingsprocedure. Gezien de ervaring van de aanbesteding DHV is het zeer wenselijk deze expertise tijdelijk aan te trekken in een extern projectleider.

Analyse benodigde dienstverlening

Er dient door de Kiesraad onderzoek te worden gedaan naar de vraag of de huidige OSV2020 dienstverlening ook voor een verlengde periode voldoet of dat er aanpassingen nodig of gewenst zijn die kunnen worden meegenomen in een aanbestedingsprocedure.²

Doorlooptijd

Een Europese aanbesteding duurt gemiddeld 9 tot 12 maanden vanaf de kick-off tot gunning. Deze periode is exclusief de tijd voor een eventuele gerechtelijke procedure mocht deze aanhangig worden gemaakt.

Uitgangspunt bij een nieuwe aanbesteding is dat we het advies van de landsadvocaat volgen en een Europese openbare aanbesteding aangaan. Deze heeft een kortere doorlooptijd dan een niet-openbare Europese aanbesteding.

De uiteindelijke scope van de aan te besteden dienstverlening heeft ook effect op de doorlooptijd van de aanbesteding. Indien de scope veel aanpassing vraagt wordt de doorlooptijd vanzelfsprekend langer.

Een andere factor van betekenis is zekere capaciteit en expertise die in het aanbestedingsteam aanwezig moet zijn, opdat hierdoor geen vertraging in een procedure plaatsvindt. Tot slot is het van belang dat de aanbesteding voor continuering van OSV2020 zo (goed en) spoedig mogelijk wordt gestart. Dit om (a) na 13 juli 2025 niet in een situatie terecht te komen dat de OSV2020 programmatuur niet meer ondersteund wordt en (b) om geïnteresseerde partijen een realistische mogelijkheid te bieden om succesvol in te kunnen schrijven.

Kosten continuering gebruik OSV2020

De Kiesraad heeft op dit moment geen budget om een continuering van het gebruik van OSV2020 te financieren. Komende periode moeten we bekijken of en op welke manier middelen die gereserveerd zijn voor de ontwikkeling en implementatie van verkiezingssoftware hiervoor en voor een eventuele ontwikkeling van nieuwe software kunnen worden ingezet. Het is realistisch dat er in de voorliggende periode een aanvraag voor tijdelijke middelen bij BZK moet worden gedaan.

iii. Wat betekent dit voor gebruikers/afnemers

Technisch inhoudelijk zal er voor gebruikers weinig veranderen inzien zij langer gebruik maken van OSV2020. Daarbij komt dat er mogelijk betere functionaliteit en/of gebruikersinterface kan worden gerealiseerd.

Het is wel van belang dat wordt onderkend dat een continuering van het gebruik van OSV2020 betekent dat gebruikers langer gebruik gaan maken van deze software. Hierover dient de Kiesraad de gebruikers zorgvuldig te informeren.

² Hieronder valt ook een mogelijkheid om OSV2020 te laten doorontwikkelen tot een centrale variant of het aanpassen van de bestaande gebruikers interface / experience (UI/UX) met als doel de gebruikersvriendelijkheid van OSV2020 te vergroten.

5. Uitwerking: Europees Aanbesteden ontwikkeling verkiezingssoftware

i. Wat betekent dit voor de Kiesraad

De landsadvocaat heeft geadviseerd om – indien dit voor de Kiesraad opportuun wordt - met een openbare Europese aanbesteding leverancier voor de ontwikkeling van nieuwe verkiezingssoftware te contracteren. Praktisch betekent dit dat er in 2023 twee aanbestedingen gedeeltelijk parallel moeten worden uitgevoerd door de Kiesraad, zowel voor de interim oplossing als voor de (her)aanbesteding voor nieuwe verkiezingssoftware. Dit legt een zeer grote druk op het bureau van de Kiesraad.

Verkend moet worden of beide trajecten (de continuering van OSV2020 en de bouw van nieuwe verkiezingssoftware) ook in een gecombineerde aanbesteding kunnen worden uitgezet. De Landsadvocaat zag hiertoe juridisch geen belemmeringen. De Kiesraad zal nader moeten bezien welke voordelen dit biedt.

Het opnieuw aanbesteden van het ontwikkelen van nieuwe verkiezingssoftware een DHV applicatie zal een significante druk op de Kiesraad met zich meebrengen en dan met name voor de Business Analisten.

Hoewel we gedeeltelijk terug kunnen vallen op aanbestedingsdocumenten die bij de vorige aanbesteding zijn gebruikt, zal een nieuwe grondige functionele analyse moeten plaatsvinden, waarbij ook lessen worden getrokken uit de afgelopen aanbestedingsprocedure.

Conform het advies van de landsadvocaat ligt een keuze voor een openbare Europese aanbesteding voor de hand, bij een openbare procedure mogen alle gegadigden direct een inschrijving indienen, de doorlooptijd van deze procedure is korter.

Bij een niet-openbare procedure wordt eerst een aan de hand van geschiktheidseisen een selectie gemaakt van de gegadigden die zich aanmelden. Deze procedure duurt langer en is met name relevant:

- Als er sprake is van een marktsegment met potentieel veel inschrijvers of wanneer een bijzondere inspanning van inschrijvers wordt gevraagd, ligt het in de rede een niet-openbare procedure uit te schrijven. Daarmee blijft de kans om een opdracht gegund te krijgen in balans met de inspanning die het kost om een inschrijving op te stellen. Hiervan lijkt geen sprake.
- Het ontwikkelen van een DHV is een technisch complexe opgave en het vergt een behoorlijke inspanning om tot een inschrijving te komen. De belangstelling uit de markt was bij de vorige aanbesteding in 2020 zeer beperkt. Wel dient er aandacht te zijn voor tijdsdruk als een mogelijke oorzaak voor de geringe interesse uit de markt bij de vorige aanbesteding voor de ontwikkeling van de oplossing.

ii. Wat heeft de Kiesraad nodig

Lessons learned

De Kiesraad dient lessons learned uit de vorige aanbesteding mee te nemen in het vormgeven en uitvoeren van een nieuwe aanbesteding.

Zoals eerder in deze notitie is aangegeven is het raadzaam zowel intern lessons learned op te nemen alsook een externe partij onafhankelijk te laten kijken naar de lessons learned.

Samenstelling aanbestedingsteam

Hiervoor gelden dezelfde uitgangs- en aandachtspunten als bij de beschrijving van de interim-oplossing. Belangrijk te onderstrepen is dat het ook bij deze aanbesteding gewenst is een extern projectleider gespecialiseerd in Europese aanbestedingen tijdelijk aan te trekken.

Analyse benodigde dienstverlening

De documenten van de afgelopen aanbesteding kunnen als basis dienen voor een nieuwe aanbesteding. Lessons learned en nieuwe inzichten, wensen en eisen vanuit nieuwe wet- en regelgeving dienen hierbij te worden meegenomen bij herijking.

Doorlooptijd

Een openbare Europese aanbestedingsprocedure duurt ongeveer negen maanden. Hieraan vooraf gaat een evaluatie (lessons learned) en het formuleren van eventuele aanvullende eisen. Met dit in het achterhoofd moet rekening gehouden worden met een totale doorlooptijd van tenminste twaalf maanden.

Ook moet worden bekeken wat het eventueel combineren van een Europese aanbesteding voor de continuering van OSV2020 en voor nieuw te ontwikkelen verkiezingssoftware betekent voor de doorlooptijd en intensiteit voor het bureau van de Kiesraad.

iii. Wat betekent dit voor gebruikers/afnemers

Een nieuwe aanbesteding betekent dat de gebruikers langer met de huidige software dienen te blijven werken. Dit vraagt zorgvuldige communicatie aan gebruikers.

Bij de nieuwe aanbesteding dienen gebruikers goed te worden betrokken (functionaliteit, gebruikersoverleg, klankbordgroep).

6. Uitwerking: modulair ontwikkelen verkiezingssoftware

In een bijlage bij deze notitie is een gedetailleerdere uitwerking gegeven van de beoogde opzet, indien de Kiesraad kiest voor het modulair ontwikkelen van verkiezingssoftware.

i. Wat betekent dit voor de Kiesraad

De implicaties voor de Kiesraad zijn gedeeltelijk vergelijkbaar met de optie voor het aanbesteden van nieuwe verkiezingssoftware. Het zwaartepunt ligt in eerste instantie bij het begeleiden van de procedure. Daarna ligt het zwaartepunt in het begeleiden van de (door)ontwikkelingen bij de business analisten.

Het, bij modulair ontwikkelen, opknippen van de functionaliteit van de nieuwe verkiezingssoftware vraagt meer afstemming tussen deelprojecten onderling. Dit is van belang om te zorgen dat de gewenste functionaliteit op elkaar aan (blijft) sluiten.

Eén van de uitgangspunten bij het modulair ontwikkelen, is dat tussentijds makkelijker kan worden bijgestuurd en prioriteiten kunnen worden verschoven. Dit vraagt wel intensievere afstemming met gebruikers en naadloze aansluiting op (toekomstige) wetswijzigingstrajecten. Het vraagt van het team I&I om (nog) meer de afdelingen JKA en RKV bij dit traject te betrekken, en de doorontwikkeling van ondersteunende software voor het verkiezingsproces als integraal Kiesraad project aan te pakken.

ii. Wat hebben we hiervoor nodig

Lessons learned

Ook in de optie modulair ontwikkelen willen we de lessons learned meenemen, zoals bovenstaand bij de optie Europees aanbesteden beschreven.

Deels aanbesteden, deels zelf ontwikkelen

Voor onderdelen die we aanbesteden is extra aandacht nodig in hoe de aanbesteding op te zetten. Het moet voor marktpartijen aantrekkelijk zijn om op kleinere onderdelen in te schrijven. Voor het goed uitvragen van deze aanbesteding(en) hebben we expertise nodig van een partij die ervaring heeft met dergelijke trajecten.

Voor het overige zijn de punten genoemd bij de onderdelen continuering gebruik OSV2020 en Europees aanbesteden nieuwe verkiezingssoftware relevant.

Voor onderdelen die relatief klein zijn, en/of onderdelen waar een beperkt onderhoudscontract (of andere vorm van dienstverlening) bij hoort, is het wellicht nodig om hiervoor zelf een grotere rol in te nemen en een andere vorm te kiezen. Idee hierbij is dat een aantal software ontwikkelaars hiervoor tijdelijk wordt aangetrokken om de ontwikkeling te realiseren. Dit dient dan door de Kiesraad te worden begeleid. Voordeel hiervan is dat de Kiesraad zelf nauwer betrokken is en dichter op het resultaat kan (bij)sturen. Nadeel is dat dit een aansturing van de Kiesraad vraagt

die we op dit moment niet kunnen bieden: naast het team van software ontwikkelaars vraagt dit het aantrekken van tijdelijke extra expertise op dit terrein.

System integrator

Een ander voordeel van een modulaire aanpak, is dat de Kiesraad ook per module een partij kan selecteren voor de ontwikkeling (en beheer) die voor dat specifieke onderdeel de vereiste expertise biedt. Zo kan de Kiesraad voor een digitaal platform verkiezingen (distributie software/informatie/data etc. tussen ketenpartners in de verkiezingsketen) een partij aan zich binden die hier ervaring mee heeft, voor een vernieuwde KS-module een partij die ervaring heeft met webapplicaties met een DigiD-koppeling en voor het (door)ontwikkelen van de module voor uitslagvaststelling een partij die ervaring heeft met verkiezingssoftware. Hierbij is de Kiesraad dan system integrator.

iii. Wat betekent dit voor gebruikers/afnemers

Doordat we in dit scenario uitgaan van kleinere projecten, die gelijk bruikbare functionaliteit opleveren, zal de gebruiker sneller resultaat zien en verbeteringen ervaren.

Tevens is het idee de gebruikers nadrukkelijk te betrekken bij de opzet, invulling en prioritering van de deelprojecten. Dit past bij de meer agile werkwijze die we in dit geval kunnen volgen.

7. Planning

In bijlage 3 geven we een eerste inzicht in de stappen en doorlooptijd van de twee routes.

8. Middelen

Het bureau van de Kiesraad heeft niet de expertise in huis om aanbestedingen te begeleiden. Ook heeft het bureau van de Kiesraad niet de expertise in huis om zelfstandig verkiezingssoftware te bouwen/ontwikkelen. Op beide aspecten (aanbesteding en bouw/implementatie) is externe expertise nodig. Per scenario is een eerste inzicht uitgewerkt van de benodigde externe expertise.

Dekking van de benodigde tijdelijke externe middelen kan op een aantal manieren:

- Uit het lopende bestedingsplan
- Bij voorjaarsnotaclaim of bij najaarsnota
- Uit de meerjarige middelen die nu beschikbaar zijn gesteld voor de implementatie van DHV

Dit bekijken we bij nadere uitwerking en vraagt overleg met collega's van BZK en Financiën.

Bijlage 1: Modulair ontwikkelen

Lessen en uitgangspunten

Uit de aanbesteding, gunning en huidige staat van de realisatie van DHV is een aantal globale lessen door de Kiesraad getrokken, die we nadrukkelijk mee willen nemen in een alternatief vervolgtraject:

1. De **complexiteit van DHV** maakt een realisatietraject (a) moeilijk planbaar en (b) moeilijk uitvoerbaar.
2. Het werken met **beperkte flexibiliteit in oplevertermijnen** maakt het lastig om met de leverancier tot een flexibele vorm van samenwerking te komen, en vasthouden aan fatale termijnen legt bij tijdsdruk ook druk op de geleverde kwaliteit;
3. Een **watervalaanpak** werkt suboptimaal:
 - a. Er is nu veel tijd gaan zitten – en deze fase loopt feitelijk nog steeds – in het doorvertalen van de eisen van de Kiesraad in een functioneel ontwerp;
 - b. Er gaat veel tijd en moeite zitten in het reviewen van documentatie;
 - c. Vaste oplevermomenten waarbij in één keer een gehele werkende applicatie met alle functionaliteiten wordt opgeleverd zorgt ervoor dat bij opgelopen vertraging (zoals bij DHV gebeurd in het vaststellen van de functionele specificaties) de kwaliteit van de levering onder druk komt te staan;
 - d. Er is weinig flexibiliteit en capaciteit om in te kunnen springen op wijzigingen in het ontwerp, zoals die bijvoorbeeld uit (concept) wetswijzigingen komen, of voortschrijdende inzichten/wensen vanuit de Kiesraad;
 - e. Het staat een iteratieve manier (meer ‘agile’) van samenwerken in de weg, waarbij we in korte iteratieve increments bestaande werkende code verbeteren, en we als klant/behoeftesteller nauw betrokken zijn bij de ontwikkeling.

