Versie 1.0 / 9 november 2020

Verkiezingen en optelcomputers: een oproep tot onafhankelijke controle in het belang van betrouwbare verkiezingen

Stichting Tegen Hackbare Verkiezingen

Veilinghavenkade 145
3521AT Utrecht
www.hackbareverkiezingen.nl

Samenvatting

Overheid vertrouwt op hackbare computers om in maart 2021 de Tweede Kamer-verkiezingsuitslag uit te rekenen.

Op 17 maart 2021 zijn de Tweede Kamerverkiezingen. Er wordt met potlood en papier gestemd in tussen de 9.000 en 10.000 stembureaus. 's Avonds worden alle stemmen handmatig geteld in stembureaus en de totalen opgeschreven in een proces-verbaal. De processen-verbaal worden naar de burgemeester gebracht. Vervolgens typen ambtenaren de processen-verbaal over in een computerprogramma (genaamd Ondersteunende Software Verkiezingen 2020). Wanneer dat klaar is wordt de uitslag geprint. Deze uitdraai wordt door de burgemeester ondertekend en is daarmee definitief in een gemeente.

De Kiesraad*, het ministerie van Binnenlandse Zaken (BZK) en gemeentes vinden het niet nodig om de totalen op de verschillende niveaus te verifiëren, bijvoorbeeld door handmatig stemtotalen uit processen-verbaal bij elkaar op tellen en het resultaat te vergelijken met de uitslag die door de computer werd berekend. Terwijl alleen op die manier mogelijke hacks en manipulaties aan het licht komen. Een belangrijke reden waarom de Kiesraad en BZK het niet nodig vindt om ook handmatig op te tellen is dat de optelcomputers niet op internet zijn aangesloten.

Buitenlandse inlichtingendiensten hebben echter geavanceerde hackmogelijkheden, veel budget, en goed doordachte plannen om zelfs toegang tot de meest afgeschermde militaire computernetwerken te krijgen als ze dit echt willen. Buitenlandse inlichtingendiensten beschikken over de technische vaardigheden om de uitslag te beïnvloeden door bij de gemeentes in te breken. Daarnaast bestaat altijd de mogelijkheid dat een opportunistische, afgeperste of omgekochte gemeentelijke systeembeheerder eigenhandig en ongezien de software op de optelcomputers aanpast om met de uitslag te frauderen.

Stichting Tegen Hackbare Verkiezingen is van mening dat computers niet veilig genoeg zijn om erop te vertrouwen bij een verkiezing, rekening houdend met mogelijke dreigingen en de ongekende impact van een gehackte verkiezing. Computers kunnen worden gehackt, zeker als de belangen groot zijn. Een verkiezing hoort zo transparant, robuust en weerbaar te zijn dat deze bestand is tegen externe inmenging (zelfs als het gaat om buitenlandse inlichtingendiensten), maar ook tegen inmenging van binnenuit.

Om twijfel over de uitslag weg te nemen moet onafhankelijke verificatie van de resultaten verplicht worden. De kosten om de optelling te verifiëren, bijvoorbeeld door handmatig op te tellen of te laten verifiëren door derden, vallen in het niet bij de totale kosten en impact van een gehackte verkiezing. Het is dan ook een *no-brainer* om deze maatregel door te voeren. De stichting wil dat een verificatie van de computeruitslagen wordt ingevoerd, zodat onze democratie weerbaar wordt tegen hedendaagse dreigingen en risico's.

***Update:** In een reactie op 9 november 2020, laat de Kiesraad weten dat zij een natelling van de computertotalen op alle niveaus inmiddels ook noodzakelijk acht.

Inhoudsopgave

1 Introductie

Deze rapportage en analyse is geschreven door Stichting Tegen Hackbare Verkiezingen. Deze stichting is op 2 oktober 2020 opgericht en vertegenwoordigt een groep bezorgde IT-beveiligingsexperts, ethische hackers en hoogleraren cybersecurity. Zij zien dat de overheid nog steeds volledig op computers vertrouwt om de verkiezingsuitslag mee uit te rekenen op de Tweede Kamerverkiezingen op 17 maart 2021, ondanks het mogelijke risico van een gehackte uitslag.

Op 30 januari 2017 toonde RTL Nieuws in samenwerking met een ethisch hacker aan dat de verkiezingsuitslag makkelijk te hacken was. In de loop der jaren is er veel aandacht voor de aangetoonde problematiek geweest en ook het een en ander veranderd. Het is niet meer *makkelijk* om een uitslag te hacken, maar wel nog steeds mogelijk, en daarmee is de huidige situatie nog steeds onacceptabel.

De stichting wil de samenleving, Kiesraad[1], BZK, en gemeentes bewust maken van nut en noodzaak van een controle van de computeruitslagen door de stemtotalen uit de processen-verbaal van stembureaus bij elkaar op te tellen (handmatig of via een andere onafhankelijke verificatie), en te controleren of het resultaat overeenkomt met de door de computer berekende uitslag. Als die overeenkomen dan is de uitslag betrouwbaar. Wanneer de verificatie op alle niveaus wordt uitgevoerd, kunnen menselijke telfouten worden ondervangen en hebben hackers geen kans meer.

Daarnaast heeft de stichting zich tot doel gesteld om het bewustzijn in de samenleving te vergroten dat software niet vertrouwd kan worden in verkiezingsprocessen, en zeker niet om zonder grondige handmatige validatie de definitieve verkiezingsuitslag mee uit te rekenen. Software zou alleen gebruikt moeten worden om de handmatige of onafhankelijk uitgevoerde optellingen te valideren die leidend zouden moeten zijn.

De integriteit van een verkiezingsuitslag moet onweerlegbaar zijn en niet tot discussies leiden. Er is nu een hackrisico dat eenvoudig weggenomen kan worden door handmatig op te tellen.

[1] Update: In een reactie op 9 november 2020, laat de Kiesraad weten dat zij een natelling van de computertotalen op alle niveaus inmiddels ook noodzakelijk acht.

2 Hackbare computers berekenen Tweede Kamer-verkiezingsuitslag

Omdat stemcomputers onveilig bleken te zijn, verbood het kabinet in 2008 het gebruik hiervan. Sindsdien stemt Nederland weer met potlood en papier. Wel gebruikt de overheid sinds 2009 software om alle stemtotalen bij elkaar op te tellen en de verkiezingsuitslag uit te rekenen.