Naast bovenstaande lessen ten aanzien van het proces, is er ook een aantal meer inhoudelijke punten waarop we het huidige ontwerp van DHV opnieuw tegen het licht zouden moeten houden:

1. **Terugvaloptie.** Omdat DHV een centrale (web)applicatie is, is het daarbij ook een *single point of failure*. Er moet een alternatief beschikbaar zijn voor het geval DHV niet beschikbaar is (bijvoorbeeld door een hackaanval op de infrastructuur van de (web)applicatie, of het wegvallen van de vereiste connectiviteit bij een gemeente). In de aanbesteding van DHV is deze decentrale terugvaloptie onvoldoende gespecificeerd;
2. **Digitale handtekeningen.** Één van de sterke punten van DHV is dat sterke authenticatie (MFA) vereist is voor iedereen. Tevens worden (tussen)resultaten digitaal ondertekend. Voor deze laatste stap is eHerkenning voorzien in het ontwerp van DHV. Inzet van een eIDAS lijkt wellicht beter aan te sluiten bij de behoefte, en meer toekomstbestendig te zijn.
3. **Beschikbaarheid.** DHV wordt via Diginetwerk ontsloten naar de gebruikers toe bij het proces van tellen en uitslagvaststelling. Sinds het ontwerp van DHV, zorgt (a) de invoer van centrale stemopname en (b) het feit dat invoer van stemlokaaluitslagen in de ondersteunende software onderdeel moet zijn van de openbare zitting van het GSB voor praktische uitdagingen. Grote gemeentes hebben nu vaak zitting van het GSB op locatie (zoals sportzalen of conferentielocaties). Op deze plekken is geen Diginetwerk aanwezig, dit realiseren is voor veel gemeentes moeilijk binnen hun huidige invulling van de ICT-afdeling. Daarnaast zijn ook de (meeste) waterschappen niet op Diginetwerk aangesloten.
4. **Beveiliging.** Beveiligingsoverwegingen zijn één van de belangrijkste overwegingen geweest om over te gaan tot een volledig gecentraliseerde oplossing. Bij OSV2020 is er geen zicht op

wat er op de systemen gebeurt die ingezet worden voor OSV2020. Er is geen logging wie wat doet, en geen zicht op of een systeem mogelijk gecompromitteerd is. Dit is anders in het DHV ontwerp. Paradoxaal gezien is het decentrale karakter van OSV2020 juist een beveiligingskracht. Het wordt voor een aanvaller moeilijker gemaakt om via een aanval op de software de uitslag te beïnvloeden. Om dit te bewerkstelligen moeten meerdere gemeentes aangevallen worden. Bovendien publiceren gemeentes lokaal (op de eigen website) hun eigen lokale uitslagen. Mocht een digitale aanvaller verderop in de verkiezingsketen zitten (HSB/CSB), dan kan een aanpassing van de telresultaten opgemerkt worden, omdat er discrepantie zal zijn tussen de lokale uitslag en de centrale uitslag. Bij een alternatief traject willen we goed kijken hoe we de sterke beveiligingswaarborgen van een decentrale opzet kunnen behouden, en tegelijkertijd de beveiligingsbeperkingen zoals bij het concept van OSV2020 vastgesteld aan pakken.

5. **Onafhankelijk papieren spoor.** Een sterke waarborg (controleerbaarheid) in het beheersen van de risico's van de inzet van software bij het optellen en de uitslagvaststelling is het separate papieren spoor van stembiljetten en de processen-verbaal zoals bij telling van de stemmen op stemlokaalniveau. Doordat de processen-verbaal lokaal (op de website van de gemeenten) worden gepubliceerd, is dit een onafhankelijk kanaal om fouten/aanvallen op de software te kunnen detecteren (zoals ook in het punt hierboven genoemd). De software is altijd ondersteunend en het papieren spoor is leidend. Doordat DHV zowel de module voor uitslagvaststelling als het platform waarop processen-verbaal wordt gepubliceerd omvat, is de scheiding tussen software en processen-verbaal minder sterk, en daarmee de waarborgen die aan deze scheiding kan worden toegekend.

Naast de geleerde lessen uit de aanbesteding, gunning en gedeeltelijk realisatie van DHV, is het ook van belang de uitgangspunten van de ontwikkeling van DHV mee te nemen. Doel van DHV was voornamelijk om een aantal verbeterpunten van de huidige (inzet van) OSV2020 op te pakken, en deze doelen moeten we ook bij een alternatief traject voor ogen houden:

1. **Moderniseren code.** De codebase van OSV2020 is groot en complex. Idealiter is de code kleiner (bijvoorbeeld zonder onnodige code die alleen bij verkiezingen in Duitsland wordt gebruikt) en beter modulair opgezet;
2. **Distributie OSV2020 via Dvd's afschaffen.** De software voor OSV2020 wordt nu per DVD verspreid en vanaf DVD geïnstalleerd. Dit om de integriteit van de software zo goed mogelijk te kunnen waarborgen. In de toekomst willen we toewerken naar een situatie waarbij, net als bij DHV, er geen software meer per Dvd wordt verspreid;
3. **Overdracht digitale telbestanden en certificaten van GSB->(HSB->)CSB verbeteren.** Bij verkiezingen met meerder lagen, moeten de digitale telbestanden worden overgebracht naar het bovenliggend niveau. Hiervoor worden nu twee verschillende digitale uitwisselingsplatformen ingericht (één door de Kiesraad voor de certificaten, één door de VNG voor de digitale telbestanden). Dit is een omslachtig en foutgevoelig proces.
4. **Proces ondertekening telbestanden verbeteren.** Op dit moment wordt het sleutelmateriaal bij installatie van OSV2020 bij de gebruikers gegenereerd, die het bijbehorende certificaat moeten uploaden naar het bovenliggend verkiezingsorgaan, zodat die het kan gebruiken bij de validatie van het digitale telbestand. Het liefst zouden we hier gebruik maken van een kleine PKI, waarbij we de uitvoerende partijen niet belasten met het genereren en distribueren van certificaten, maar dat wij deze distributie organiseren;
5. **Verbeteren gebruiksvriendelijkheid (UI/UX).** De userinterface van OSV2020 is ouderwets en soms onduidelijk. Bij nieuwe ondersteunende software moet dit beter en duidelijker.

6. **Moderniseren instructiemateriaal.** Het instructiemateriaal voor OSV2020 wordt met de beste intenties gemaakt door de producent, maar verdient een doorontwikkeling om professioneler over te komen en (vooral) de gebruikers beter te ondersteunen.
7. **Vereenvoudigen datamodellen.** De datamodellen en dataformaten die binnen OSV2020 worden gebruikt zijn complex, vooral omdat er zowel Nederlandse als Duitse modellen en formaten door elkaar heen gebruikt worden.
8. **Verbeteren zicht op gebruikers systemen.** Op dit moment is er onvoldoende zicht in de uitvoering op wie wat doet, en geen monitoring op de (beveiliging)staat van het systeem. We zouden graag meer controle/zekerheid willen hebben over het systeem waarop de ondersteunende software wordt geïnstalleerd, en kunnen herleiden wie welke acties op het systeem heeft uitgevoerd tijdens gebruik van de ondersteunende software

Om de bovenstaande verbeteringen door te voeren, kunnen we het grote DHV project opknippen in kleinere deelprojecten. Hierbij is het doel dat:

- a) De individuele projecten beter behapbaar zijn en een kortere realisatietijd zullen hebben;
- b) Verschillende projecten door verschillende partijen uitgevoerd kunnen worden;
- c) Verschillende projecten simultaan uitgevoerd zouden kunnen worden;
- d) Per project gekeken kan worden welke vorm van ontwikkeling het beste past bij het project en de mogelijkheid binnen de Kiesraad om het project te begeleiden en aan te sturen: inbesteden of aanbesteden;
- e) We altijd beschikken over werkende code, en niet hoeven te wachten tot alles is afgerond.

Voorbeeld

Om een concreter beeld te geven, volgt hier een voorbeeld van opdeling en fasering:

Het opknippen van de verschillende functionaliteiten houdt rekening met de verschillende modules zoals die binnen OSV2020 worden gebruikt. Er zijn zeven deelprojecten:

- I. Consultatie gebruikers over voorgestelde oplossing
- II. Digitaal uitwisselingsplatform, geschikt voor integere uitwisseling software (vanuit KR naar gebruikers), informatie/handleidingen (vanuit KR en BZK naar gebruikers) en bestanden (tussen gebruikers onderling). (Dit maakt de distributie van software met DVD's overbodig, en kan tot deelproject IV gerealiseerd is ingezet worden bij de digitale overdracht van telbestanden.)
- III. Moderniseren module voor politieke groeperingen en de kandidaatstellings-applicatie, conform concept wetgeving en om dit gebruiksvriendelijker te maken;
- IV. Ontwikkelen webapplicatie waar resultaat vanuit GSB, HSB en CSB wordt ingevoerd, en de uitslag en zetelverdeling wordt berekend. (Dit maakt de digitale overdracht tussen GSB/HSB/CSB overbodig.). Dit zou een geheel nieuwe applicatie kunnen zijn, of een doorontwikkeling zijn van het stuk van OSV2020 dat deze functionaliteit nu biedt.
- V. Ontwikkelen applicatie voor invoer uitslagen stembureaus binnen gemeentes. Dit zou een geheel nieuwe applicatie kunnen zijn, of een doorontwikkeling zijn van het stuk van OSV2020 dat deze functionaliteit nu biedt.
- VI. Door ontwikkelen databank (verkiezingsuitslagen.nl) tot centraal uitslagenportaal. Door dit los te doen van de modules IV en V, waarborgen de scheiding tussen de publicatie van proces-verbaal (op stembureau-niveau) en de software die ter ondersteuning wordt gebruikt bij de vaststelling van de uitslag;

- VII. Onderzoeken wenselijkheid/meerwaarde integreren modules. Als de deelprojecten I-VI zijn afgerond, kunnen we kijken of we modules wellicht alsnog meer willen integreren om dichter bij het originele beeld van DHV te komen.

Opmerkingen

Door de applicatie voor invoer na telling stembureaus (V) los te knippen van het doorgeven van het resultaat naar het bovenliggende niveau (IV) bereiken we:

- Er is geen toegang tot de centrale infrastructuur (zoals via Diginetwerk binnen DHV) nodig op zittingslocaties van het GSB (zoals sporthallen of conferentielocaties);
- Doordat invoerders niet op het centrale systeem werken (zoals bij DHV voorzien), is de belasting voor het centrale systeem beter te managen (van circa 4000 piek-gebruikers naar circa 300 piek-gebruikers). Dit kan de oplossing stabielere maken bij gebruik van technologie als VDI/Citrix, en maakt het vanuit security-oogpunt nog beter te monitoren;
- De centrale component uit IV zorgt er ook voor dat er geen digitale overdracht meer nodig is, en er dus geen certificaten hoeven te worden uitgewisseld zoals nu het geval is. Door gebruik te maken van eIDAS (of andere) middelen, kunnen de voorzitters van de betrokken verkiezingsorganen (GSB/HSB/CSB) de uitslagen zoals door hen vastgesteld ondertekenen en kan sterke authenticatie worden gefaciliteerd;
- Deze scheiding maakt het gehele systeem ook robuuster tegen aanvallen op de centrale infrastructuur. Immers, een aanvaller die een GSB onder controle heeft, kan moeilijker via deze toegang de uitslag van andere bureaus beïnvloeden.

Fasering

Een fasering van de verschillende deelprojecten zou er zo uit kunnen zijn:

Deelproject	Fase			
	1	2	3	4
I				
II				
III				
IV				
V				
VI				
VII				

	Kiesraad voert zelf uit
	Inbesteden: inhuren devops team door kiesraad
	Uitbesteden: ontwikkelen door externe partij

**BIJLAGE 2: OVERZICHT ACTIVITEITEN EN VERANTWOORDELIJKHEDEN
AANBESTEDINGSTEAM**

Fase	Functionaris/rol
Algemeen	(Gemandateerd) opdrachtgever
	<p><u>Opdrachtgever</u>: is verantwoordelijk voor de te nemen beslissingen en keurt de in paragraaf 5.2 genoemde documenten goed.</p> <p><u>Gemandateerd opdrachtgever</u>: door de opdrachtgever aangewezen om tijdens de uitvoering van het inkoopproces namens de opdrachtgever beslissingen te nemen en namens opdrachtgever de in paragraaf 5.2 genoemde documenten goed te keuren.</p>
	Projectleider/Inkoopadviseur RIS
	<p>Bewaken dat de aanbestedingsprocedure binnen de planning en correct wordt uitgevoerd.</p> <p>Onder deze 'formele' begeleiding verstaan we onder meer:</p> <ul style="list-style-type: none"> - het voorzitten van de overleggen van het projectteam; - het afstemmen en akkoord vragen bij de opdrachtgever; - de aanwezigheid bij eventuele toelichtingsgesprekken met (afgewezen) inschrijvers.
	senior Inkoopadviseur
	<ul style="list-style-type: none"> - Bewaken en uitvoeren van de Europese aanbestedingsprocedure - Zorgdragen dat de procedure wordt uitgevoerd in overeenstemming met interne richtlijnen, nationale wet- en/of regelgeving en de Europese Richtlijn 2014/24/EU (overheidsopdrachten).
	Projectsecretaris
	<ul style="list-style-type: none"> - het ondersteunen van de <senior> inkoopadviseur bij deze Europese aanbesteding; - het bewaken van de planning; - het up-to-date houden en samenstellen van een volledig Europees aanbestedingsdossier; - monitoren/bewaken van de documenten.
	Reviewer
	<p>Uitvoeren van een review op alle in paragraaf 5.3.3 genoemde documenten. De reviewer brengt een advies uit aan de <senior> inkoopadviseur over het betreffende document.</p>

	<p>Juridisch adviseur RIS</p> <p>De inzet van een juridisch adviseur RIS in het proces is in ieder geval verplicht:</p> <ul style="list-style-type: none"> - bij een complexe/risicovolle aanbesteding; - bij het niet toepassen van de van kracht zijnde algemene Rijksvoorwaarden en er sprake is van een (zelfdragende) maatwerkovereenkomst; - bij toepassing van één van de uitzonderingsgronden voor Europees aanbesteden in de Aanbestedingswet 2012; - bij een kort geding procedure. <p>De senior inkoopadviseur en de reviewer beoordeelt verder zelf de inzet van een juridisch adviseur in het proces.</p>
	<p>Projectteamlid/materiedeskundige</p> <p>Levert een bijdrage aan het project door:</p> <ul style="list-style-type: none"> - deelname aan de vergaderingen van het projectteam; - inhoudelijke input te leveren aan de aanbestedingsdocumenten vanuit materiedeskundigheid.
	<p>Contractmanager</p> <ul style="list-style-type: none"> - het leveren van tekst over contractmanagementaspecten voor het beschrijvend document en programma van eisen. - het meedenken en input leveren voor formulering van geschikte (sub)gunningscriteria, social return verplichtingen en andere MVOI aspecten. - de review van de concept overeenkomst voor duidelijkheid en compleetheid tijdens de uitvoering.
	<p>Deskundige</p> <p>De projectleider of de <senior> inkoopadviseur schakelt indien nodig deskundigen in op het gebied van financiën, ICT, HRM, MVOI.</p>
Vorbereidingsfase	<p>senior Inkoopadviseur</p> <ul style="list-style-type: none"> - het opstellen van het projectplan; - het samenstellen van het beschrijvend document inclusief bijlagen; - het adviseren over de effecten van geschiktheidseisen en de (sub)gunningscriteria; - het toetsen van het beschrijvend document op de Aanbestedingswet 2012 en de Gids proportionaliteit 2020, respectievelijk de Europese Richtlijn 2014/24/EU (overheidsopdrachten);

	<ul style="list-style-type: none"> - de correspondentie met en informatie verstrekken aan de (potentiële) inschrijvers in de digitale applicatie (CTM Solution); - het opstellen van de voortgangsnoties (keys update); - het beantwoorden van vragen van de (potentiële) inschrijvers van algemene en procedurele aard en het samenstellen van de nota('s) van inlichtingen; - het opstellen van de beoordelingsdocumenten.
--	--

	<p>Projectsecretaris</p> <ul style="list-style-type: none"> - toetsen van de planning van de Europese aanbesteding op de Aanbestedingswet 2012, de Gids proportionaliteit 2016 en de Europese Richtlijn 2014/24/EU (overheidsopdrachten); - het verzorgen van de projectcommunicatie; - de correspondentie met en informatie verstrekken aan de (potentiële) inschrijvers in de digitale applicatie (CTM Solution); - het samenstellen van de juiste bijlagen uit het definitieve beschrijvend document; - het bewaken van de voortgang van de nota('s) van inlichtingen; - de publicatie van het beschrijvend document (inclusief bijlagen) op CTM Solution gereed zetten (inhoudelijk vullen) en publiceren.
	<p>Projectteamlid/ materiedeskundige</p> <ul style="list-style-type: none"> - het opstellen van het programma van eisen en wensen (is onderdeel van één van de bijlagen bij het beschrijvend document); - het leveren van input voor de (sub)gunningscriteria; - het beantwoorden van de (materie)vragen bij de nota('s) van inlichtingen.
	<p>Contractmanager</p> <ul style="list-style-type: none"> - het leveren van tekst over contractmanagementaspecten voor het beschrijvend document en programma van eisen - het meedenken en input leveren voor formulering van geschikte (sub)gunningscriteria, social return verplichtingen en andere MVOI aspecten. - de review van de concept overeenkomst voor duidelijkheid en compleetheid tijdens de uitvoering.
Inschrijvingsfase	senior Inkoopadviseur
	<ul style="list-style-type: none"> - het (mede) openen van de digitale aanbiedingskluis (CTM Solution);