2.1 Berekening van de Tweede Kamer-verkiezingsuitslag

In Nederland verloopt een verkiezing als volgt. Zoals vrijwel iedereen weet, wordt tegenwoordig met potlood en papier gestemd in zo'n 10.000 stembureaus. Omdat wat daarna gebeurt niet bij iedereen bekend is, vatten we het hier samen[2].

Stembureaus (ca. 9.000 - 10.000x)
De stemmen worden op dezelfde dag in de avond en soms nacht handmatig geteld door stembureauleden en vastgelegd in een proces-verbaal (N10). Dit proces-verbaal wordt vervolgens naar het gemeentelijk centraal stembureau gebracht, wat regelmatig het stadhuis is. Tot zover het voor iedereen welbekende, transparante en robuuste proces.

Gemeentelijk Centraal Stembureau[3] (355x)
Wat weinig mensen echter weten, is dat op het 'Gemeentelijk Centraal Stembureau'[2] vervolgens een aantal ambtenaren klaar staan die alle stemmen per partij en voorkeurskandidaat invoeren in het computerprogramma Ondersteunende Software Verkiezingen (OSV2020-U):

1. Het gemeentelijk centraal stembureau verzamelt alle papieren processen-verbaal (N10) van stembureaus.
2. De stemtotalen worden vervolgens elk door twee personen overgetypt in OSV2020-U (vier-ogen controle).
3. Als alle processen-verbaal (N10) zijn ingevoerd, dan berekent OSV2020-U de gemeentelijke telling (de optelling).
4. Deze wordt vervolgens geprint (N11) en ondertekend door de voorzitter van het Gemeentelijk Centraal Stembureau (de burgemeester).
5. De ondertekende uitslag wordt vervolgens naar de Kieskring gebracht waar de gemeente onder valt.

[2] Stichting Tegen Hackbare Verkiezingen is de Kiesraad erkentelijk voor haar hulp bij het boven tafel krijgen van deze gegevens. De Kiesraad merkte hierbij op dat het precieze tijdschema nog onder voorbehoud is van een door te voeren wetswijziging.

[3] De term 'gemeentelijk centraal stembureau' wordt momenteel niet in de Kieswet gebruikt (men spreekt over 'de burgemeester'), maar voor het begrip van wat er op dit niveau gebeurt, is het handig om er expliciet een naam aan te geven. De voorgestelde wetswijziging die in de Kamer ligt zorgt inderdaad ook voor de instelling van een gemeentelijk stembureau.

Hoofdstembureau (20x)
In Nederland zijn er twintig Kieskringen. In iedere Kieskring wordt een Hoofdstembureau ingesteld. De hoofdstembureaus moeten de uitslagen van de verschillende gemeentes bij elkaar optellen:

1. Het hoofdstembureau van een Kieskring verzamelt alle papieren processen-verbaal (N11) van onderliggende gemeentes.
2. De stemtotalen worden vervolgens elk door twee personen overgetypt in OSV2020-U.
3. Als alle processen-verbaal zijn ingevoerd, dan berekent OSV2020-U de uitslag voor de Kieskring.
4. De uitslag wordt vervolgens geprint (O3) en ondertekend door de alle leden van het hoofdstembureau en naar het centraal stembureau gebracht.
5. Via een openbare zitting op 19 maart 2021 wordt de uitslag officieel bekendgemaakt, waar ook eventuele bezwaren tegen de uitslag officieel doorgegeven kunnen worden.
6. Het hoofdstembureau brengt tevens de processen-verbaal N10, de opgave N11 en eventuele waarnemersverslagen over naar de Tweede Kamer alsmede een afschrift van het proces-verbaal O3.

Centraal Stembureau (1x)
Bij landelijke verkiezingen treedt de Kiesraad op als Centraal Stembureau. Het Centraal Stembureaus is verantwoordelijk voor het vaststellen van de verkiezingsuitslag:

1. Het Centraal Stembureau ontvangt de kieskringtotalen (O3) van de twintig Hoofdstembureaus op papier.
2. De stemtotalen worden vervolgens elk door twee personen overgetypt in OSV2020-U.
3. Als alle uitslagen (O3) ingevoerd zijn, dan berekent OSV2020-U de uitslag voor Nederland.
4. Deze wordt vervolgens uitgeprint en ondertekend door alle leden van het Centraal Stembureau.
5. Via een openbare zitting wordt kort daarna de uitslag officieel bekendgemaakt (P22), waar ook eventuele bezwaren tegen de uitslag officieel doorgegeven kunnen worden.
6. De Kiesraad verstuurt de berekende verkiezingsuitslag (P22) door naar de huidige zittende Tweede Kamer ter acceptatie.
7. Als de Tweede Kamer de uitslag accepteert, dan is de uitslag onherroepelijk geworden.

Donderdag 25 maart 2021 is de dag waarop zittende leden van de Tweede Kamer aftreden. Drie maanden na de toelating van de gekozenen worden de verzegelde pakken met stembescheiden en processen-verbaal van de stembureaus vernietigd.

2.2 Sinds 2017 is bekend dat onveilige software wordt gebruikt

Op 30 januari 2017 maakte de onderzoeksredactie van RTL Nieuws bekend dat slecht beveiligde optelsoftware wordt gebruikt om de verkiezingsuitslag uit te rekenen en dat hackers met de uitslag kunnen frauderen. Minister Plasterk verbood de gemeentes toen de software nog te gebruiken. Omdat gemeentes geen alternatieve werkwijze hadden en de verkiezingen over enkele weken gepland stonden, werd de software toch maar wel ingezet. Met één uitzondering: de overdracht van stemtotalen via USB-sticks werd definitief geschrapt.

De software is de afgelopen 3,5 jaar veiliger gemaakt, maar nog steeds fundamenteel kwetsbaar voor hackaanvallen en manipulatie, omdat de computeroptellingen niet handmatig of anderszins onafhankelijk van de software worden geverifieerd.
Ook een 'veilig' en gecertificeerd computerprogramma is altijd manipuleerbaar binnen de omgeving waarin het draait. De harde schijf en het computergeheugen waarop het programma draait kunnen elk moment worden aangepast door malware die bijvoorbeeld in de officiële installatiebestanden of het besturingssysteem is geslopen, of later handmatig is toegevoegd aan de officiële setup.