	<ul style="list-style-type: none"> - het bewaken van de beoordelingsprocedure; - de beoordeling van de minimumeisen, de geschiktheidseisen (niet zijnde referenties) en de prijs; - het samenvoegen van de scores van het beoordelingsteam; - aanwezigheid bij de plenaire beoordelingsbijeenkomst.
	Projectsecretaris
	<ul style="list-style-type: none"> - het (mede) openen van de digitale aanbiedingskluis (CTM Solution); - het versturen van het proces-verbaal van inschrijving; - de beoordeling van de minimumeisen en de geschiktheidseisen (niet zijnde referenties) en de prijs; - het checken en verzamelen van de ingevulde beoordelingsformulieren van de beoordelaars; - het plannen van de gezamenlijke beoordelingsbijeenkomst, zorgen voor eventuele verslaglegging (niet zijnde deugdelijke motivering van de brieven).
	Beoordelaar
	<ul style="list-style-type: none"> - het beoordelen van de inschrijvingen en hierbij een correcte en volledige (deugdelijk gemotiveerd) onderbouwing geven; - aanwezigheid bij de plenaire beoordelingsbijeenkomst; - aanwezigheid bij eventuele toelichtingsgesprekken met (afgewezen) inschrijver(s).
Gunningsfase	senior Inkoopadviseur
	<ul style="list-style-type: none"> - het opstellen van het proces-verbaal van opdrachtverlening; - het opstellen van het format voor de brieven m.b.t. de gunningsbeslissing (afwijzing en gunning); - de aanwezigheid bij eventuele toelichtingsgesprekken met (afgewezen) inschrijver(s); - de verificatie van de gegevens van het Uniform Europees Aanbestedingsdocument van de voorlopig gegunde partij.
	Projectsecretaris
	<ul style="list-style-type: none"> - de brieven m.b.t. de gunningsbeslissing (afwijzing en gunning) voor publicatie op CTM Solution; - het plannen van eventuele toelichtingsgesprekken van afgewezen inschrijver(s);

	<ul style="list-style-type: none"> - de verificatie van de gegevens aangaande het Uniform Europees Aanbestedingsdocument van de voorlopig gegunde partij, - het bespreken van de bevindingen met de senior inkoopadviseur en zo nodig aanvullende informatie opvragen.
	<p>Beoordelaar</p> <ul style="list-style-type: none"> - het leveren van de inhoudelijke input voor het proces-verbaal van opdrachtverlening en een de deugdelijke motivering van de brieven m.b.t. de gunningsbeslissing (afwijzing en gunning).
Nazorgfase	senior Inkoopadviseur
	<ul style="list-style-type: none"> - het opstellen van de definitieve overeenkomst; - het sturen van de evaluatieformulieren naar de afgewezen inschrijvers; - het controleren van het dossier op volledigheid, inclusief de checklist invullen; - het invullen van de MVI-Zelfevaluatie Tool van PIANOo.
	<p>Projectsecretaris</p> <ul style="list-style-type: none"> - het gereed zetten van de definitieve overeenkomst en het bewaken van het ondertekeningproces; - het plannen van het evaluatiegesprek en monitoren dat de afgewezen evaluatieformulieren worden ingevuld, eventueel verslaglegging; - het controleren van het dossier op volledigheid, inclusief de checklist invullen; - het controleren van de MVI-Zelfevaluatie Tool van PIANOo; - het overdragen van de meervoudig ondertekende en geparafeerde overeenkomst aan de afdeling Contractbeheer van de RIS; - het zorgdragen voor de aankondiging van gegunde opdracht (afkondiging) in CTM Solution (en TED); - het opslaan van het dossier op de juiste plek op de G-schijf (afroning).
	<p>Projectteamlid/ materiedeskundige</p> <ul style="list-style-type: none"> - het zorgen voor afstemming met de achterban binnen de eigen organisatie alsmede de implementatie of het intakegesprek aangaande de overeenkomst.

Bijlage 3: Globale planning vervolg scenario's

Vervolg Scenario's DHV	2023								2024					2025				2026				
	Q2	Q3		Q4		Q1	Q2	Q3		Q4	Vr	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4			
	1-mei	1-jun	1-jul	1-aug	1-sep	1-okt	1-nov	1-dec	1-jan	1-mrt	1-aug	1-sep	1-okt	1-nov	1-dec	13-jul				1-jan	1-nov	
Huidige OSV 2020																						
Beheer & Onderhoud																						
Lessons Learned project DHV																						
Intern & Extern																						
Continuering OSV 2020																						
Onderzoek Requirements																						
Europese Aanbesteding																						
Doorontwikkeling																						
Europese Aanbesteding DHV																						
Aanscherpen Requirements																						
Aanbesteding																						
Ontwikkeling																						
Modulair Ontwikkelen DHV																						
Aanscherpen Requirements																						
Selectie ontwikkelpartij																						
a) Raamovereenkomst																						
Ontwikkelen																						
Selectie ontwikkelpartij																						
b) Aanbesteden																						
Ontwikkelen																						

PELS RIJCKEN

Landsadvocaat

Notitie

voor Kiesraad
van 5.1.2.e en 5.1.2.e
datum 23 februari 2023
inzake Beëindiging van de Overeenkomst Digitaal Hulpmiddel Verkiezingen
zaaknr 11019745

Samenvatting

De Kiesraad heeft in 2022 de Overeenkomst gesloten met Paragon. De Kiesraad ervaart bij de uitvoering van die overeenkomst dat Paragon op verschillende vlakken de gemaakte afspraken niet nakomt en dat Paragon aanstuurt op aanpassing van de gemaakte afspraken. Bovendien heeft Paragon aangegeven de overeengekomen oplevertermijn van 11 april 2023 niet te zullen halen.

De Kiesraad overweegt daarom momenteel of hij de Overeenkomst zal beëindigen. In dit advies zijn daartoe de mogelijkheden uiteengezet.

5.2.1 i.c.m. 5.1.2.i

5.2.1 i.c.m. 5.1.2.i

Inleiding

- 1.1 De Staat der Nederlanden, Ministerie van Binnenlandse Zaken en Koninkrijkrelaties, de Kiesraad (hierna: de Kiesraad) heeft op 13 mei 2022 met Paragon Communicatie Services B.V. (hierna: Paragon) de Overeenkomst Digitaal Hulpmiddel Verkiezen gesloten (hierna: de Overeenkomst). Op grond van de Overeenkomst dient Paragon software te leveren en vervolgens beschikbaar te stellen die de Kiesraad kan inzetten ter ondersteuning van het verkiezingsproces.
- 1.2 De Overeenkomst gaat uit van een oplevering van de door Paragon te realiseren oplossing per 1 maart 2023. Kort na het sluiten van de Overeenkomst hebben Partijen een afwijkende afspraak gemaakt die uitgaat van een gefaseerde oplossing van de verschillende delen van de oplossing. Op basis van die planning dienen de onderdelen herindelings- gemeenteraad- en Europees parlamentsverkiezing per 11 april 2023 te worden opgeleverd. Nadien volgen opleveringen per 21 juni 2023 en 13 september 2023.
- 1.3 Tijdens de uitvoering van de Overeenkomst ervaart de Kiesraad dat Paragon op verschillende vlakken de gemaakte afspraken niet nakomt en dat Paragon aanstuurt op aanpassing van de gemaakte afspraken. Bovendien heeft (een medewerker van) Paragon tijdens de stuurgroepvergaderingen van 17 januari 2023 en 24 januari 2023 aangegeven dat Paragon op 11 april 2023 de onderdelen herindelings- gemeenteraad- en Europees parlamentsverkiezing niet volledig zal opleveren.
- 1.4 In dat licht heeft de Kiesraad ons de volgende drie vragen gesteld:
 1. Op welke manier en op welke gronden kan de Overeenkomst met Paragon voortijdig worden beëindigd?
 2. Op welke manier kan de Kiesraad zoveel mogelijk geld van de reeds betaalde voorschotfacturen terugvorderen?
 3. Kan de Kiesraad betaling van de voorschotfactuur van maart 2023 opschorten?
- 1.5 In het eerst deel van dit advies hebben wij deze vragen beantwoord (hoofdstuk 2 – 4). In het tweede deel van dit advies hebben wij verschillende vervolgsenario's geschetst (hoofdstuk 5).

2 Beantwoording vraag 1: Op welke manier en op welke gronden kan de Overeenkomst voortijdig worden beëindigd?

Onderscheid opzegging en ontbinding

- 2.1 De wet onderscheidt twee manieren waarop een overeenkomst voortijdig kan worden beëindigd: door opzegging of ontbinding.
- 2.2 Voor het opzeggen van een overeenkomst is geen tekortkoming vereist. In het geval van een rechtsgeldige opzegging eindigt de overeenkomst op de datum waartegen de opzegging plaatsvindt. Dat betekent dat in beginsel alle prestaties die voorafgaand aan die datum verricht zijn hun waarde behouden. Afhankelijk van de gemaakte afspraken (zie daarover hierna onder 2.7 e.v.) zal de partij die tot opzegging overgaat de gemaakte kosten en geleden schade van de andere partij moeten vergoeden.
- 2.3 Ontbinding is in beginsel alleen mogelijk indien sprake is van een tekortkoming in de nakoming van de overeenkomst en er bovendien sprake is van verzuim (zie daarover hierna onder 2.11 e.v.). Anders dan bij opzegging, worden partijen als gevolg van een ontbinding verplicht alle prestaties die zijn verricht op grond van een ontbonden overeenkomst ongedaan te maken, hetgeen dus ook kan resulteren in terugbetalingen. Daarnaast is de partij die tekort is geschoten in de nakoming van een ontbonden overeenkomst ten opzichte van de wederpartij gehouden tot schadevergoeding.
- 2.4 In de volgende paragrafen beschrijven wij de mogelijkheden tot opzegging en ontbinding waar de Kiesraad in het onderhavige geval (mogelijk) een beroep op kan doen.

Opzegging van de Overeenkomst op grond van artikel 4.5 van de Overeenkomst

- 2.5 Op grond van artikel 4.5 van de Overeenkomst heeft de Kiesraad te allen tijde het recht om tot opzegging van de Overeenkomst over te gaan. 5.2.1 i.c.m. 5.1.2.i

5.2.1 i.c.m. 5.1.2.i

- 2.6 Opzegging op grond van artikel 4.5 van de Overeenkomst (eventueel in combinatie met artikel 30.6 van de ARBIT-2018) 5.2.1 i.c.m. 5.1.2.i

5.2.1 i.c.m. 5.1.2.i

¹ Opzegging kan wel naar maatstaven van redelijkheid en billijkheid onaanvaardbaar zijn, maar dat is niet snel aan de orde.

2.7 5.2.1 i.c.m. 5.1.2.i

2.8 5.2.1 i.c.m. 5.1.2.i

Ontbinding van de Overeenkomst

- Ingebrekestelling vormt het uitgangspunt

2.9 Tenzij nakoming tijdelijk of blijvend onmogelijk is, kan ontbinding alleen plaatsvinden indien de wederpartij in verzuim verkeert. Verzuim ontstaat in beginsel pas nadat de wederpartij in gebreke is gesteld en ook niet heeft gepresteerd binnen de in de ingebrekestelling gestelde redelijke termijn voor nakoming.

2.10 Aan ingebrekestelling wordt pas toegekomen indien een prestatie opeisbaar is. Voor die tijd is immers nog geen sprake van een tekortkoming, zodat de wederpartij ook niet een tweede gelegenheid kan worden geboden om te presteren.

2.11 5.2.1 i.c.m. 5.1.2.i

2.12 5.2.1 i.c.m. 5.1.2.i

2.13 5.2.1 i.c.m. 5.1.2.i

2.14

5.2.1 i.c.m. 5.1.2.i

2.15

5.2.1 i.c.m. 5.1.2.i

- Ontbinding voordat prestatie opeisbaar is

2.16

In afwijking van het uitgangspunt dat pas tot ontbinding kan worden overgegaan nadat een prestatie opeisbaar is geworden, bepaalt de wet dat de gevolgen van niet-nakoming reeds intreden:

- a. indien de schuldeiser uit een mededeling van de schuldenaar moet afleiden dat deze in de nakoming zal tekortschieten (artikel 6:80 lid 1 aanhef en sub b BW); of
- b. indien de schuldeiser goede gronden heeft te vrezen dat de schuldenaar in de nakoming zal tekortschieten en deze niet voldoet aan een schriftelijke aanmaning met opgave van die gronden om zich binnen een bij die aanmaning gestelde redelijke termijn bereid te verklaren zijn verplichtingen na te komen (artikel 6:80 lid 1 aanhef en sub c BW).

2.17

5.2.1 i.c.m. 5.1.2.i

5.2.1 i.c.m. 5.1.2.i

5.1.2.e

5.2.1.c.m. 5.1.2.i

5.2.1 i.c.m. 5.1.2.i
5.1.2.e

2.18

5.2.1 i.c.m. 5.1.2.i

2.19

5.2.1 i.c.m. 5.1.2.i

5.1.2.e

5.2.1 i.c.m. 5.1.2.i

2.20

5.2.1 i.c.m. 5.1.2.i

2.21

5.2.1 i.c.m. 5.1.2.i

- Niet-halen fatale termijn van 11 april 2023

2.22 In uitzondering op de hoofdregel dat verzuim pas ontstaat nadat een prestatie opeisbaar is geworden en ingebrekestelling heeft plaatsgevonden, geldt dat in het

geval dat een partij binnen een fatale termijn niet presteert, verzuim zonder ingebrekestelling ontstaat en de wederpartij in beginsel direct tot ontbinding kan overgaan.² Op grond van de ARBIT-2018 gelden als fatale termijn uitsluitend termijnen die als zodanig zijn aangeduid.

2.23

5.2.1 i.c.m. 5.1.2.i



5.2.1 i.c.m. 5.1.2.i



2.24

5.2.1 i.c.m. 5.1.2.i



2.25

5.2.1 i.c.m. 5.1.2.i



2.26

Indien er sprake is van een levering die niet aan de overeengekomen voorwaarden voldoet, dan zal eerst de acceptatieprocedure van artikel 11 en artikel 59 ARBIT-2018 moeten worden doorlopen, voordat tot ontbinding kan worden overgegaan (zie hierna).

2.27

5.2.1 i.c.m. 5.1.2.i



² Waarbij opnieuw geldt dat wel zal moeten worden vastgesteld dat de tekortkoming ontbinding ook rechtvaardigt.

5.2.1 i.c.m. 5.1.2.i

2.28

5.2.1 i.c.m. 5.1.2.i

- 5.2.1 i.c.m. 5.1.2.i

2.29

5.2.1 i.c.m. 5.1.2.i

2.30

5.2.1 i.c.m. 5.1.2.i

5.2.1 i.c.m. 5.1.2.i

- Contractuele ontbindingsregeling van artikel 4.4

2.31 Artikel 4.4 bevat een afzonderlijke bepaling die ziet op het ontbinden van de Overeenkomst. 5.2.1 i.c.m. 5.1.2.i

5.2.1 i.c.m. 5.1.2.i

- Risico van ontbinding

2.32 De ontbinding van een overeenkomst is risicovoller dan de opzegging van een overeenkomst. Komt namelijk achteraf vast te staan dat een partij ten onrechte tot

ontbinding is overgegaan, dan is daarmee gegeven dat *de ontbindende partij* tekort is geschoten in de nakoming van de overeenkomst en daarmee aansprakelijk is voor de schade die de wederpartij door de ontbinding heeft geleden (vaak: misgelopen winst, voor zover de overeengekomen exonerationen vergoeding daarvan mogelijk maken).

2.33 Daarbij speelt een rol dat een partij niet tot ontbinding kan overgaan indien de ontbindende partij zelf (een deel van) de gemaakte afspraken niet is nagekomen en daardoor in schuldeisersverzuim verkeert. Zeker in IT-projecten als het onderhavige ontstaat daardoor na ontbinding vaak een debat over de vraag of de ontbindende partij zelf wel alle onderdelen van de gesloten overeenkomst is nagekomen. Gezien de vaak zeer feitelijke gang van zaken van een IT-project is het in de regel nog niet zo eenvoudig om dat vast te stellen.

2.34 5.2.1 i.c.m. 5.1.2.i

5.2.1 i.c.m. 5.1.2.i 5.1.2.e

5.2.2 e.c.m. 5.1.2.i

5.2.1 i.c.m. 5.1.2.i

5.2.1 i.c.m. 5.1.2.i

5.2.1 i.c.m. 5.1.2.i

5.2.1 i.c.m. 5.1.2.i

2.35 5.2.1 i.c.m. 5.1.2.i

5.2.1 i.c.m. 5.1.2.i

5.2.1 i.c.m. 5.1.2.i

2.36

5.2.1 i.c.m. 5.1.2.i

3 Beantwoording vraag 2: Op welke manier kan de Kiesraad zoveel mogelijk geld van de reeds betaalde voorschotfacturen terugvorderen?

3.1

5.2.1 i.c.m. 5.1.2.i

3.2

5.2.1 i.c.m. 5.1.2.i

3.3

5.2.1 i.c.m. 5.1.2.i

4 Beantwoording vraag 3: Kan de Kiesraad betaling van de voorschotfactuur van maart 2023 opschorten?

4.1 De gronden zoals die bij de beantwoording van vraag 1 aan de orde zijn gekomen, kunnen ook grond vormen voor opschorting van de betalingsverplichting van maart 2023, waarbij zij opgemerkt dat in algemene zin voor het opschorten van een verplichting een lagere drempel bestaat dan voor ontbinding van een overeenkomst.

4.2 In de eerste plaats geldt dat het niet-nakomen van een verplichting grond kan vormen voor de opschorting van een betalingsverplichting (artikel 2:262 BW).^{5.2.1}

5.2.1

5.2.1 [Redacted]

4.3 In de tweede plaats geldt dat in het geval een schuldeiser goede gronden heeft te vrezen dat de wederpartij een toekomstige prestatie niet zal nakomen, de schuldeiser ook tot opschorting van zijn prestatie over mag gaan (artikel 6:263 BW). ^{5.2.1} [Redacted]

5 Hoe verder?

5.1 Bij de beantwoording van de vragen van de Kiesraad hebben wij getracht de verschillende mogelijkheden die de Kiesraad heeft in beeld te brengen. Wij hebben die mogelijkheden vertaald naar vijf scenario's, die met elkaar gecombineerd zouden kunnen worden.

5.2.1 i.c.m. 5.1.2.i [Redacted]

5.2 5.2.1 i.c.m. 5.1.2.i [Redacted]

5.3 5.2.1 i.c.m. 5.1.2.i [Redacted]

5.4 5.2.1 i.c.m. 5.1.2.i [Redacted]

5.5 5.2.1 i.c.m. 5.1.2.i [Redacted]

5.2.1 i.c.m. 5.1.2.i

5.6 5.2.1 i.c.m. 5.1.2.i

5.7 5.2.1 i.c.m. 5.1.2.i

5.8 5.2.1 i.c.m. 5.1.2.i

5.2.1 i.c.m. 5.1.2.i

5.9 5.2.1 i.c.m. 5.1.2.i

5.10 5.2.1 i.c.m. 5.1.2.i

5.11 5.2.1 i.c.m. 5.1.2.i



5.12 5.2.1 i.c.m. 5.1.2.i

5.13 5.2.1 i.c.m. 5.1.2.i

5.14 5.2.1 i.c.m. 5.1.2.i

5.2.1 i.c.m. 5.1.2.i

5.15 5.2.1 i.c.m. 5.1.2.i

5.16 5.2.1 i.c.m. 5.1.2.i

5.17 5.2.1 i.c.m. 5.1.2.i

5.2.1 i.c.m. 5.1.2.i

5.18 5.2.1 i.c.m. 5.1.2.i

5.19 5.2.1 i.c.m. 5.1.2.i

5.2.1 i.c.m. 5.1.2.i

5.20

5.2.1 i.c.m. 5.1.2.i

6

5.2.1 i.c.m. 5.1.2.i

5.2.1 i.c.m. 5.1.2.i

Plan van Aanpak

Digitale hulpmiddelen in de verkiezingsketen

10 september 2019

Vastgesteld in Stuurgroep 4 sept 2019

Aan de Stuurgroep Digitale hulpmiddelen

5.1.2.e

5.1.2.e

BZK

5.1.2.e

5.1.2.e

Kiesraad

5.1.2.e

5.1.2.e

5.1.2.e

ABD Interim
Muzenstraat 97
2511 WB Den Haag

1. Aanleiding

In februari 2019 heeft ABD Topconsult een briefadvies afgerond naar het gebruik van digitale hulpmiddelen in de verkiezingsketen. Aanleiding voor deze verkenning was de discussie die is ontstaan rond het gebruik van digitale hulpmiddelen in het verkiezingsproces. Hierbij kan gedacht worden aan de discussie over de betrouwbaarheid van het elektronisch stemmen en tellen met stemmachines (2007), maar ook rond het gebruik van de Ondersteunende Software Verkiezingen in 2017. Net voor de Tweede Kamerverkiezingen in 2017 verbood de minister de digitale overdracht van bestanden. Naar aanleiding van discussie rond het gebruik van OSV ontstond de noodzaak om nieuwe software voor de uitslagberekening te ontwikkelen. De Kiesraad gaf in 2018 aan dat zij vond dat zij niet de aangewezen partij was om opnieuw het initiatief te nemen voor de ontwikkeling van een hulpmiddel waarmee de uitslag kan worden berekend. Vervolgens is de verkenning, resulterend in het briefadvies, gestart.

Het gebruik van digitale hulpmiddelen wordt door alle bij verkiezingen betrokken partijen noodzakelijk geacht voor een betrouwbare en snelle uitslag van de verkiezingen. Betrouwbaar omdat je zeker wil weten dat alle stemmen goed geteld zijn en de uitslag correct is. Hierbij speelt dat er ook bij handmatig werk fouten worden gemaakt. Bij een verkiezing in Nederland zijn op dit moment 60.000 mensen betrokken die onder hoge tijdsdruk op ongebruikelijke arbeidsuren moeten presteren. Voor een goede uitvoerbaarheid van het verkiezingsproces zijn digitale hulpmiddelen onontbeerlijk. Tegelijkertijd is er een discussie rond de betrouwbaarheid van de hulpmiddelen, zeker in het licht van toegenomen cybersecuritydreigingen en buitenlandse inmenging. Ook internationaal is er grote aandacht rond de betrouwbaarheid van verkiezingen.

De opdracht voor ABD Topconsult was te verkennen op welke wijze de verantwoordelijkheid kan worden belegd voor alle digitale hulpmiddelen in het verkiezingsproces. Gedurende de verkenning is de opdracht afgebakend en beperkt tot digitale hulpmiddelen voor de vaststelling van de uitslag. In het advies wordt onderscheid gemaakt tussen de korte termijn (de transitiefase) en de middellange termijn. Op de middellange termijn (1 tot 1½ jaar) komt de verantwoordelijkheid voor digitale hulpmiddelen te liggen bij de Kiesraad. Verantwoordelijkheden en bevoegdheden voor deze eindsituatie worden verankerd in de Kieswet. In de transitiefase wordt - onder verantwoordelijkheid van de Minister van Binnenlandse Zaken - het programma voor het ontwerp en de ontwikkeling van digitale hulpmiddelen (inclusief aanbesteding) vormgegeven. Ook wordt de benodigde aanpassingen aan wetgeving in gang gezet en wordt in kaart gebracht wat de consequentie is voor de aard, omvang en samenstelling van de eindsituatie voor de Kiesraad. Alle betrokken partijen (BZK, Kiesraad en VNG) hebben ingestemd met de conclusies van deze verkenning.

In dit Plan van Aanpak wordt geschetst hoe de transitiefase vorm wordt gegeven, wat de planning is, wie worden betrokken en wat er benodigd is om tot een succesvolle implementatie over te gaan.

2. Opdracht

De transitie heeft tot doel:

Al het nodige te doen en te regelen (in juridisch, organisatorisch en financieel opzicht) om in de wet- en regelgeving een heldere verantwoordelijkheids- en bevoegdheidsverdeling te verankeren én om de Kiesraad in staat te stellen de nieuwe taken en bevoegdheden ook voor de digitale hulpmiddelen (die kunnen worden gebruikt in het proces voor de kandidaatstelling en om de uitslag van de verkiezingen en de zeteltoedeling te berekenen) op een adequate wijze te kunnen uitvoeren.

De transitie duurt maximaal 1,5 jaar en is medio mei 2019 gestart. Het einde van de transitie is november 2020. De deskundigheid en capaciteit die nodig is om de resultaten van de transitie te realiseren wordt ingebracht door het ministerie van BZK, Kiesraad, VNG en NVVB. Zou die deskundigheid/capaciteit specifiek voor de transitie worden aangetrokken, dan is het de bedoeling dat de kennis en ervaring die tijdens de transitie wordt opgebouwd (met betrekking tot de aanbesteding en ontwikkeling van het digitaal middel voor de uitslagvaststelling) na de transitie behouden blijft en ter beschikking komt van de Kiesraad.

Op 8 juli jl. heeft er een startsessie Digitale hulpmiddelen plaatsgevonden. De conclusies hiervan maken integraal deel uit van dit plan van aanpak, zie bijlage 1. Het doel van deze sessie was om gezamenlijk (BZK, Kiesraad en VNG) de opdracht voor de Programmadirecteur transitie vast te stellen en om een start te maken met het programma. Tijdens de startsessie zijn als beoogde resultaten voor de transitie vastgesteld:

- Programma van eisen, aanbesteding, gunning en ontwikkeling digitaal hulpmiddel uitslagvaststelling (digitaal hulpmiddel nog niet gereed bij afloop transitie);
- Wet- en regelgeving taken en verantwoordelijkheid voor digitale hulpmiddelen naar Raad van State;
- Bepaal of en zo ja in welke mate het verkiezingsproces of onderdelen daarvan tot de vitale infrastructuur moeten gaan behoren en wat de gevolgen zijn. Let op: deze formulering wijkt af van het advies van de verkenner. De aanwezigen stemmen in met het beoogde resultaat voor de Programmadirecteur transitie. Bij de uitwerking van deze scenario's worden AIVD, NCTV, NCSC, IBD en VNG Realisatie betrokken;
- Vernieuw de Kiesraad (opleveren impact analyse wat nodig is voor uitvoering nieuwe taken door Kiesraad (incl. formatie, competenties en financiering);
- Kader voor afstemming / samenwerking tussen Kiesraad, gemeenten en ministerie van BZK.

In dit Plan van Aanpak wordt aangegeven hoe deze resultaten worden behaald en binnen welk tijdsbestek.

De globale planning laat zien dat bij het einde van de transitie (november 2020) er weliswaar al grote stappen zijn gezet, maar ook laat de planning zien dat de wet- en regelgeving en het nieuwe digitale hulpmiddel dan nog niet gereed zijn. Eind tweede kwartaal 2020 zal besloten moeten worden of de transitieperiode verlengd moet worden en er een onafhankelijke procesbegeleider nodig blijft of dat partijen zelf de producten vervolmaken. Ook moet dan worden besloten wanneer de verkiezingsautoriteit zal starten.

3. Aanpak

Het ontwerpen en maken van digitale hulpmiddelen, bijbehorende aanpassingen aan de wetgeving en het komen tot een verkiezingsautoriteit in een kort tijdsbestek is een ambitieus project. Binnen de bestaande organisaties is er (in ieder geval op korte termijn) weinig capaciteit en/of deskundigheid beschikbaar. Het bureau van de Kiesraad heeft voorgesteld om te werken met een programmateam. Dit voorstel is gevolgd. Er is per 1 september een programmasecretaris aangesteld (0,8 fte) en op korte termijn wordt deskundigheid en capaciteit voor het schrijven aan opdrachtverlening en bestek voor digitale hulpmiddelen aan het programmateam toegevoegd (2,0 fte). Deze capaciteit wordt buiten Kiesraad, BZK, VNG en NVVB gezocht, bij voorkeur bij ICTU. Het programmateam zal wekelijks voortgangsoverleg hebben met een medewerker van Kiesraad, VNG / NVVB en BZK.

De werkzaamheden die nodig zijn voor de realisatie van de beoogde eindresultaten worden door de werkgroepen uitgevoerd. Deelnemende organisaties zullen vanuit deskundigheid een bijdrage moeten leveren. Door waar nodig zelf te produceren of waar nodig te reflecteren op de geproduceerde notities. Inbreng van Kiesraad (bureau en bestuurlijk), BZK, VNG en NVVB is nodig. Er worden vier werkgroepen ingesteld:

- 1) Verkiezingsproces en nieuwe digitale hulpmiddelen;
- 2) Verkiezingsautoriteit bestuurlijk (taken, bevoegdheden, samenstelling, vergoeding, verantwoording, vormgeving etc.) en organisatorisch (personeel, huisvesting, facilitair etc.);
- 3) Financiën (incidentele en structurele begroting verkiezingsautoriteit, benodigde middelen ontwerp en beheer digitale hulpmiddelen);
- 4) Communicatie en informatiestrategie in en na transitiefase, opbouw en onderhoud netwerkfunctie, toekomstige samenwerking Kiesraad, gemeenten en ministerie.

De op te leveren producten worden ter besluitvorming voorgelegd aan de stuurgroep die inhoudelijk dus bepalend is. Vervolgens worden deze besluiten via de reguliere lijn van Binnenlandse Zaken aan de minister van BZK voorgelegd.

De eerste taak van de werkgroepen is het nader uitwerken van wat moet worden opgeleverd en het opstellen van een detailplanning. Hierbij wordt in kaart gebracht wanneer er besluitvorming door de stuurgroep nodig is en de planning tot aan het voorleggen van de besluiten van de stuurgroep aan de minister van BZK.

In het plan van aanpak wordt in bijlage 2 ingegaan op de acties rond het urgente onderhoud van OSV en mitigerende maatregelen. De acties rond het urgente onderhoud aan OSV maakt geen deel uit van de transitie. Mitigerende maatregelen rond OSV maken wel deel uit van de transitie omdat deze maatregelen nauw verbonden zijn aan de verantwoordelijkheid van de Kiesraad.

Wetgeving

Bij het realiseren van deze wet- en regelgeving is het Grondwettelijk kader het uitgangspunt. Artikel 59 stelt immers "Alles, wat verder het kiesrecht en de verkiezingen betreft, wordt bij de wet geregeld". Dit laat onverlet dat er altijd interpretatieruimte is. Er zal expliciet worden besloten wat in de Kieswet geregeld moet worden (bijvoorbeeld kaders, raamwerk en verantwoordelijkheden) en wat in andere, "lagere" regelgeving (meer het "hoe"). Het grote voordeel van deze indeling is dat lagere regelgeving sneller aangepast kan worden aan nieuwe ontwikkelingen. De snelheid in de digitale wereld zoals op het terrein van cybersecurity ligt immers doorgaans in elk geval hoger dan van aanpassing van formele wetgeving.

De voortgang van de wetgeving hangt sterk af van de voortgang van besluitvorming rond het digitale hulpmiddel en de verkiezingsautoriteit. Medewerkers van de directie Constitutionele Zaken en Wetgeving worden betrokken bij de werkgroep "verkiezingsproces en nieuwe digitale hulpmiddelen" en "verkiezingsautoriteit bestuurlijk en organisatorisch", zodat wetgeving (en memorie) hand in hand optrekt met voortgang rond het digitale hulpmiddel. Eind juni 2020 zal de concept wet gereed zijn en voor consultatie worden voorgelegd. Na de zomer 2020 zal het wetsvoorstel voor reactie naar de Raad van State gaan. Begin 2021 zal de wet aan de Tweede Kamer worden voorgelegd.