2.3 Hoe gaan de verkiezingen in 2021 verlopen en waar zit de kwetsbaarheid?

Op woensdag 17 maart 2021 zijn de Tweede Kamerverkiezingen. Burgers kunnen hun stem met potlood op papier vastleggen. Aan het eind van de dag worden alle stemmen in het openbaar geteld door stembureauleden. Van deze telling en daarmee de stembureau-uitslag wordt een papieren proces-verbaal[4] opgemaakt en ondertekend op een openbare zitting. Deze wordt vervolgens naar het gemeentelijk centraal stembureau gebracht door de stembureauvoorzitter.

De volgende dag zit een team van ambtenaren klaar dat vervolgens alle ontvangen processen-verbaal overtypt in een computerprogramma genaamd Ondersteunende Software Verkiezingen 2020 (OSV2020-U). Als twee personen hetzelfde proces-verbaal exact overtypen (vier-ogen principe) dan worden de stemtotalen van het stembureau definitief in de database opgeslagen op de centrale computer. Die staat in een tijdelijk aangelegd offline computernetwerk van een klein aantal computers.

Aan het eind van de dag[5], drukt een ambtenaar op een knop, en OSV2020-U telt alle stemtotalen per partij en voorkeurskandidaat bij elkaar op en rekent vervolgens de uitslag uit. Die wordt geprint en ondertekend door de burgemeester. Op een publieke zitting wordt de uitslag bekend en definitief gemaakt.

Papieren proces-verbaal: gedigitaliseerd en niet meer naar omgekeken
De fundamentele kwetsbaarheid zit in het feit dat alle papieren processen-verbaal (tussen de 9.000 en 10.000 stuks) van stembureaus overgetypt worden door gemeenteambtenaren in het programma OSV2020-U dat in de meeste gevallen op Windows draait. Daarna gaat het papier de kluis in en er wordt verder niet meer naar omgekeken in het optelproces, *omdat het gedigitaliseerd is*. De computer berekent de uitslag en die wordt vertrouwd. Ambtenaren of externe partijen tellen in het formele proces geen enkel stemtotaal van stembureaus bij elkaar op[6].

[4] Een N10 proces-verbaal is een rechtsgeldig document waarop de uitslag van een stembureau staat. Deze is vaak zo'n twintig pagina's lang, omdat van iedere partij ook de stemtotalen per voorkeurskandidaten benoemd zijn.

[5] Of in sommige gemeentes in geval van problemen wettelijk gezien uiterlijk op vrijdag 19 maart 2021.

[6] Een aantal kleine uitzonderingen daargelaten.

2.4 Papieren processen-verbaal inzichtelijk voor burgers

Burgers kunnen enkele dagen na de verkiezing de papieren processen-verbaal van de stembureaus in hun gemeente onder begeleiding van een ambtenaar inzien op het gemeentehuis. Deze mogelijkheid geldt maar voor enkele dagen, totdat de verkiezingsuitslag bekend wordt gemaakt. Daarna gaan de papieren weer in de gemeentekluis[7]. Bij verkiezingen voor de Tweede Kamer gebeurt dit meestal op de maandag na de dag van stemming. Er kan dan gecontroleerd worden of de digitaal openbaar gemaakte documenten overeenkomen met de ter inzage gelegde stukken op het gemeentehuis.

2.5 10.000 processen-verbaal van stembureaus nu op Internet

Om bezorgde burgers tegemoet te komen, moeten alle 10.000 processen-verbaal (N10 en N11) van elk stembureau sinds 1 maart 2019 door elke gemeente op hun website worden gezet. Dit is enorme winst in transparantie en de controleerbaarheid van verkiezingen ten opzichte van voorgaande jaren, waarin het fotograferen of inscannen van processen-verbaal zelfs verboden was.

Het door gemeentes online zetten van processen-verbaal wordt overigens lang niet altijd, en soms ook niet op tijd gedaan, bleek vorig jaar bij de verkiezingen. De Kiesraad merkt hierover het volgende op:

- *"[..] De Kiesraad wijst erop dat op het moment dat het gemeentelijk stembureau zijn taken vervult, de processen-verbaal van de stembureaus nog niet openbaar zijn. Kiezers kunnen op dat moment dus niet zelf nagaan of deze goed leesbaar zijn of optelfouten bevatten. Kiezers kunnen tijdens de openbare zitting van het gemeentelijk stembureau kortom niet controleren of het gemeentelijk stembureau de stemtotalen correct heeft vastgesteld. Dat kunnen zij pas als het gemeentelijk stembureau zijn werkzaamheden heeft afgerond en de processen-verbaal van het gemeentelijk stembureau en de stembureaus openbaar zijn gemaakt. [..]*

  Kiezers kunnen tot vierentwintig uur voor aanvang van de openbare zitting van het centraal stembureau waarin het de verkiezingsuitslag officieel vaststelt, bij het centraal stembureau melding maken van vermeende fouten in de openbaar gemaakte en ter inzage gelegde processen-verbaal. [..]"

Er ligt een wetsvoorstel bij de Tweede Kamer dat de publicaties van processen-verbaal voorzien moeten zijn van een digitale handtekening. Zoals we verderop in dit document zullen betogen is het echter ook van belang dat het online zetten van de processen-verbaal overal op dezelfde manier en op dezelfde plaats gebeurt, zodat derden die de uitslagen willen controleren dat zonder onnodige extra zoekwerk kunnen doen. Ook vindt Stichting Tegen Hackbare Verkiezingen dat de stemtotalen in makkelijk te verwerken vorm zichtbaar moeten worden gemaakt, zodat iedereen (1) kan zien dat de totalen overeenkomen met die op de processen-verbaal, en (2) deze totalen kan kopiëren en thuis kan optellen, bijvoorbeeld met een spreadsheet.

[7] Ter beeldvorming van de omvang: gemeente Utrecht heeft ongeveer 180 stembureaus die bij elkaar twee verhuisdozen vol aan papieren processen-verbaal opleveren.

2.6 Vergroting transparantie en controleerbaarheid

Minister Ollongren informeert gemeentes op 11 december 2018 in een circulaire over deze wetswijziging:

- *"[..] Dat nu ook de processen-verbaal N10 en de opgave N11 elektronisch openbaar worden gemaakt, heeft als doel een vergroting van de transparantie en controleerbaarheid van het verkiezingsproces. Iedere belangstellende kan op deze manier nagaan hoe de verkiezingsuitslag tot stand is gekomen. [..] Ik attendeer met nadruk op het belang van de digitale openbaarmaking en de terinzagelegging. Ik verzoek u dus dringend om zich strikt te houden aan de nieuwe wettelijke regels. De kiezer wordt daarmee beter in staat gesteld om het proces van uitslagvaststelling te volgen."*

2.7 Burgers kunnen computeruitslag zelf narekenen, overheid vindt dat niet nodig

Omdat alle stemtotalen uit processen-verbaal worden overgetypt in OSV2020-U, vindt de Kiesraad[8] dat ambtenaren zelf niet handmatig stemtotalen bij elkaar op hoeven te tellen. Dit maakt daarom ook geen deel uit van het formele proces. Gemeentes en de Kiesraad zijn van mening dat de reeds genomen beveiligingsmaatregelen afdoende zijn. Voorbeelden van deze maatregelen zijn de beter beveiligde software (OSV2020-U) die niet op internet mag worden aangesloten, en processen-verbaal van stembureaus die nu op internet gezet moeten worden.