Dreigingsanalyse en betrouwbaarheidsvereisten

Er is contact gelegd met de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en het Nationale Cyber Security Center (NCSC). Beide organisaties zijn - los van de vraag of het verkiezingsproces als vitale infrastructuur wordt bestempeld - bereid te helpen met het opstellen van een dreigings-, belangen en risico-analyse. Om deze analyses zo grondig als mogelijk te doen worden de verschillende fasen van het digitaal hulpmiddel apart in beschouwing genomen; er komen dus meerdere risico-analyses (vooralsnog 3, zie ook "werkgroep verkiezingsproces en digitale hulpmiddelen". De te volgen werkwijze is afgestemd met AIVD en NCSC en is als volgt (zie ook bijlage 3):

1. Opstellen dreigingsanalyse (wie heeft intentie en wie heeft potentie tot spionage, sabotage of manipulatie; tweede helft september gereed);
2. Belangenanalyse (wat zijn de te beschermen belangen en op welke wijze kan dit. Dit verschilt per digitaal hulpmiddel (november gereed);
3. Risicoanalyses (wat zijn de risico's en hoe deze te waarderen, november gereed);
4. Accepteren of mitigeren (hoe gaan we om met de risico's. Aanpassingen in software of in proces? Terugvalopties?);
5. Forensic readiness beoordelen (zorg er bij ontwerp van digitaal hulpmiddel voor dat te achterhalen is of en hoe er met software, hardware etc. "geknoeid" is).

Indien nodig kunnen genoemde organisaties ook helpen met cryptografie rond de te ontwikkelen producten. Dit hangt o.a. af van de uitkomsten van de dreigings- en belangenanalyse.

AIVD en NCSC geven aan over voldoende informatie te beschikken om een dreigingsanalyse te maken. De dreigingsanalyse is eind september gereed. Om te komen tot een goede belangen- en risico-analyse is meer informatie nodig over hoe het verkiezingsproces nu precies werkt, welke rol digitale middelen hebben etc. De belangen- en risico-analyses zijn eind november gereed.

Begin september komt er duidelijkheid of de NCTV en zo ja hoe zij vanuit haar deskundigheid kan adviseren over de aanbestedingsstrategie van de digitale hulpmiddelen (onderhands of openbaar, te stellen voorwaarden en eisen etc.).

Werkgroep 'verkiezingsproces en nieuwe digitale hulpmiddelen'

- Prioriteit ligt bij digitaal hulpmiddel vaststelling uitslag. Welke eisen worden er gesteld aan dit hulpmiddel en aan de processen hieromheen?
- In de verschillende fasen in het verkiezingsproces is behoefte aan verschillende vormen van digitale hulpmiddelen. Denk bijv. aan kandidaatstelling maar ook aan register ongeldige stemmen. Voorbereiden besluitvorming een of meerdere hulpmiddelen (reikwijdtedocument). Per hulpmiddel vervolgens aangeven wat Program van Eisen is.
- Vaststellen onderhouds- en beheer strategie (wie beheert hard- en software etc.)
- Vaststellen aanbestedingsstrategie
- Besluitvorming over al dan niet certificering
- Vaststellen keuze t.a.v. aanbesteding digitaal hulpmiddel kandidaatstelling
- Besluiten of vereisten 'elektronisch tellen stemmen' deel uit maakt van transitie
- Qua wet- en regelgeving te regelen welke organen welke verantwoordelijkheden en bevoegdheden hebben i.v.m. de ontwikkeling, het beheer en het onderhoud van de digitale hulpmiddelen die in het verkiezingsproces mogen worden gebruikt, alsmede te regelen aan welke betrouwbaarheidseisen deze digitale hulpmiddelen moeten voldoen
- *Uiteindelijk resultaat: reikwijdtedocument, aanbestedingsstrategie en PvE digitale hulpmiddelen. Uiteindelijk leidt dit tot één of meerdere nieuwe digitale hulpmiddelen*

Een succesvol ICT-traject begint bij het doordenken (en waar nodig herontwerpen) van de verschillende fasen van het verkiezingsproces. Ook voor het bepalen van de rol en verantwoordelijkheid en voor het programma van eisen van de digitale hulpmiddelen (in brede zin des woords, zie eerder) is dit doordenken noodzakelijk. De te onderscheiden fasen zijn:

- o Bepalen kiesgerechtigdheid;
- o Vaststellen kandidatenlijsten;
- o Voorbereiding stemming;
- o Stemming;
- o Stemopneming;
- o Berekening uitslag;
- o Uitslagvaststelling en zeteltoedeling;
- o Toelating leden.

Bepalen kiesgerechtigdheid

Het is aan gemeenten om de kiesgerechtigdheid vast te stellen. Gemeenten maken daarbij gebruik van de basisregistratie personen (BRP). Vernieuwing aan deze basisregistratie en burgerzakenmodules maken geen deel uit van de transitie.

Vaststellen kandidatenlijsten

Bij het digitale hulpmiddel voor de kandidaatstelling betreft het een digitaal hulpmiddel dat gebruikt kan worden door politieke partijen voor het aanmaken van hun kandidatenlijst en alle overige formulieren die benodigd zijn in het kader van de kandidaatstelling. Het hulpmiddel kan ook worden gebruikt door het centraal stembureau voor het onderzoek van de ingeleverde lijsten, het vaststellen van verzuimen en daaropvolgende besluitvorming over de geldigheid van de lijsten en de nummering daarvan.

Op dit moment is het vaststellen van de kandidatenlijsten een module binnen de Ondersteunende Software Verkiezingen. Het is een te maken keuze of hieraan wordt vastgehouden of dat een andere opzet beter aansluit bij het verkiezingsproces en het gebruik van de middelen. Voor het nieuwe digitale hulpmiddel kan bijvoorbeeld ook gekozen worden voor bijvoorbeeld een zelfstandige webapplicatie. Deze keuze maakt deel uit van de aanbestedingsstrategie en zou kunnen leiden tot 1 of meerdere aanbestedingen.

Vorbereiding stemming

Gemeenten zijn en blijven verantwoordelijk voor de organisatie van de verkiezingen, voor het produceren en distribueren van stempassen, kiezerspassen, schriftelijke volmachten, kandidatenlijsten en stembiljetten, voor administratieve systemen zoals het register ongeldige stempassen, voor stempassen/kiezerspassen/schriftelijke volmachten, voor overzichten van kandidaten/stembiljetten en voor administratie/organisatie van de stemlokalen/stembureaus. Tevens zijn en blijven gemeenten verantwoordelijk voor het toegankelijk maken van de stemlokalen en voor het werven, selecteren, trainen en benoemen van stembureauleden en -tellers. Voor zover gemeenten bij de uitoefening van deze taken gebruik maken van digitale hulpmiddelen, maken deze geen deel uit van deze transitie.

In de transitie wordt wel bezien in hoeverre op bovenstaande punten de Kiesraad de bevoegdheid moet krijgen om voorschriften te kunnen geven. In de stuurgroep van december 2019 vindt een eerste bespreking plaats; in januari 2020 besluitvorming.

Stemming

Tijdens de stemming wordt bij een aantal stembureaus gebruik gemaakt van de stembureau-app. Deze app wordt gebruikt als communicatiemiddel (is het stembureau voltallig? Zijn er voldoende stembiljetten? Zijn er onregelmatigheden? Hoe hoog ligt de opkomst? etc.) en ook als digitaal hulpmiddel voor de controle van kiesgerechtigheid. Deze app controleert of het nummer (of de QR-code) van de stempas voorkomt in het register van ongeldige stempassen en bepaalt of de kiezer kan deelnemen aan de stemming. Ook 'telt' de app het aantal gescande geldige stempassen zodat dit ter controle vergeleken kan worden met het aantal handmatig getelde stemmen.

In de startsessie is afgesproken dat in de transitieperiode eisen geformuleerd worden aan de digitale hulpmiddelen die direct dan wel indirect invloed hebben op de uitslag(berekening). Er kan gediscussieerd worden of dit uitgangspunt betekent dat de Kiesraad eisen moet stellen aan de Stembureau app. Het communicatie en management deel heeft immers geen invloed op de uitslag (Berekening) en de beoordeling of iemand wel of niet mag stemmen alleen indirect. Indirect omdat de afspraak is dat als de Stembureau app aangeeft dat als een stem ongeldig is, ook in de papieren uitdraai wordt gekeken. Tegelijkertijd kan dit papieren proces (gebaseerd op digitale registratie) ook kwetsbaar zijn en indien digitale hulpmiddelen beschikbaar zijn, kunnen ze in de praktijk leidend zijn. Het verkiezingsproces is gebaseerd op vertrouwen van burgers. Daarom zal in de transitie ook worden gekeken welke eisen gesteld moeten worden aan de Stembureau app (software, hardware, infrastructuur, procedures en processen). Hierbij worden Kiesraad, BZK, VNG (beleid en realisatie), NVVB, AIVD, NCC, NCSC en IBD betrokken. Hierbij wordt nadrukkelijk gebruik gemaakt van al beschikbare studies. In februari 2020 zal dit in de stuurgroep worden vastgesteld.

Tenslotte zal in de transitiefase worden onderzocht of de stembureau-app bij meerdere gemeenten uitgerold kan worden en wat daarvoor nodig is. Dit zal in januari 2020 in de stuurgroep worden besproken.

Stemopneming, Berekening uitslag, uitslagvaststelling, zeteltoedeling en toelating leden

Bepaald moet worden aan welke functionaliteiten en aan welke betrouwbaarheids- en beveiligingseisen de nieuwe digitale software moet voldoen. Ook moet duidelijk worden wie hiervoor aan zet is en of en zo ja hoe een toezichtsrol nodig is (stuurgroep februari 2020).

Aanpak

Per fase van het verkiezingsproces zal worden bepaald wat de behoefte is aan een digitaal hulpmiddel en welke rol en verantwoordelijkheid helder moet worden. Dit betreft niet alleen wie doet wat, maar ook wie controleert vervolgens wat, wie stelt eisen, is er een certificerende partij etc. Uit voorgaande volgt dat er drie 'blokken' zijn:

- 1) Kandidaatstelling;
- 2) Stemming en stemopnemen (vgl. stembureau app);
- 3) Berekening uitslag, uitslagvaststelling en zeteltoedeling, toelating leden.

Rond deze drie 'blokken' zal o.a. een Programma van Eisen moeten worden opgesteld. In september 2019 wordt gestart met een reikwijdte document en wat er nog meer nodig is om tot een bestek te komen. Daarbij zal gebruik worden gemaakt van eerdere aanbestedingen (zowel OSV, urgent onderhoud aan OSV als Stembureau-app). Ook kan gebruik worden gemaakt van de eerste inventarisatie die onder regie van de Kiesraad heeft plaatsgevonden¹. Het Programma van Eisen zal in december 2019 - indien nodig - worden aangevuld met de bevindingen van de risico-analyse van de AIVD, NCC en NCSC. Er zal vervolgens met deze partijen gewerkt worden aan het bepalen van de noodzakelijke betrouwbaarheid en beveiligingsvereisten aan apparatuur, programmatuur en (digitale) infrastructuur (waaronder ook de gebruikte netwerken).

Er dient voor alle drie 'blokken' een heldere kaders en voorwaarden te worden bepaald en indien er een nieuw product (of onderdeel) ontwikkeld dient te worden een aanbestedingsstrategie. Deze aanbestedingsstrategie wordt in februari 2020 vastgesteld. De aanbestedingsstrategie moet o.a. waarborgen dat er sprake is van (zie ook Kiesbesluit en Kiesregeling voor de huidige eisen):

- Transparantie en controleerbaarheid van het digitaal hulpmiddel;
- Continuïteit van het gebruik van het digitaal hulpmiddelen voor een lange periode (7 tot 10 jaar) en bij voorkeur langer. Doorontwikkeling of opnieuw ontwikkelen van het digitaal hulpmiddel moet derhalve mogelijk zijn;
- Weerbaarheid bij ontwikkeling, onderhoud, ondersteuning en gebruik tegen dreigingen van statelijke en andere actoren;
- Dat er geen afhankelijkheid ontstaat van één leverancier.

Bij deze aanbestedingsstrategie worden - naast HIS - BZK, Kiesraad en VNG realisatie betrokken. De aanbesteding(en) voorbereiden en uitvoeren zal zeker tot de zomer 2020 in beslag nemen. Er resteert dan 1 tot 1½ jaar om de programmatuur te ontwikkelen, te testen en te accepteren voor gebruik. Ook zal samen met VNG en NVVB nagedacht moeten worden hoe het wordt uitgerold, hoe gebruikers worden getraind etc.

Elektronisch tellen: geen onderdeel van de transitie

Op termijn zullen stemmen elektronisch geteld worden. Dit wordt mogelijk met het nieuwe kiesbiljet en aangekondigde experimenten. Om te komen tot elektronisch tellen van stemmen is een aanbesteding vereist. Deze aanbesteding maakt geen deel uit van de transitie en daarmee dus ook geen deel van dit programma, Te zijner tijd zal de Kiesraad of BZK deze aanbesteding op zich zal nemen

¹ In april 2019 hebben de kiesraad en BZK afgesproken dat er "fullspeed" aan het programma van eisen moet worden gewerkt met als doel om in het najaar een aanbesteding te kunnen starten en gunning rond de jaarwisseling mogelijk te maken kan zijn. De Kiesraad heeft dit tot 1 september 2019 getrokken en draagt de activiteiten per 1 september 2019 over aan de programmadirecteur.

BR



BR



BR



BR



BR



BR



BR



BR



BR



4. Project inrichting en voorwaarden

De minister van Binnenlandse Zaken en Koninkrijksrelaties (BZK) is opdrachtgever voor de transitie. Materieel zal de Stuurgroep als opdrachtgever fungeren. De stuurgroep is samengesteld uit vertegenwoordigers van het ministerie van BZK, de Kiesraad en de Vereniging van Nederlandse Gemeenten (VNG). De vaste leden van de stuurgroep zijn:

BR.2.e	5.1.2.e	BZK
5.1.2.e	5.1.2.e	Kiesraad
5.1.2.e	5.1.2.e	
	5.1.2.e	VNG

Bij de stuurgroep zijn met het oog op juridische, bestuurlijke en uitvoeringstechnische deskundigheid verder aanwezig:

5.1.2.e	5.1.2.e	BZK
5.1.2.e	5.1.2.e	
5.1.2.e	5.1.2.e	NVVB

Ook de 5.1.2.e en 5.1.2.e zijn bij de stuurgroep aanwezig.

De stuurgroep stuurt op de voortgang van het totale programma en neemt daarvoor noodzakelijke besluiten, ziet toe op de aanwezigheid van voldoende groot draagvlak bij de eigen en andere organisaties, ziet toe op de capaciteitstoedeling conform afspraken en ziet toe op de kwaliteit van de programmadirecteur en programmateam. De programmasecretaris is verantwoordelijk voor de procesmatige voorbereiding en verslaglegging van de vergaderingen van de stuurgroep. De stuurgroepleden zorgen voor afdoende mandaat namens hun organisatie. De stuurgroep vergadert in beginsel één keer per maand. Dit zal worden gepland iedere derde week van de maand. De eerste vergadering vindt plaats in de eerste week van september.

Minimaal 2 keer per jaar bespreken de directeur-generaal BRW, de voorzitter van de Kiesraad en de algemeen directeur van de VNG de voortgang van de transitie en eventuele knelpunten die zich daarbij voordoen. De Programmadirecteur transitie verzorgt het secretariaat.

Bij het bestaande bestuurlijke overleg tussen VNG en BZK Democratie en Bestuur wordt de voortgang van de transitie geagendeerd. Bij dit agendapunt zal ook de voorzitter van de Kiesraad worden uitgenodigd.

De programmadirecteur treedt in overleg met VNG over hoe bestuurders van gemeenten verder betrokken zullen worden bij het transitieproces.

Het programmateam bestaat uit de programmadirecteur transitie, een programmasecretaris en twee medewerkers voor het digitale hulpmiddel. Daarnaast is inzet nodig voor de werkgroepen van de deelnemende organisaties. Dit betreft de wekelijkse vergadering van het programmateam (0,1 fte voor Kiesraad, BZK en VNG/NVVB). Het is op dit moment moeilijk in te schatten wat het tijdsbeslag is voor het digitale hulpmiddel. Verondersteld wordt dat het capaciteitsbeslag voor Kiesraad, BZK en VNG / NVVB daar in de periode 1 sept 2019 – 1 maart 2020 0,5-1 fte is. Voor de verkiezingsautoriteit zal dit voor Kiesraad naar verwachten 1 fte zijn. Voor BZK en VNG/NVVB naar verwachting één tot twee dagen per week zijn. Tenslotte stelt BZK voldoende capaciteit ter beschikking voor het wetgevingsproces. De programmadirecteur bewaakt of er voldoende capaciteit is. Als deze onvoldoende is, zal dit besproken worden in de stuurgroep. De deelnemers aan de werkgroepen zitten vanuit hun deskundigheid in de werkgroep en leggen geen verantwoording af aan de programmadirecteur.