Een paar dagen na de uitslag zou verwacht mogen worden dat alle gemeentes de processen-verbaal van de stembureaus in hun gemeente op hun website hebben geplaatst. Burgers kunnen dan zelf handmatig stemtotalen bij elkaar gaan optellen om de resultaten te vergelijken met de officiële (computer)uitslag. Als een afwijking wordt geconstateerd, dan zou dit kunnen wijzen op een gehackte optelcomputer.

Het is belangrijk om eventuele afwijkingen vast te stellen voordat de verkiezingsuitslag definitief wordt gemaakt door de Tweede Kamer. Serieuze en gevalideerde afwijkingen kunnen tijdens de openbare zitting op maandag 22 maart 2021 kenbaar worden gemaakt. De voorzitter van het centraal stembureau (de Kiesraad) zal dan het aangemelde bezwaar tegen de uitslag opnemen als aantekening op het proces-verbaal dat van de zitting wordt opgemaakt. Dat kan ertoe leiden dat de uitslag nader wordt onderzocht door de Kiesraad of de Tweede Kamer voordat deze definitief wordt gemaakt.

2.8 Drie maanden de tijd

De verkiezingsuitslag is definitief nadat deze is vastgesteld door de Kiesraad op 22 maart 2021 én daarna is geaccepteerd door de Tweede Kamer.

Drie maanden na de verkiezing moeten gemeentes volgens de Kieswet alle papieren processen-verbaal vernietigen. Het idee daarvan is dat de uitslag dan onherroepelijk wordt, doordat alle bewijsstukken zijn

[8] Update: In een reactie op 9 november 2020, laat de Kiesraad weten dat zij een natelling van de computertotalen op alle niveaus inmiddels ook noodzakelijk acht.

vernietigd. Dat zou de legitimiteit van de gekozen regering versterken. Niemand kan tenslotte meer kan bewijzen dat de uitslag niet klopt.

Het is dus goed om te weten dat er na het stemmen maar drie maanden de tijd is om te bewijzen dat de computeruitslag niet klopt. Als binnen die tijd een afwijking wordt geconstateerd tussen de handmatige optelling en de computeruitslag, kunnen namelijk altijd nog de originele processen-verbaal uit de gemeentekluis gehaald worden die het verschil kunnen verklaren (of bevestigen dat een optelcomputer is gehackt).

3 Waarom zijn computers niet te vertrouwen in verkiezingen?

Computers zijn voor veel alledaagse zaken te vertrouwen, zoals internetbankieren en zakendoen met de overheid via DigiD. Toch zijn computers niet veilig genoeg om een verkiezingsuitslag mee uit te rekenen. Dat zit in het feit dat moderne computers complexe hardware en zeer veel software nodig hebben om standaard te kunnen functioneren. Naast het operating systeem (bijvoorbeeld Windows, Linux, of macOS) gaat het om drivers en om firmware op allerlei componenten. Computers zijn een *black box* geworden waarvan we allang niet meer precies weten hoe deze werkt en Microsoft en andere softwareleveranciers zijn hier lang niet altijd open over.

Het hele verkiezingsproces tot en met de ondertekening van het papieren proces-verbaal in een stembureau is robuust en doordacht, en in de Kieswet goed verankerd. Maar daarna volgt de digitaliseringsslag.

Alle stemtotalen worden de dag na de verkiezingen door ambtenaren overgetypt in een computerprogramma dat door een Duits bedrijf[9] wordt ontwikkeld. De Kiesraad stuurt de software op CD-ROM per post naar gemeentes. Gemeentes mogen zelf kiezen of ze dit programma op Windows, Linux of macOS installeren in hun eigen in te richten netwerk van (meestal) laptops. Veel gemeentes kiezen daarbij voor Windows, omdat hun eigen laptops en kennis daarop ingericht zijn.

Malware op laptops of fysieke toegang tot computers in de weken en maanden voor de verkiezing, vormen een reële bedreiging voor de integriteit en werking van de optelsoftware. Een hacker kan de werking beïnvloeden van de software: dan lijkt alles aan de voorkant te kloppen, maar als de definitieve uitslag wordt geprint, dan wordt toch de frauduleus aangepaste uitslag getoond.

[9] IVU Elect GmbH, dat in mei 2020 is overgenomen door vote iT GmbH

4 Wie zouden de optelcomputers kunnen hacken?

Een verkiezing kan kwetsbaar zijn voor manipulatie. Dit wil niet zeggen dat er altijd daadwerkelijk misbruik van wordt gemaakt. Daarvoor moet er ook een dreiging zijn. Deze dreiging kan van meerdere kanten komen. In het geval van de optelcomputers kunnen statelijke actoren en andere organisaties de hardware en software van de computersystemen hacken. Hetzelfde geldt voor de gemeentelijke systeembeheerder. Wat betreft motivatie geldt dat buitenlandse overheden baat kunnen hebben bij het manipuleren van Nederlandse verkiezingen.

Ook kan het in het belang zijn van binnenlandse en buitenlandse actoren om alleen al twijfel te zaaien over de betrouwbaarheid en daarmee de geloofwaardigheid van de verkiezingsuitslag.

4.1 Waarom zou iemand het optelproces willen beïnvloeden?

Als iemand het optelproces wil beïnvloeden gaat het ofwel om de beïnvloeding van de verkiezingsuitslag door de zetelverdeling te veranderen, ofwel om twijfel te zaaien over de betrouwbaarheid van verkiezingen. Voor het zaaien van twijfel zijn relatief weinig, maar goed zichtbare incidenten nodig. Om de zetelverdeling te beïnvloeden moeten voldoende uitslagen gemanipuleerd worden.

Het stemproces vindt decentraal plaats in 10.000 stembureaus. Manipulatie op een enkel stembureauniveau zal niet snel tot zetelwisselingen leiden. Een stembureau vertegenwoordigt namelijk gemiddeld 1.000 stemmen. Om een zetel in het parlement te behalen zijn ongeveer 65.000 stemmen nodig. Manipulatie wordt interessanter als alle stemtotalen bij elkaar opgeteld worden, want dan kan bij grote gemeentes of op Kieskring-niveau wel degelijk met genoeg stemmen geschoven worden om zetels frauduleus te claimen.

Dit is waar hacken een rol kan spelen. De *schaalbaarheid* van fraude met stemmen is vele malen groter als dit in de software bij het optellen plaatsvindt dan wanneer wordt gefraudeerd in een stembureau.

4.2 Actoren

De volgende actoren vormen een extra dreiging en risico bij de betrouwbaarheid van de verkiezingsuitslag.

4.2.1 Frauderende gemeentelijke systeembeheerders

De mogelijkheid bestaat dat een opportunistische, politiek-gedreven, omgekochte of afgeperste gemeentelijke systeembeheerder met de uitslag fraudeert, aangezien deze volledig toegang (beheerdersrechten) heeft tot de optelcomputer die de beheerder ook nog eens zelf heeft ingericht.

Daarnaast hebben collega-ict'ers op de afdeling vaak toegang tot de werkplek van diegene die OSV2020-U op de laptops installeert in de weken en maanden voor de verkiezingen. Zij kunnen in een onbewaakt moment op de laptops inbreken, al dan niet op verzoek van een ander.

4.2.2 Buitenlandse inlichtingendiensten

Buitenlandse inlichtingendiensten, waaronder die van Rusland, China, Iran en Noord-Korea, hebben de technische mogelijkheden om Nederlandse gemeentes te hacken. Inmenging van buitenlandse statelijke actoren in verkiezingsprocessen is niet theoretisch. Een inmiddels bekend voorbeeld is de Russische inmenging en beïnvloeding in de Amerikaanse verkiezingen in 2016. En in 2014 hackte een Russische hackersgroep genaamd CyberBerkut de website van de Oekraïense centrale stemcommissie en wijzigde de uitslagen die later worden gepubliceerd. Ook in 2020 waren volgens Microsoft hackers gelinkt aan Rusland, Iran en China betrokken bij pogingen de Amerikaanse presidentsverkiezingen te beïnvloeden.

Het zou voor andere landen als Rusland of China interessant kunnen zijn om een politieke partij te bevoordelen die weinig op heeft met de EU, om het Europese handels- en machtsblok te verzwakken. Onrust en twijfel over de verkiezingsuitslag zouden een land en haar regering eveneens zwakker kunnen maken.

4.2.3 Personen die vanuit hun functie toegang hebben tot vergaderruimte waar optelcomputers staan

Iedereen die toegang heeft tot het gebouw waar het lokale OSV-netwerk actief is zou zich toegang kunnen verschaffen tot de (als het goed is afgesloten) vergaderruimte waar de hardware en optelcomputers staan, om hardware-implantaten zoals USB-keyloggers met simkaarten aan te sluiten om op afstand toegang tot de computers te krijgen.

Een voorzitter van een stembureau wist aan de stichting te melden dat in zijn gemeente vorig jaar voorzitters van stembureaus het proces-verbaal van hun stembureau moesten inleveren op de verkiezingsavond in de ruimte waar ook de optelcomputers stonden. Blijkbaar hebben in sommige gemeentes dus ook bepaalde burgers toegang gehad tot de ruimte waar de optelcomputers staan.

4.2.4 OSV-invoerders

OSV-invoerders zijn gemeenteambtenaren die fysiek toegang tot de ruimte waar het opgebouwde OSV2020-U-netwerk staat. In een grote gemeente kunnen dit wel zes tot acht invoerders zijn. Kwaadwillende, omgekochte, of onder druk gezette invoerders kunnen een hardware-implantaat plaatsen. Ook kan een besmetting direct via een fysiek aangesloten apparaat worden geïnitieerd. Hoewel het "vier-ogen" principe wordt toegepast bij het invoeren van de stemtotalen kunnen twee kwaadwillende of omgekochte invoerders de waarden ook bij het invoeren manipuleren.

4.2.5 Activisten

Activisten zouden het risico kunnen nemen een aanvalspoging te ondernemen om aan te tonen dat de verkiezing manipuleerbaar is. Dit zal veel media-aandacht opleveren voor de problematiek, maar ook onrust onder de bevolking en in de politiek, en tevens het vertrouwen aantasten in verkiezingen. Stichting Tegen

Hackbare Verkiezingen is nadrukkelijk van mening dat dit niet de juiste manier is om het verkiezingsproces veiliger te maken.

4.2.6 Individuele hackers

Een niet-ethische hacker zou een gemeentewebsite kunnen hacken, bijvoorbeeld om als 'grap' digitale processen-verbaal van stembureaus vier maanden na de verkiezingen aan te passen. De originelen zijn dan al vernietigd. Dit kan resulteren in media-aandacht voor de hacker, maar ook verwarring en onrust zaaien onder de bevolking en politiek.

4.2.7 Ervaren hackersgroep

Een hackersgroep die de *air-gap* naar het lokale OSV2020-U-netwerk weet te overbruggen, door fysiek in te breken en een hardware-implantaat achter te laten, of door de gemeentelijke infrastructuur vooraf te hacken zou in opdracht, eventueel betaald, of voor eigen gewin de verkiezingen kunnen beïnvloeden.

In 2016 bekende een hacker uitgebreid tegenover Bloomberg dat hij veel geld heeft verdiend door bijna tien jaar lang overal verkiezingen in Latijns-Amerika te manipuleren.

4.2.8 Optelsoftwareleverancier

De Duitse softwareleverancier vote iT GmbH en de OSV2020-U-broncode kan op gecompromitteerd zijn. vote iT kan (de onwaarschijnlijke) opdracht krijgen van de Duitse overheid om de software heimelijk aan te passen. Medewerkers van vote iT kunnen omgekocht of afgeperst worden.

5 Waar gaat het mis?

De kern van het probleem is dat software die best geschikt is voor het bepalen voor een voorlopige uitslag, gebruikt wordt voor de definitieve uitslag. De belangrijkste spelers lijken niet van zins of niet van machte om de benodigde veranderingen door te voeren.