De deelname aan de vier werkgroepen is als volgt:

Werkgroep	BZK	VNG/ NVVB	Kiesraad
1) Verkiezingsproces en nieuwe digitale hulpmiddelen	5.1.2.e [redacted] 5.1.2.e [redacted] @minbzk.nl 5.1.2.e [redacted] 5.1.2.e [redacted] @minbzk.nl 5.1.2.e [redacted] 5.1.2.e [redacted] @minbzk.nl (agendalid)	5.1.2.e [redacted] 5.1.2.e [redacted] @vng.nl 5.1.2.e [redacted] 5.1.2.e [redacted] @utrecht.nl 5.1.2.e [redacted] 5.1.2.e [redacted] @rotterdam.nl (vervanger 5.1.2.e [redacted] 5.1.2.e [redacted] 5.1.2.e [redacted] @rotterdam.nl) Voor de aanbestedingsstrategie: 5.1.2.e [redacted] 5.1.2.e [redacted] @vng.nl 5.1.2.e [redacted] 5.1.2.e [redacted] @vng.nl 5.1.2.e [redacted] 5.1.2.e [redacted] : 5.1.2.e [redacted] 5.1.2.e [redacted] @vng.nl	5.1.2.e [redacted] 5.1.2.e [redacted] @Kiesraad.nl 5.1.2.e [redacted] 5.1.2.e [redacted] @kiesraad.nl 5.1.2.e [redacted] 5.1.2.e [redacted] @kiesraad.nl
2) Verkiezingsautoriteit bestuurlijk en organisatorisch	5.1.2.e [redacted] 5.1.2.e [redacted] @minbzk.nl 5.1.2.e [redacted] 5.1.2.e [redacted] @minbzk.nl	5.1.2.e [redacted] 5.1.2.e [redacted] @vng.nl Of 5.1.2.e [redacted] 5.1.2.e [redacted] @vng.nl 5.1.2.e [redacted] 5.1.2.e [redacted] @nvvb.nl 5.1.2.e [redacted] (agendalid) 5.1.2.e [redacted] @vng.nl 5.1.2.e [redacted] (agendalid) 5.1.2.e [redacted] @vng.nl	5.1.2.e [redacted] 5.1.2.e [redacted] @kiesraad.nl 5.1.2.e [redacted] 5.1.2.e [redacted] @kiesraad.nl 5.1.2.e [redacted] 5.1.2.e [redacted] @kiesraad.nl 5.1.2.e [redacted] 5.1.2.e [redacted] @kiesraad.nl 5.1.2.e [redacted] (agendalid) 5.1.2.e [redacted] @kiesraad.nl
3) Financiën	Pm	5.1.2.e [redacted] 5.1.2.e [redacted] @vng.nl 5.1.2.e [redacted] 5.1.2.e [redacted] @vng.nl	5.1.2.e [redacted] 5.1.2.e [redacted] @kiesraad.nl
4) Communicatie en informatiestrategie	Pm	5.1.2.e [redacted] 5.1.2.e [redacted] @vng.nl	5.1.2.e [redacted] 5.1.2.e [redacted] @kiesraad.nl 5.1.2.e [redacted] 5.1.2.e [redacted] @kiesraad.nl 5.1.2.e [redacted] (agendalid) 5.1.2.e [redacted] @kiesraad.nl

Budget programma

BZK draagt zorg dat er voldoende budget en bemensing is voor het programmateam.

Kwaliteitsborging

Voor kwaliteitsborging zal de programmadirecteur een klankbordgroep instellen voor reflectie. Het betreft kennis op het terrein van ICT (bijvoorbeeld een (oud) CIO van het rijk), institutionele vormgeving en cyber security.

Risico analyse

Risico	Kans (1 klein, 5 groot)	Impact (1 klein, 5 groot)	Gevolg	Beheersmaatregel
Te weinig capaciteit vanuit Kiesraad, VNG/NVVB en BZK	4	5	Vertraging Afstand tussen voortgang project en besluitvorming	In plan van aanpak extra capaciteit toegevoegd voor 'productieproces' aan projectteam Maandelijks rapportage aan stuurgroep van programmadirecteur
Wederzijdse afhankelijkheden (wetgeving en digitaal hulpmiddel, verkiezingsautoriteit bestuurlijk en organisatorisch en financiën)	4	4	Vertraging	Strakke sturing op planning en frequente stuurgroep
Onvoldoende draagvlak deelnemende organisaties	3	4	Vertraging	Stuurgroep stuurt op planning Bestuurlijk overleg Wekelijks overleg projectteam en medewerkers betrokken organisaties
Onvoldoende draagvlak politiek / bestuurlijk	3	3	Vertraging	2x per jaar bestuurlijk overleg 2x per jaar voortgangsrapportage aan Kamer Uitvoering actief betrekken
Te weinig deskundigheid opstellen PvE	3	3	Vertraging Geen goed opdrachtgeverschap	Aan projectteam externe deskundigheid op ICT en opdrachtverlenerschap toegevoegd Instellen klankbordgroep kwaliteitsborging
Te weinig financiële middelen voor ontwikkeling digitale hulpmiddel	2	4	Geen opdracht kunnen verstrekken medio 2021	Vroegtijdige betrokkenheid FEZ Voorbereiden claim voorjaarsnotabesluitvorming

5. Planning

In september 2019 zal onder regie van BZK de aanbesteding plaatsvinden van noodzakelijk en urgent onderhoud aan OSV. Deze verbeterde versie OSV (aangevuld met mitigerende maatregelen) dient gebruikt te worden bij de herindelingsverkiezingen van 2020 en 2021, de Tweede Kamerverkiezingen van 2021 en de gemeenteraadsverkiezingen 2022. De uiterlijke datum wanneer het nieuwe Digitaal Hulpmiddel Uitslagberekening gereed moet zijn is 1 juli 2022 (afloop contract OSV).

De inzet is om bij enkele gemeenten bij de gemeenteraadsverkiezingen van 16 maart 2022 proef te draaien met de nieuwe digitale hulpmiddelen. Dit betekent dat de wetgeving rond de verkiezingsautoriteit eind 2021 vastgesteld moet worden om de diverse uitvoerders voldoende tijd te bieden zich goed voor te bereiden. Dit betekent dat 1 juli 2020 de wet voor consultatie moet worden voorgelegd. Na de zomer 2020 zal het wetsvoorstel voor reactie naar de Raad van State gaan. Begin 2021 zal de wet aan de Tweede Kamer worden voorgelegd.

Ook de nieuwe digitale hulpmiddelen moeten eind 2021 volledig gereed zijn. Om dit te realiseren zal het programma van eisen eind eerste kwartaal 2020 gereed moeten zijn en den aanbesteding verder worden voorbereid. Gunning zal medio 2020 moeten plaatsvinden zodat er 1 tot 1½ jaar beschikbaar is om de programmatuur te ontwikkelen, te testen en te accepteren voor gebruik. Tijdens de ontwikkeling zal ook gewerkt worden aan een uitrolstrategie en worden trainingen en dergelijke voorbereid.

De Tweede Kamer zal in fasen worden meegenomen. In september 2019 zal de Tweede Kamer worden geïnformeerd over de planning van de nieuwe digitale hulpmiddelen en nieuwe wetgeving om te komen tot een verkiezingsautoriteit. In het vierde kwartaal ontvangt de Tweede Kamer voortgangsinformatie van de transitie. Eind eerste kwartaal 2020 zullen hoofdlijnen voor de hulpmiddelen en voor de Verkiezingsautoriteit worden besproken met de Tweede Kamer, zodat aanbesteding en consultatie kan plaatsvinden. Na gunning zal de Kamer opnieuw worden geïnformeerd.

Iedere maand is er een stuurgroep. Twee keer per jaar (om te beginnen in november / december zal er een overleg plaatsvinden tussen de DG BZK, VNG en Kiesraad. De tweede sessie is eind tweede kwartaal 2020). Ook twee keer per jaar is er een bestuurlijk overleg.

Chronologisch

September 2019

- Informeren Tweede Kamer over planning nieuwe digitale hulpmiddelen en transitie Kiesraad tot verkiezingsautoriteit
- Vaststellen Plan van Aanpak in stuurgroep (incl. samenstelling werkgroepen)
- Dreigingsanalyse AIVD, NCC en NCSC gereed
- Vaststellen wat nodig is om tot reikwijdte document en andere delen bestek te komen
- Schets door Kiesraad wat de te nemen besluiten zijn rond transitie tot verkiezingsautoriteit

Oktober 2019

- Communicatiestrategie gereed
- Schets door Kiesraad van huidige organisatie

November 2019

- Eerste bespreking scenario's rond digitale hulpmiddelen
- Aanbestedingsstrategie op hoofdlijnen vaststellen
- Eerste bespreking scenario's verkiezingsautoriteit
- Eerste voortgangsnotitie TK vaststellen
- Besluitvorming (aanvullende) mitigerende maatregelen rond OSV (verkiezingen 2021)

December 2019

- Eerste bespreking over of en welke voorschriften Kiesraad moet kunnen geven aan gemeenten rond verkiezingen

Januari 2020

- Besluitvorming verkiezingsautoriteit rol en verantwoordelijkheden
- Besluitvorming over of en welke voorschriften Kiesraad moet kunnen geven aan gemeenten rond verkiezingen
- Vaststellen claim voorjaarsnotabesluitvorming

Februari 2020

- Tweede voortgangsnotitie TK vaststellen
- Vaststellen Programma van Eisen voor digitale hulpmiddelen
- Vaststellen aanbestedingsstrategie
- Analyse huidig secretariaat Kiesraad (budget, personeel, huisvesting etc.) en hoe dit aansluit bij (toekomstige) taken.

Juni 2020

- Vaststellen wetsvoorstel voor consultatie
- Gunning aanbesteding(en) / start ontwikkeling digitale hulpmiddelen

Juni 2021

- Start testen digitale hulpmiddelen

December 2021

- Digitale hulpmiddelen gereed
- Wetgeving gereed

Bijlage 1 Verslag startsessie 8 juli 2019

Conclusies Startsessie Digitale hulpmiddelen maandag 8 juli van 13.00 tot 17.15

Aanwezigen: Kiesraad: 5.1.2.e [redacted] 5.1.2.e [redacted] 5.1.2.e [redacted] 5.1.2.e [redacted]
5.1.2.e [redacted] en 5.1.2.e [redacted]
Bureau Kiesraad: 5.1.2.e [redacted] 5.1.2.e [redacted] 5.1.2.e [redacted] en 5.1.2.e [redacted]
VNG: 5.1.2.e [redacted] (vanaf 16.00 u), 5.1.2.e [redacted] en 5.1.2.e [redacted]
BZK: 5.1.2.e [redacted] 5.1.2.e [redacted] 5.1.2.e [redacted] 5.1.2.e [redacted] 5.1.2.e [redacted] en 5.1.2.e [redacted]
5.1.2.e [redacted]

- De conclusies en aanbevelingen van de verkenner (zie briefadvies bijlage 3 bij agendastukken) worden onderschreven. De verantwoordelijkheid voor de digitale hulpmiddelen wordt uiteindelijk bij de Kiesraad gelegd waarbij verantwoordelijkheden en bevoegdheden worden verankerd in de kieswet. Onder verantwoordelijkheid van de minister van BZK zal de transitie plaatsvinden om de Kiesraad in staat te stellen deze verantwoordelijkheid verantwoord te dragen.
- De opdracht voor de transitie en daarmee voor de programmadirecteur wordt onderschreven (zie bijlage 4 bij agenda stukken). Op hoofdlijnen betekent dit dat de programma directeur al het nodige doet en regelt (juridisch, organisatorisch en financieel) om in wet- en regelgeving heldere verantwoordelijkheids- en bevoegdheidsverdeling te krijgen en de Kiesraad in staat te stellen nieuwe taken en bevoegdheden adequaat uit te voeren. De beoogde resultaten voor de transitie zijn:
 - Wet- en regelgeving taken en verantwoordelijkheid voor digitale hulpmiddelen
 - Programma van eisen, aanbesteding, gunning en ontwikkeling digitaal hulpmiddel uitslagvaststelling.
 - Bepaal of en zo ja in welke mate verkiezingsproces of onderdelen tot vitale infrastructuur moeten gaan behoren en wat de gevolgen zijn. Let op: deze formulering wijkt af van het advies van de verkenner. De aanwezigen stemmen in met het beoogde resultaat voor de transitiedirecteur. Bij de uitwerking van deze scenario's worden AIVD, NCTV, NCSC en IBD betrokken
 - Vernieuw de Kiesraad (impact analyse wat nodig is voor uitvoering nieuwe taken door Kiesraad (incl. formatie, competenties en financiering)
 - Kader voor afstemming / samenwerking tussen Kiesraad, gemeenten en ministerie
- De programmadirecteur betreft bij het transitieproject naast VNG (beleid en realisatie), Kiesraad (Leden en bureau) en BZK (beleid en wetgeving) indien dit toegevoegde waarde heeft SSO-ICT en Logius. De NVVB wordt zeker betrokken.
- De aanwezigen zijn het eens met de navolgende richting voor verantwoordelijkheids- en bevoegdheidsverdeling. Deze richting wordt na de zomer verder uitgewerkt in scenario's en een risico-analyse:
 - BR [redacted]

BR

○

BR

○

BR

○

BR

○

- Er worden in de transitieperiode eisen geformuleerd aan de digitale hulpmiddelen (centraal en decentraal, verplichtend en vrijwillig) die direct dan wel indirect invloed hebben op de uitslag (berekening). Deze eisen kunnen verschillen tussen de hulpmiddelen voor wat betreft betrouwbaarheid en beveiliging;
- De Kiesraad wordt verantwoordelijk voor het digitaal hulpmiddel voor het elektronisch tellen van de stembiljetten en de Kiesraad wordt verantwoordelijk voor het digitale hulpmiddel voor de berekeningen van de uitslag en zetelverdeling van alle verkiezingen. Bij het stellen van voorschriften wordt telkens afgewogen in hoeverre deze noodzakelijk zijn voor het waarborgen van de betrouwbaarheid van de verkiezingen (proportionaliteit);
- Er is een vernieuwing nodig van de software voor de kandidaatstelling. In de transitie wordt vastgesteld of deze software onderdeel wordt van het digitale hulpmiddel voor de uitslagberekening of dat het een zelfstandig hulpmiddel wordt en er dus ook een aparte aanbesteding wordt gedaan. De Kiesraad wordt verantwoordelijk voor het

digitale hulpmiddel voor de kandidaatstelling. Het voordeel van meerdere digitale hulpmiddelen is dat gemakkelijker gedifferentieerd kan worden in beveiligingsvereisten. Wel is dan een vorm van communicatie tussen de hulpmiddelen nodig. Prioriteit ligt bij het digitale hulpmiddel voor de vaststelling van de uitslag;

- De prioriteit voor het (de) digitale hulpmiddel(len) ligt bij de vaststelling van de uitslag. Dit dient tot uiting te komen in de geplande werkzaamheden;

- BR [Redacted]

- BR [Redacted]

- De transitiedirecteur zorgt dat er aan het einde van 2019 een (eerste) onderbouwde claim is voor het versterken van de organisatie van de Kiesraad, voor de tot standkoming van het digitale hulpmiddel(len) en voor het beheer en onderhoud van het digitale hulpmiddel(len);
- Er is bij alle partijen de behoefte om gebruik te maken van programmatuur voor het vaststellen van de uitslag en van de zeteltoedeling. Zolang er geen nieuw digitaal hulpmiddel is, is OSV de enige programmatuur dat voldoet aan de wet- en regelgeving. Dit betekent dat OSV nog gebruikt moet kunnen worden zolang het nieuwe digitale hulpmiddel er niet is. Hierbij kan onderscheid worden gemaakt tussen een OSV "plankversie" (huidige OSV zonder doorontwikkeling voor als er versneld Tweede Kamer verkiezingen zijn) en een verbeterde versie van OSV. Dit vereist allereerst dat de Staat het contract verlengt met de leverancier/onderhouder van OSV. BZK neemt hiervoor het initiatief. Het contract zal worden verlengd tot juli 2022. Om te komen tot een verbeterde versie van OSV heeft BZK het initiatief genomen om met de leverancier te verkennen enkele technische kwetsbaarheden aan OSV aan te pakken. Medio augustus is er een beslissingnotitie waarover BZK het gesprek zal voeren met VNG en Kiesraad. Verbeteringen in OSV zouden dan voor de herindelingsverkiezingen van november 2020 gerealiseerd moeten zijn. In de OSV vangnet zal de beoogde wetgeving 2021 bevatten. BZK is bezig met een notitie op welke wijze digitale overdracht plaats gaat vinden in 2021. Deadline is halverwege augustus. De verbeterde versie OSV is bruikbaar voor de herindelingsverkiezingen van 2020 en 2021, de Tweede Kamer verkiezingen 2021 en de gemeenteraad 2022. Dan loopt het contract af en dit is de uiterlijke datum wanneer het nieuwe Digitaal Hulpmiddel Uitslagberekening gereed moet zijn.
- De aanwezigen achten het heroïsch en onaannemelijk te veronderstellen dat het nieuw digitaal hulpmiddel voor de gemeentelijke herverdelingen in 2021 en de TK verkiezingen in 2021 gereed is. Dit is nog wel het beeld in de Tweede Kamer. Kort na het zomerreces zal de Kamer worden geïnformeerd over een nieuwe planning rond het nieuwe digitale hulpmiddel(len), over de te verrichten stappen rond OSV vangnet en zal worden aangegeven dat de komende verkiezingen nog met OSV verricht zullen moeten worden. De programmadirecteur levert input die als onderbouwing meegestuurd kan worden over de onaannemelijkheid dat het nieuwe digitaal hulpmiddel gereed is voor TK 2021. Deadline halverwege augustus.