5.1 Nut van onafhankelijk optellen wordt niet ingezien

De gemeentes, de Kiesraad[10] en het ministerie van Binnenlandse Zaken achten het niet noodzakelijk om stemtotalen van politieke partijen op alle niveaus handmatig na te rekenen of anderszins onafhankelijk te verifiëren:

1. De Kiesraad schrijft niet voor dat gemeentes ook (handmatig of anderszins onafhankelijk) stemtotalen per politieke partij uit de processen-verbaal bij elkaar op moeten tellen en deze uitslag daarna te vergelijken met de door de computer berekende uitslag. Deze controle zou een eventuele hack van een optelcomputer aan het licht kunnen brengen.
2. Omdat het niet wordt voorgeschreven, nemen gemeentes - op één na - niet de moeite om de door de optelsoftware berekende verkiezingsuitslag na te rekenen om eventuele fraude (hacks) op te sporen. Van de gemeente Utrecht is het bekend dat ze in 2017 voor drie door de burgemeester willekeurig gekozen partijen wel handmatig de stemtotalen op partijniveau bij elkaar opgeteld hebben, om de resultaten te vergelijken met de computeruitslag.
3. Gemeentes willen mogelijk niet handmatig optellen omdat ze dit ouderwets, foutgevoelig en tijdrovend vinden. Veel mensen vinden software betrouwbaar en zien het gevaar ervan niet in.
4. Gemeentes hebben wettelijk gezien maar een paar dagen de tijd om alle stemtotalen bij elkaar op te tellen en de uitslag te berekenen. Daar zijn ze al druk genoeg mee en op extra werk zitten ze waarschijnlijk niet te wachten.

De Kiesraad controleert zelf wel altijd de totalen van de hoofdstembureaus.

5.2 Kiesraad heeft (nog) geen mandaat over gemeentes

De Kiesraad heeft in zijn adviserende rol richting gemeentes in 2018 voor het eerst beveiligingsrichtlijnen opgesteld. Niemand controleert echter of deze in de praktijk correct worden doorgevoerd door gemeentes. De Kiesraad ondergaat daarvoor momenteel ook de transitie naar een “Kiesautoriteit”, zodat ze zeggenschap gaat krijgen over hoe gemeentes verkiezingen organiseren en dit kan en mag controleren. Dit is echter nog niet bekrachtigd.

[10] Update: In een reactie op 9 november 2020, laat de Kiesraad weten dat zij een natelling van de computertotalen op alle niveaus inmiddels ook noodzakelijk acht.

5.3 Het is aan burgers om fraude met optelcomputers te constateren

De overheid heeft als standpunt ingenomen dat als burgers bezorgd zijn over hacks of manipulatie van de computerberekening, ze sinds vorig jaar zelf altijd nog kunnen narekenen of alles wel klopt. Overigens kan dit vaak pas nadat de uitslag al bekend gemaakt is. Omdat weinigen zomaar zin hebben om onbetaald een paar dagen/weken te gaan zitten optellen en het bewustzijn veelal ontbreekt dat dit nuttig is, zijn serieuze burgerinitiatieven daaromtrent vooralsnog uitgebleven. Stichting Tegen Hackbare Verkiezingen concludeert hieruit dat dit anders moet worden georganiseerd.

6 Wat is de oplossing?

De oplossing is eenvoudig en ligt voor de hand.

Verifieer of de computeruitslag niet gehackt is door onafhankelijke optelling op de gemeentelijke, hoofd-, en centrale stembureaus door een validatiecommissie, via handmatig tellen of via onafhankelijke verificatie van de gepubliceerde uitslagen op het Internet.

6.1 Gemeentes en Hoofdstembureaus

6.1.1 Maakt onafhankelijke verificatie van stemtotalen eenvoudiger

In de eerste plaats moeten gemeentes zorgen dat onafhankelijke verificatie van de stemtotalen mogelijk is. De stichting raadt hiervoor de volgende procedure aan:

- De gescande processen-verbaal moeten zo snel mogelijk en op een vaste plaats online worden gezet.
- De in de computer ingevoerde stemtotalen moeten zo snel mogelijk online worden gezet.
- De hierboven genoemde gegevens moeten direct naast elkaar komen te staan, zodat snel kan worden gecontroleerd of de aantallen overeenkomen.
- De resultaten van de optellingen moeten zo snel mogelijk online worden gezet.
- Al deze documenten moeten worden voorzien van een digitale handtekening.

Dan wordt het voor iedereen eenvoudiger om de uitslagen te controleren. Deze controle zou verplicht moeten zijn en uitgevoerd moeten worden door een validatiecommissie. Hierbij mogen of helemaal geen computers gebruikt worden, of in elk geval geen gemeentelijke computers of computers die vooraf publiekelijk bekend zijn. Idealiter zou deze procedure niet alleen gevolgd worden bij de gemeentelijke centrale stembureaus, maar ook bij de hogere lagen (hoofdstembureau en centraal stembureau).

Daarnaast zouden gemeentes ter verificatie zelf handmatig op partijniveau alle stemtotalen bij elkaar op kunnen tellen uit de processen-verbaal van stembureaus. Er zou als compromis ook gekozen kunnen worden om de stemtotalen van een vooraf vastgesteld aantal politieke partijen na te rekenen (naar voorbeeld van Gemeente Utrecht die van drie willekeurige gekozen partijen de totaaltelling handmatig natelt).

Voorbeeld: Gemeente Utrecht had ongeveer 180 stembureaus (en dus 180 processen-verbaal) en 27 politieke partijen tijdens de Tweede Kamerverkiezingen in 2017. Dat betekent dat er 180 * 17 = 4.860 stemtotalen bij elkaar opgeteld moesten worden om te valideren of de software integer is geweest.

Tijdens een uitgevoerde steekproef in 2017 in gemeente Utrecht bleek dat het drie[11] uur kost om voor één politieke partij alle stemtotalen bij elkaar op te tellen. Geschat wordt dat het drie tot vier dagen in beslag zal nemen voor één persoon om voor alle partijen de uitslag te berekenen. De doorlooptijd kan echter ook verkort worden door meer ambtenaren voor de klus in te schakelen en door de optellingen op te knippen. Een relatief kleine moeite als gekeken wordt naar wat de maatschappelijke impact is van een gehackte verkiezing.

6.1.2 Hoeveel kost het per gemeente om handmatig op te tellen?

Voor een gemeente als Utrecht zou één ambtenaar met behulp van pen, papier en een (accountants)rekenmachine (geen mobiele telefoon of Excel), bovenstaande controle wel in drie dagen uit moeten kunnen voeren. Het betreft het invoeren van 3.060 getallen uit 180 processen-verbaal op een rekenmachine. De inschatting van drie dagen is overigens geen luxe, en zeker niet als het voor het eerst moet gebeuren. Als Gemeente Utrecht vijf ambtenaren één dag vrijmaakt die alle vijf 20% van de stemtotalen van alle 180 processen-verbaal laat optellen, dan zouden binnen één dag al handmatig alle stemtotalen op partijniveau bij elkaar opgeteld moeten kunnen worden.

Stel dat een medewerker € 400 per dag kost, dan zou het de gemeente Utrecht € 1.200 tot 1.600 kosten om eenmalig alles op te laten tellen. Als de opteller ruim de tijd krijgt voor de klus, zeg vijf dagen, dan kost het ongeveer € 2.000. Er zijn 355 gemeentes in Nederland. Veel kleine gemeentes hebben weinig stembureaus en zijn daarmee ook zo klaar met optellen. Natuurlijk moet je extra tijd rekenen voor het napluizen van mogelijke onregelmatigheden en extra budget voor het regelen van veilige ruimtes, maar voor één tot twee miljoen euro zou de overheid alles wel bij elkaar op moeten kunnen tellen.[12]

6.2 Politieke partijen

Grote politieke partijen moeten worden aangemoedigd hun eigen stemmen bij elkaar op te tellen, dan komt een mogelijke hack ook aan het licht. Dat zijn 10.000 optellingen (want 10.000 stembureaus) per partij. Zelfs handmatige verificatie van deze resultaten is best te doen met een klein aantal medewerkers. Als de gegevens uniform online zijn gezet, zoals hierboven aangegeven is, is de verificatie zelfs heel snel en eenvoudig te regelen.

6.3 Burgers

Totdat gemeentes hun verantwoordelijkheid nemen en handmatig gaan totaliseren, kunnen bezorgde burgers de processen-verbaal (N10 en N11) zelf downloaden om de verkiezingsuitslag te controleren: is er gefraudeerd met de optelsoftware? Dit is momenteel echter erg bewerkelijk om uit te voeren.

[11] De tijd van drie uur kan drastisch verkort worden als goed nagedacht wordt over hoe efficiënt en effectief handmatig getotaliseerd kan worden. Zo staat nu op elk proces-verbaal (N10) de totaaltelling per partij niet op het voorblad. Hierdoor moet er 180 keer afzonderlijk gezocht worden naar de juiste bladzijde om de totaaltelling van een partij op te zoeken.

[12] Het organiseren van een verkiezing kost ongeveer vijftig miljoen euro per keer.

Als de uitslagen online worden gezet (zoals beschreven in hoofdstuk 6.1), kunnen deze door burgers worden gedownload en met behulp van eigen computers gecontroleerd worden om te zien of de optellingen kloppen. Omdat het onwaarschijnlijk is dat alle computers van alle mensen die de optellingen controleren worden gehackt, geeft dit bijna dezelfde veiligheidsgarantie als de handmatige optelling. Het is wel zaak dat een controle niet afhankelijk wordt van de bereidwilligheid van vrijwilligers, maar verplicht georganiseerd wordt.

Kortom, de stichting is van mening dat er meerdere mogelijkheden zijn om de verificatiestap te regelen. Het uitgangspunt blijft dat we de resultaten van computersystemen niet zonder meer kunnen vertrouwen: verificatie is essentieel.

7 Wat is de kern van het probleem?

Het ministerie van Binnenlandse Zaken (BZK) is verantwoordelijk voor het organiseren van verkiezingen. De Kiesraad (ca. 16 FTE) is een onafhankelijk zelfstandig bestuursorgaan, belast met het organiseren van verkiezingen en levert de software. In Nederland is het verkiezingsproces sterk gedecentraliseerd. De rol van gemeenten daarbij is groot. Zij zijn verantwoordelijk voor de 10.000 stembureaus en bepalen de gemeentelijke uitslag.

De Kiesraad is zich inmiddels wel bewust van de onveilige software en wil ervan af. Ze heeft echter nog geen nieuwe oplossing en moet nu nog wel door met de oude versie die ieder jaar weer een stukje wordt verbeterd. De Kiesraad heeft waarschijnlijk wel de juiste kennis aan boord, maar het ontbreekt de Kiesraad aan mandaat, nieuwe software en controleerbare processen en procedures.

De Kiesraad is adviserend en levert de software aan gemeentes, maar de gemeentes bepalen nog steeds hoe ze de verkiezing willen organiseren in hun gemeente (binnen de wettelijke marges). De Kiesraad heeft op grond van de Kieswet geen bevoegdheid om een inspectie uit te voeren naar de veiligheid van de computerapparatuur. Wel heeft ze de bevoegdheid om onder voorwaarden tot een hertelling te besluiten (verschillen zijn geconstateerd die invloed kunnen hebben op de zetelverdeling), maar omdat er geen hiërarchische verhouding of toezichtsrelatie bestaat tussen de Kiesraad en andere organisaties in de verkiezingsketen, kunnen zij niet iets voorschrijven.

Veel gemeentes willen het liefst geen papier en zijn (groot) voorstander om alles te automatiseren. Vaak erkennen zij de hackdreiging niet, zijn zich hier niet bewust van, of denken dat de verschillende maatregelen die nu al genomen worden voldoende zijn om de veiligheid te waarborgen. Hoe dan ook, zij zien de noodzaak niet de uitslag handmatig na te tellen, zeker niet als de Kiesraad dit niet voorschrijft. Daarnaast hebben gemeentes vaak een (te) groot vertrouwen in computers. Gemeentes zijn vooral ingericht op efficiëntie, en veel minder op IT-integriteit en computerveiligheid.

De Kiesraad is druk en handmatig tellen is een impopulaire maatregel
De Kiesraad is volgens hun jaarverslag 2019 druk geweest met zes verkiezingen, de transitie van een Kiesraad naar een Kiesautoriteit en het ontwikkelen van nieuwe software. Voor die transitie hebben ze de samenwerking van gemeentes en BZK hard nodig.