- Betrouwbaarheid van een hulpmiddel (zoals het huidige OSV) wordt niet alleen bepaald door de software, maar ook door de processen hier om heen. Omdat bij de komende geplande verkiezingen OSV vangnet gebruikt zal worden, is het verstandig te beoordelen of er aanvullende mitigerende maatregelen mogelijk zijn. De Kiesraad (5.1.2.e) neemt hiervoor het initiatief en betreft BZK en VNG hier bij.
- De aanpassing rond de beoogde wetgeving van 2021 voor verbeteringen in de vaststelling verkiezingsuitslag vindt plaats onder regie van BZK. Belangrijke aanpassingen zijn dat het centraal stembureau kan "vragen" (dwingend) aan GSB om fouten in het stem- en telproces te herstellen (terugverwijzen), de mogelijkheid te creëren opnieuw te tellen en de tijd voor vaststelling van de uitslag te vergroten van 8 naar 13 dagen. In het wetsvoorstel is verwerkt dat digitale overdracht van de uitslag plaats zal moeten vinden. De planning is er op gericht om net na het zomerreces het wetsvoorstel naar de RvS te sturen. De RvS heeft gemiddeld drie maanden nodig. De vervolgplanning hangt af van het dictum.
- Voor het bepalen van de rol en verantwoordelijkheid voor en het programma van eisen van de digitale hulpmiddelen (in brede zin des woords, zie eerder) zal het verkiezingsproces worden opgedeeld in fasen, te weten: Bepalen kiesgerechtigdheid en kandidaatstelling -> Voorbereiding stemming -> Stemming -> Stemopneming -> Berekening uitslag -> Uitslagvaststelling en zeteltoedeling -> Toelating leden. Opzetten driedimensionale matrix, het per onderdeel in de fasering wordt aangegeven wie verantwoordelijk is en welke digitale middelen er gebruikt (gaan) worden. De programmadirecteur maakt hiervoor een opzet.
- Per fase wordt stil gestaan bij of en zo ja wat de eisen zijn voor processen en procedures, apparatuur, programmatuur en (digitale) infrastructuur (waaronder ook de gebruikte netwerken). De op te stellen scenario's worden beoordeeld aan de hand van de mate van BR controleerbaarheid, integriteit en betrouwbaarheid, onafhankelijkheid, waarborgen stemvrijheid en stemgeheim en uitvoerbaarheid. In de wet wordt proportionaliteit als maatstaf gehanteerd en is een beleid analytische toets een handig hulpmiddel.

BR



○

BR

○

•

BR

- De stuurgroep vergadert minimaal 1 maal per maand. Minimaal 2 keer per jaar bespreken de directeur-generaal BRW, de voorzitter van de Kiesraad en de algemeen directeur van de VNG de voortgang van de Transitie en eventuele knelpunten die zich daarbij voordoen. Bij het bestaande bestuurlijke overleg tussen VNG en BZK Democratie en Bestuur wordt de voortgang van de transitie geagendeerd. Bij dit agendapunt zal ook de voorzitter van de Kiesraad worden uitgenodigd. De programmadirecteur treedt in overleg met VNG over hoe bestuurders van gemeenten verder betrokken zullen worden bij het transitieproces.
- De programmadirecteur stelt voor half juli een plan van aanpak op waarbij hij in gaat op de structuur, de te verrichten werkzaamheden (met verdeling wie doet wat) en de planning. De stuurgroep zal dit plan van aanpak bespreken en vaststellen medio augustus.

AD, 12 juli 2019

Bijlage 2 Mitigerende maatregelen en urgent onderhoud aan OSV

In het briefadvies van de Verkenner wordt (terecht) gesteld dat “Het proces van wetswijziging voor verantwoordelijkheden en bevoegdheden over het gebruik van digitale middelen in het verkiezingsproces, inclusief het herontwerp van de governance en het opnieuw beleggen van taken en bevoegdheden tussen partijen, is er een van lange adem”. Tegelijkertijd lijkt deze tijd te ontbreken. Er zijn immers verkiezingen in 2021. Uit de eerste inventarisatie van de Programmadirecteur transitie en uit de startsessie komt naar voren dat het onaannemelijk is dat het nieuwe digitale hulpmiddel voor de gemeentelijke herverdelingen in 2021 en de TK-verkiezingen in 2021 gereed is. De Tweede Kamer zal hierover eind augustus worden geïnformeerd.

Bij alle partijen is er behoefte om gebruik te maken van programmatuur voor het vaststellen van de uitslag en van de zeteltoedeling. Op dit moment is de bestaande Ondersteunende Software Verkiezingen (OSV) de enige programmatuur die voldoet aan de wet- en regelgeving. Dit betekent dat OSV nog gebruikt moet kunnen worden zolang het nieuwe digitale hulpmiddel er niet is. Hierbij kan onderscheid worden gemaakt tussen een OSV “plankversie” (huidige OSV zonder het urgente onderhoud aan OSV voor als er versneld Tweede Kamerverkiezingen zijn) en een verbeterde versie van OSV. Dit vereist allereerst dat de Staat het contract verlengt met de leverancier/onderhouder van OSV. BZK neemt hiervoor het initiatief.

Om te komen tot een verbeterde versie van OSV heeft BZK het initiatief genomen om met de leverancier te verkennen enkele technische kwetsbaarheden aan OSV aan te pakken. Medio augustus is er een beslisnotitie waarover BZK het gesprek zal voeren met VNG en Kiesraad. Verbeteringen in OSV zouden dan voor de herindelingsverkiezingen van november 2020 gerealiseerd moeten zijn. De verbeteringen aan OSV maken geen deel uit van de transitie.

In de startsessie heeft BZK aangegeven digitale overdracht bij de bestaande infrastructuur weer mogelijk te maken. Dit maakt geen deel uit van deze transitie.

De betrouwbaarheid van een hulpmiddel (zoals het huidige OSV) wordt niet alleen bepaald door de software, maar ook door de processen hieromheen. Omdat bij de komende geplande verkiezingen OSV gebruikt zal worden, is het verstandig te beoordelen of er aanvullende mitigerende maatregelen mogelijk zijn. In de startsessie is afgesproken dat de Kiesraad hiervoor het initiatief neemt en BZK, VNG en NVVB hierbij betreft. Besluitvorming hierover zal in november in de stuurgroep plaatsvinden.



TE DOORLOPEN STAPPEN



Fox rapporten	Fox memo	OSV JIRA	Bevinding	Origineel Risico	Huidig Risico	Originele Status	Status na hertest Q4 2019	Huidige opmerkingen	Verwijzing
11			Niet ondersteunde software in gebruik Unsupported and old Jboss and Java SE software used	GEMIDDELD	GEMIDDELD	Deels opgelost	niet getest		Onderzoek Fox-IT 2017, bevinding 2 Security-assessment-of-Dutch-election-software-OSV, par. 4.1.4 (p. 29)
2			Stand-alone OSV installation is risky	LAAG	LAAG	Deels opgelost	niet getest		Security-assessment-of-Dutch-election-software-OSV, par. 4.1.7 (p. 35)
14			Transport door middel van USB-sticks	LAAG	LAAG	Deels opgelost	niet getest		Onderzoek Fox-IT 2017, bevinding 6
25			Incomplete source code and unsigned binary code	LAAG	LAAG	Deels opgelost	niet getest		Onderzoek VUsec, par. 6, issue 1
	5 OSV-2001		Improve protection against XSS (OSV P4 and P5)	-	LAAG	Deels opgelost	niet getest		MEMO_Kiesraad_PR180188_Hertest_2019Q2_1_0
								Kan nog steeds omzeild worden. Let wel, de implementatie van additionele autorisatie controles maakt deze maatregel minder relevant.	RAP_Kiesraad_PR180188_Beviligingsonderzoek OSV-PUBLIC
5			HMAC-controle is te omzeilen	HOOG	LAAG	Deels opgelost	Deels opgelost		Security-assessment-of-Dutch-election-software-OSV, par. 4.1.3 (p. 26)
1			Unnecessary ports are opened by Java	LAAG	LAAG	Gemittigeerd	Gemittigeerd		Onderzoek Fox-IT 2017, bevinding 11, sub 4
19			Overige tekortkomingen OSV	GEMIDDELD	LAAG	Gemittigeerd	Gemittigeerd		
	1 OSV-2009		Prevent showing stacktrace and server info to the user (OSV P4 and P5)	-	-	Deels opgelost	Opgelost	Enkel generieke meldingen worden getoond.	MEMO_Kiesraad_PR180188_Hertest_2019Q2_1_0
	10 OSV-2122		Privilege escalation vulnerability (second HMAC bypass)	-	-	Deels opgelost	Opgelost	Nieuw autorisatiemodel lijkt goed te werken	MEMO_Kiesraad_PR180188_Hertest_2019Q2_1_0
6			Onvoldoende autorisatiecontrole	HOOG	-	Niet opgelost	Opgelost		RAP_Kiesraad_PR180188_Beviligingsonderzoek OSV-PUBLIC
3			Persistent Cross-Site Scripting (XSS)	GEMIDDELD	-	Niet opgelost	Opgelost		RAP_Kiesraad_PR180188_Beviligingsonderzoek OSV-PUBLIC
2			Pagina's bereikbaar zonder authenticatie	LAAG	-	Niet opgelost	Opgelost	Direct ISP bestanden aanroepen controleert autorisatie	RAP_Kiesraad_PR180188_Beviligingsonderzoek OSV-PUBLIC
4			Gedetailleerde stack traces	LAAG	-	Niet opgelost	Opgelost	Enkel generieke meldingen worden getoond.	RAP_Kiesraad_PR180188_Beviligingsonderzoek OSV-PUBLIC
	6 OSV-2081		Verkiezingsleider is not allowed to enter polling station results (P4_P5B)	-	-	Niet opgelost	Opgelost	Strikt genomen opgelost, maar een verkiezingsleider kan altijd een extra account voor zichzelf aanmaken. Kan gemittigeerd worden door audit logs te controleren.	MEMO_Kiesraad_PR180188_Hertest_2019Q2_1_0
	7 OSV-2082		Verkiezingsleider is not allowed to enter municipality results (P4_H5B)	-	-	Niet opgelost	Opgelost	Strikt genomen opgelost, maar een verkiezingsleider kan altijd een extra account voor zichzelf aanmaken. Kan gemittigeerd worden door audit logs te controleren.	MEMO_Kiesraad_PR180188_Hertest_2019Q2_1_0
	8 OSV-2083		Verkiezingsleider is not allowed to enter kieskring results (P4_CS5B)	-	-	Niet opgelost	Opgelost	Strikt genomen opgelost, maar een verkiezingsleider kan altijd een extra account voor zichzelf aanmaken. Kan gemittigeerd worden door audit logs te controleren.	MEMO_Kiesraad_PR180188_Hertest_2019Q2_1_0
			OSV database isn't protected by a password	GEMIDDELD	-	Niet opgelost	Opgelost	Database is voorzien van wachtwoord. Let wel, dit kan door een aanval met de juiste voorbereiding omzeild worden, dit is inherent aan de opzet van de software.	Security-assessment-of-Dutch-election-software-OSV, par. 4.1.3 (p. 41)
			OSV database can be easily modified and votes can be changed	HOOG	-	Niet opgelost	Opgelost	Database is voorzien van wachtwoord. Let wel, dit kan door een aanval met de juiste voorbereiding omzeild worden, dit is inherent aan de opzet van de software.	Security-assessment-of-Dutch-election-software-OSV, par. 4.1.3 (p. 22)
			Modified EML files in archive directory on the server aren't detected	GEMIDDELD	-	Niet opgelost	Opgelost	OSV geeft een melding als de EML bestanden buiten de software om gewijzigd worden	Security-assessment-of-Dutch-election-software-OSV, par. 4.1.3 (p. 43)
1			Willekeurige bestanden kunnen geupload worden	GEMIDDELD	-	Opgelost			RAP_Kiesraad_PR180188_Beviligingsonderzoek OSV-PUBLIC
8			Gevoelige informatie in logbestand	GEMIDDELD	-	Opgelost			RAP_Kiesraad_PR180188_Beviligingsonderzoek OSV-PUBLIC
7			SHA256-hash controle kan omzeild worden	LAAG	-	Opgelost			RAP_Kiesraad_PR180188_Beviligingsonderzoek OSV-PUBLIC
3			SSL version 3.0 is detected	-	-	Opgelost			Security-assessment-of-Dutch-election-software-OSV, par. 4.1.14 (p. 40)
4			Password policy not enforced: one letter passwords possible	-	-	Opgelost			Security-assessment-of-Dutch-election-software-OSV, par. 4.1.22 (p. 51)
5			OSV can be run on an unencrypted HTTP connection on port 8080	-	-	Opgelost			Security-assessment-of-Dutch-election-software-OSV, par. 4.1.23 (p. 52)
6			jQuery security updates are missing	-	-	Opgelost			Security-assessment-of-Dutch-election-software-OSV, par. 4.1.29 (p. 59)
7			OSV database software Derby is missing security updates	-	-	Opgelost			Security-assessment-of-Dutch-election-software-OSV, par. 4.1.31 (p. 60)
8			Checking the integrity of the CD-ROM file is optional	-	-	Opgelost			Security-assessment-of-Dutch-election-software-OSV, par. 4.1.35 (p. 64)
9			Password hashing and login	-	-	Opgelost			Onderzoek VUsec, par. 6, issue 2
10			OSV-webapplicatie toegankelijk zonder verbodings-versleuteling	-	-	Opgelost			Onderzoek Fox-IT 2017, bevinding 1
12			Werkwijze wachtwoorden onveilig	-	-	Opgelost			Onderzoek Fox-IT 2017, bevinding 4
13			Verificatie integriteit EML-bestanden onvoldoende	-	-	Opgelost			Onderzoek Fox-IT 2017, bevinding 5
15			Integriteitscontrole OSV installatie-cd-rom kan omzeild worden	-	-	Opgelost			Onderzoek Fox-IT 2017, bevinding 7
16			XML External Entity Injection (XXE)	-	-	Opgelost			Onderzoek Fox-IT 2017, bevinding 8
17			Vier-ogen-principe wordt niet afgedwongen	-	-	Opgelost			Onderzoek Fox-IT 2017, bevinding 9
18			Niet geverifieerde externe software vereist	-	-	Opgelost			Onderzoek Fox-IT 2017, bevinding 10
20			Browser back button works even if user is logged out (HTML code can be cached)	-	-	Opgelost			Security-assessment-of-Dutch-election-software-OSV, par. 4.1.21 (p. 49)
21			No restriction on JavaScript usage via Content Security Policy	-	-	Opgelost			Security-assessment-of-Dutch-election-software-OSV, par. 4.1.27 (p. 52)
22			Integer overflow	-	-	Opgelost			Onderzoek VUsec, par. 5, issue 1
23			XML schema validation and application checks bypass	-	-	Opgelost			Onderzoek VUsec, par. 5, issue 2
24			Election definition and XSS	-	-	Opgelost			Onderzoek VUsec, par. 5, issue 4
26			Publication of e-mail addresses	-	-	Opgelost			Security-assessment-of-Dutch-election-software-OSV, par. 4.5.2 (p. 75)
27			Strict Transport Security isn't enabled	-	-	Opgelost			Security-assessment-of-Dutch-election-software-OSV, par. 4.1.24 (p. 54)
	2 OSV-2013		Prevent the access of other .jsp sites (OSV P4 and P5)	-	-	Opgelost			MEMO_Kiesraad_PR180188_Hertest_2019Q2_1_0
	3 OSV-2121		Control the authorization of a user if he/she opens a page or performs an action	-	-	Opgelost			MEMO_Kiesraad_PR180188_Hertest_2019Q2_1_0
	4 OSV-2149		Prevent access without authentication to pages	-	-	Opgelost			MEMO_Kiesraad_PR180188_Hertest_2019Q2_1_0
	9 OSV-2087		Prevent that result is set by single result file import in P4_H5B and P4_CS5B	-	-	Opgelost			MEMO_Kiesraad_PR180188_Hertest_2019Q2_1_0
	11 OSV-2159		OSV-2121 Control the authorization of a user if he/she performs an action	-	-	Opgelost			MEMO_Kiesraad_PR180188_Hertest_2019Q2_1_0