Wat is de huidige stand van zaken omtrent OSV2020-U?
In opdracht van de Kiesraad voerde HackDefense een beveiligingsonderzoek uit op de veiligheid van de verkiezingssoftware (OSV2020-U). Het rapport dat zij opstelde werd in oktober 2020 openbaar gemaakt. Dit was het derde veiligheidsrapport dat over OSV werd opgesteld. Fox-IT heeft in 2017 en 2019 ook een rapportage geschreven. HackDefense is vrij positief over de veiligheid van de software, maar de evaluatie is niet erg diepgaand en voornamelijk het resultaat van analyses door standaardtools toe te passen op de programmacode zelf en de webomgeving van OSV. Een diepe, handmatige (regel-voor-regel) evaluatie van de veiligheid van de software maakte geen deel uit van de opdracht. Desalniettemin vond HackDefense aanwijzingen voor kwetsbaarheden in functionaliteit die weliswaar momenteel niet gebruikt wordt tijdens Nederlandse verkiezingen, maar wel duidelijk suggereren dat de software als geheel zwakheden bevat.

De broncode van OSV is inmiddels online gezet, maar nog niet in een vorm die het mogelijk maakt om zelf de uitvoerbare optelsoftware te genereren zodat geverifieerd kan worden of de aan de gemeentes beschikbaar gestelde cd-roms overeenkomen met de gepubliceerde broncode.

8 Conclusie

Verbetering en bewustzijn over kwetsbaarheid van Nederlandse verkiezingen voor hackaanvallen komen langzaam op gang binnen de overheid. Optelsoftware berekent op 17 maart 2021 nog steeds de verkiezingsuitslag en deze wordt vertrouwd zonder handmatige en onafhankelijke verificatie. Uitsluitend software de uitslag laten uitrekenen is onverantwoord en vormt een risico voor de continuïteit van onze democratie.

Software is en blijft altijd kwetsbaar voor een gemotiveerde en geavanceerde tegenstander. De impact van een gehackte verkiezing op de samenleving kan jaren zijn stempel drukken op het openbare leven, de diplomatieke verhoudingen met andere landen, en de economie.

Gemeentes, de Kiesraad[13] en het ministerie van Binnenlandse Zaken achten het niet noodzakelijk om stemtotalen van politieke partijen onafhankelijk na te rekenen, omdat de optelcomputers niet op internet zijn aangesloten. Gezien het actuele risico van (onder andere) buitenlandse inmenging in Amerikaanse en Europese verkiezingen is dit een onacceptabele situatie geworden.

De oplossing is simpel en laagdrempelig: gemeentes zullen handmatig op partijniveau stemtotalen bij elkaar op moeten gaan tellen en/of een onafhankelijke verificatie door derden moeten organiseren. Daarmee kan het risico op een gehackte verkiezing worden geminimaliseerd. De schatting van de kosten van handmatig optellen variëren van een tot twee miljoen euro.

Er zijn gelukkig nog ruim vier maanden om alles goed in goede banen te leiden voor komende verkiezingen. De Tweede Kamer moet dan wel snel ingrijpen en de minister hierop aanspreken.

Tot die tijd kunnen bezorgde burgers en politici sinds dit jaar zelf de processen-verbaal (N10 en N11) downloaden van gemeentesites en controleren of de optelsoftware (OSV2020-U) niet gehackt is. Dit is echter een tijdrovend karwei en zal waarschijnlijk lang niet voor alle gemeentes gedaan worden. De stichting betoogt dat zo'n verificatie gemakkelijk en vooral *verplicht* moet worden gemaakt.

[13] Update: In een reactie op 9 november 2020, laat de Kiesraad weten dat zij een natelling van de computertotalen op alle niveaus inmiddels ook noodzakelijk acht.

Bijlage A: Hoe kan een computer gehackt worden die niet op internet is aangesloten?

Computers bestaan uit veel onderdelen. Al die onderdelen hebben eigen aansturingssoftware. Inlichtingendiensten hebben mogelijkheden ontdekt om spionagesoftware in de firmware van bijvoorbeeld een moederbord of harde schijf te plaatsen. Het formateren/wissen van een harde schijf helpt daar niet tegen. Omdat verkiezingen niet elk jaar plaatsvinden, hergebruiken gemeentes vaak opnieuw geïnstalleerde computers waar ambtenaren jarenlang mee op internet hebben gewerkt.

Een inlichtingendienst kan maanden van tevoren gemeentecomputers hacken, of heel gericht gemeentelijke systeembeheerders digitaal aanvallen om precies mee te kijken hoe, wanneer en welke computers gebruikt gaan worden in een verkiezing.

Daarnaast geldt in cybersecurity de wetmatigheid dat als iemand fysieke toegang heeft tot een computer, het vrijwel altijd *game-over* is qua veiligheid. Tenzij onafhankelijke verificatie wordt georganiseerd, zoals de stichting bepleit. Dat betekent dat iedereen die toegang heeft tot de hopelijk afgesloten vergaderruimte waar de verkiezingsopstelling staat, met de computers of het netwerk kan rommelen.

In een grote gemeente kunnen zeven OSV2020-U-invoercomputers gebruikt worden die in een offlinenetwerk met elkaar verbonden zijn. Hiervoor worden niet echt beveiligingsstandaarden of eisen gesteld, noch wordt softwarematig gecontroleerd of besturingssystemen *up-to-date* zijn, draadloze netwerken uitstaan, etc.

1. Er zijn hardware-implantaten van een paar centimeter groot die een simkaart bevatten[14]. Zo zou iemand met fysieke toegang via 4G toch kunnen inbellen op het *air-gapped* verkiezingsnetwerk waar de optelsoftware op draait.
2. Er zijn hardware *keyloggers* met simkaart om wachtwoorden te achterhalen.
3. Door een hardware-implantaat op het offlinenetwerk aan te sluiten kunnen de computers mogelijk gehackt worden via een zwakheid in het besturingssysteem of OSV2020-U.
4. Een aanvaller met meer tijd en zonder medestanders kan de harde schijf uit de computer halen en malware erop zetten of het wachtwoord achterhalen als de harde schijf niet is versleuteld.
5. De vergaderruimte zal niet in alle gevallen een sterk slot bevatten en dus zal dit voor een geoefende *lockpicker* ongezien binnen enkele minuten te openen moeten zijn. Bovendien zal de ruimte in veel gevallen niet 24/7 fysiek bewaakt en bemand worden. Mogelijk wel een ingebouwd alarmsysteem voor als het gebouw op slot gaat 's nachts. Daarnaast zou een gemeente ad-hoc cameratoezicht met alarmfunctie kunnen installeren op eigen initiatief in de vergaderkamer.

[14] Bekijk de ANT catalogus van de NSA voor een veel meer hardware-implantaten die de Amerikaanse-inlichtingendiensten gebruiken om *air-gapped* netwerken te hacken.