Fox rapporten	Fox memo	OSV JIRA	Bevinding	Origineel Risico	Huidig Risico	Originele Status	Status na hertest Q4 2019	Huidige opmerkingen	Verwijzing
11			Niet ondersteunde software in gebruik Unsupported and old Jboss and Java SE software used	GEMIDDELD	GEMIDDELD	Deels opgelost	niet getest		Onderzoek Fox-IT 2017, bevinding 2 Security-assessment-of-Dutch-election-software-OSV, par. 4.1.4 (p. 29)
2			Stand-alone OSV installation is risky	LAAG	LAAG	Deels opgelost	niet getest		Security-assessment-of-Dutch-election-software-OSV, par. 4.1.7 (p. 35)
14			Transport door middel van USB-sticks	LAAG	LAAG	Deels opgelost	niet getest		Onderzoek Fox-IT 2017, bevinding 6
25			Incomplete source code and unsigned binary code	LAAG	LAAG	Deels opgelost	niet getest		Onderzoek VUsec, par. 6, issue 1
	5 OSV-2001		Improve protection against XSS (OSV P4 and P5)	-	LAAG	Deels opgelost	niet getest		MEMO_Kiesraad_PR180188_Hertest_2019Q2_1_0
								Kan nog steeds omzeild worden. Let wel, de implementatie van additionele autorisatie controles maakt deze maatregel minder relevant.	RAP_Kiesraad_PR180188_Beviligingsonderzoek OSV-PUBLIC Security-assessment-of-Dutch-election-software-OSV, par. 4.1.3 (p. 26)
5			HMAC-controle is te omzeilen	HOOG	LAAG	Deels opgelost	Deels opgelost		Onderzoek Fox-IT 2017, bevinding 11, sub 4
1			Unnecessary ports are opened by Java	LAAG	LAAG	Gemitigeerd	Gemitigeerd		
19			Overige tekortkomingen OSV	GEMIDDELD	LAAG	Gemitigeerd	Gemitigeerd		
	1 OSV-2009		Prevent showing stacktrace and server info to the user (OSV P4 and P5)	-	-	Deels opgelost	Opgelost	Enkel generieke meldingen worden getoond.	MEMO_Kiesraad_PR180188_Hertest_2019Q2_1_0
	10 OSV-2122		Privilege escalation vulnerability (second HMAC bypass)	-	-	Deels opgelost	Opgelost	Nieuw autorisatiemodel lijkt goed te werken	MEMO_Kiesraad_PR180188_Hertest_2019Q2_1_0 RAP_Kiesraad_PR180188_Beviligingsonderzoek OSV-PUBLIC
6			Onvoldoende autorisatiecontrole	HOOG	-	Niet opgelost	Opgelost		RAP_Kiesraad_PR180188_Beviligingsonderzoek OSV-PUBLIC
3			Persistent Cross-Site Scripting (XSS)	GEMIDDELD	-	Niet opgelost	Opgelost		RAP_Kiesraad_PR180188_Beviligingsonderzoek OSV-PUBLIC
2			Pagina's bereikbaar zonder authenticatie	LAAG	-	Niet opgelost	Opgelost	Direct ISP bestanden aanroepen controleert autorisatie	RAP_Kiesraad_PR180188_Beviligingsonderzoek OSV-PUBLIC
4			Gedetailleerde stack traces	LAAG	-	Niet opgelost	Opgelost	Enkel generieke meldingen worden getoond.	RAP_Kiesraad_PR180188_Beviligingsonderzoek OSV-PUBLIC
	6 OSV-2081		Verkiezingsleider is not allowed to enter polling station results (P4_P5B)	-	-	Niet opgelost	Opgelost	Strikt genomen opgelost, maar een verkiezingsleider kan altijd een extra account voor zichzelf aanmaken. Kan gemitigeerd worden door audit logs te controleren.	MEMO_Kiesraad_PR180188_Hertest_2019Q2_1_0
	7 OSV-2082		Verkiezingsleider is not allowed to enter municipality results (P4_H5B)	-	-	Niet opgelost	Opgelost	Strikt genomen opgelost, maar een verkiezingsleider kan altijd een extra account voor zichzelf aanmaken. Kan gemitigeerd worden door audit logs te controleren.	MEMO_Kiesraad_PR180188_Hertest_2019Q2_1_0
	8 OSV-2083		Verkiezingsleider is not allowed to enter kieskring results (P4_C5B)	-	-	Niet opgelost	Opgelost	Strikt genomen opgelost, maar een verkiezingsleider kan altijd een extra account voor zichzelf aanmaken. Kan gemitigeerd worden door audit logs te controleren.	MEMO_Kiesraad_PR180188_Hertest_2019Q2_1_0
1			Willekeurige bestanden kunnen geupload worden	GEMIDDELD	-	Opgelost			RAP_Kiesraad_PR180188_Beviligingsonderzoek OSV-PUBLIC
8			Gevoelige informatie in logbestand	GEMIDDELD	-	Opgelost			RAP_Kiesraad_PR180188_Beviligingsonderzoek OSV-PUBLIC
7			SHA256-hash controle kan omzeild worden	LAAG	-	Opgelost			RAP_Kiesraad_PR180188_Beviligingsonderzoek OSV-PUBLIC
3			SSL version 3.0 is detected	-	-	Opgelost			Security-assessment-of-Dutch-election-software-OSV, par. 4.1.14 (p. 40)
4			Password policy not enforced: one letter passwords possible	-	-	Opgelost			Security-assessment-of-Dutch-election-software-OSV, par. 4.1.22 (p. 51)
5			OSV can be run on an unencrypted HTTP connection on port 8080	-	-	Opgelost			Security-assessment-of-Dutch-election-software-OSV, par. 4.1.23 (p. 52)
6			jQuery security updates are missing	-	-	Opgelost			Security-assessment-of-Dutch-election-software-OSV, par. 4.1.29 (p. 59)
7			OSV database software Derby is missing security updates	-	-	Opgelost			Security-assessment-of-Dutch-election-software-OSV, par. 4.1.31 (p. 60)
8			Checking the integrity of the CD-ROM file is optional	-	-	Opgelost			Security-assessment-of-Dutch-election-software-OSV, par. 4.1.35 (p. 64)
9			Password hashing and login	-	-	Opgelost			Onderzoek VUsec, par. 6, issue 2
10			OSV-webapplicatie toegankelijk zonder verbodings-versleuteling	-	-	Opgelost			Onderzoek Fox-IT 2017, bevinding 1
12			Werkwijze wachtwoorden onveilig	-	-	Opgelost			Onderzoek Fox-IT 2017, bevinding 4
13			Verificatie integriteit EML-bestanden onvoldoende	-	-	Opgelost			Onderzoek Fox-IT 2017, bevinding 5
15			Integriteitscontrole OSV installatie-cd-rom kan omzeild worden	-	-	Opgelost			Onderzoek Fox-IT 2017, bevinding 7
16			XML External Entity Injection (XXE)	-	-	Opgelost			Onderzoek Fox-IT 2017, bevinding 8
17			Vier-ogen-principe wordt niet afgedwongen	-	-	Opgelost			Onderzoek Fox-IT 2017, bevinding 9
18			Niet geverifieerde externe software vereist	-	-	Opgelost			Onderzoek Fox-IT 2017, bevinding 10
20			Browser back button works even if user is logged out (HTML code can be cached)	-	-	Opgelost			Security-assessment-of-Dutch-election-software-OSV, par. 4.1.21 (p. 49)
21			No restriction on JavaScript usage via Content Security Policy	-	-	Opgelost			Security-assessment-of-Dutch-election-software-OSV, par. 4.1.27 (p. 52)
22			Integer overflow	-	-	Opgelost			Onderzoek VUsec, par. 5, issue 1
23			XML schema validation and application checks bypass	-	-	Opgelost			Onderzoek VUsec, par. 5, issue 2
24			Election definition and XSS	-	-	Opgelost			Onderzoek VUsec, par. 5, issue 4
26			Publication of e-mail addresses	-	-	Opgelost			Security-assessment-of-Dutch-election-software-OSV, par. 4.5.2 (p. 75)
27			Strict Transport Security isn't enabled	-	-	Opgelost			Security-assessment-of-Dutch-election-software-OSV, par. 4.1.24 (p. 54)
	2 OSV-2013		Prevent the access of other .jsp sites (OSV P4 and P5)	-	-	Opgelost			MEMO_Kiesraad_PR180188_Hertest_2019Q2_1_0
	3 OSV-2121		Control the authorization of a user if he/she opens a page or performs an action	-	-	Opgelost			MEMO_Kiesraad_PR180188_Hertest_2019Q2_1_0
	4 OSV-2149		Prevent access without authentication to pages	-	-	Opgelost			MEMO_Kiesraad_PR180188_Hertest_2019Q2_1_0
	9 OSV-2087		Prevent that result is set by single result file import in P4_H5B and P4_C5B	-	-	Opgelost			MEMO_Kiesraad_PR180188_Hertest_2019Q2_1_0
	11 OSV-2159		OSV-2121 Control the authorization of a user if he/she performs an action	-	-	Opgelost			MEMO_Kiesraad_PR180188_Hertest_2019Q2_1_0

Fox rapport 14-3-19	Fox memo 23-4-19	Bevinding	Verwijzing	Omschrijving + Opmerkingen	Description	OSV JIRA	Status na hertest Q3 2019
		Modified EML files in archive directory on the server aren't detected	5.1.2.e par. 4.1.18 (p. 43)	OSV software controleert niet of gegenereerde EML files nadien op de server worden aangepast door een hacker. Laat OSV continu controleren of de inhoud van de op de server opgeslagen EML bestanden buiten OSV om wordt gewijzigd.	"OSV software does not check whether generated EML files on the server are subsequently modified by a hacker. Let OSV continuously check if the content of the EML files stored on the server is changed outside of OSV. "	OSV-2000	Opgelost, let wel dit kan door een aanvaller met de juiste voorbereiding omzeild worden, dit is inherent aan de opzet van de software.
bevinding 3. nieuw	5. Deels opgelost	Persistent Cross-Site Scripting (XSS)	Rapport Fox-IT 2019, bevinding 3	XSS kan gebruikt worden om de bij een gebruiker getoonde website te veranderen of Javascript code uit te voeren op de computer van een gebruiker. Het gevolg daarvan is dat het lijkt alsof deze code afkomstig is van OSV. In tegenstelling tot een niet persistent Cross-Site Scripting (XSS) aanval wordt bij deze aanval de code op de server opgeslagen. Het risico is dat de code elke keer opnieuw aan de betreffende gebruiker getoond wordt. Mogelijk wordt de betreffende code ook getoond en uitgevoerd door andere gebruikers, bijvoorbeeld door een verkiezingsleider.	XSS can be used to change the website displayed by a user or to execute JavaScript code on a user's computer. As a result, it appears that this code is from OSV. Unlike a non-persistent Cross-Site Scripting (XSS) attack, the code stores the code on the server. The risk is that the code is shown to the relevant user every time. The relevant code may also be displayed and executed by other users, for example by an election leader.	OSV-2001	HTML bestanden in de export map kunnen niet meer aangeroepen worden
bevinding 4. nieuw	1. Deels opgelost	Gedetailleerde stack traces	Rapport Fox-IT 2019, bevinding 4	Kennis van de achterliggende structuur van de webapplicatie kan een aanvaller helpen om de webapplicatie en de systemen in kaart te brengen en zo een verdere aanval voor te bereiden.		OSV-2161 OSV-2009 OSV-1962	Enkel generieke meldingen worden getoond.
		OSV database can be easily modified and votes can be changed	5.1.2.e par. 4.1.2 (p. 22)	De door OSV gebruikte database is niet voorzien van een wachtwoord. Een persoon die toegang heeft tot de OSV programma bestanden op de OSV server computer kan als 'relatie' eenvoudig toegang krijgen tot de database, met als mogelijk gevolg het aanpassen van (uitslag)gegevens in de database. Zie ook nummer 53	The database used by OSV is not provided with a password. A person who has access to the OSV program files on the OSV server computer can easily gain access to the database as a "relation", with the possible consequence of adjusting (result) data in the database.	OSV-1994	Opgelost, database is voorzien van wachtwoord, let wel dit kan door een aanvaller met de juiste voorbereiding omzeild worden, dit is inherent aan de opzet van de software.
	6. Niet opgelost	OSV database isn't protected by a password	5.1.2.e par. 4.1.16 (p. 41)	OSV database is niet beveiligd met wachtwoord	OSV database is not protected with password	OSV-1994	Opgelost, database is voorzien van wachtwoord, let wel dit kan door een aanvaller met de juiste voorbereiding omzeild worden, dit is inherent aan de opzet van de software.
	7. Niet opgelost	Verkiezingsleider is not allowed to enter polling station results (P4_PSB)				OSV-2081	Strikt genomen opgelost, maar een verkiezingsleider kan altijd een extra account voor zichzelf aanmaken. Kan gemitigeerd worden door audit logs te controleren.
	8. Niet opgelost	Verkiezingsleider is not allowed to enter municipality results (P4_HSB)				OSV-2082	Strikt genomen opgelost, maar een verkiezingsleider kan altijd een extra account voor zichzelf aanmaken. Kan gemitigeerd worden door audit logs te controleren.
	8. Niet opgelost	Verkiezingsleider is not allowed to enter kieskring results (P4_CSB)				OSV-2083	Strikt genomen opgelost, maar een verkiezingsleider kan altijd een extra account voor zichzelf aanmaken. Kan gemitigeerd worden door audit logs te controleren.
bevinding 5. nieuw	10. deels opgelost	HMAC-controle is te omzeilen	Rapport Fox-IT 2019, bevinding 5	De HMAC is een beveiligingsmethode in OSV. Door deze te omzeilen wordt een belangrijke beveiligingsmaatregel onklaar gemaakt waarmee het voor aanvallers mogelijk wordt andere aanvallen uit te voeren of om bepaalde processen te negeren.	The HMAC is a security method in OSV. Bypassing this, an important security measure is disabled, making it possible for attackers to perform other attacks or to ignore certain processes.	OSV-2122 OSV-2098	Kan nog steeds omzeild worden. Let wel, de implementatie van additionele autorisatie controles maakt deze maatregel minder relevant.