VNG Realisatie

Impactanalyse Uniforme domeinnaamextensie

Definitieve rapport versie 1.0

Auteurs: Nienke Langejan en Mark van Dam

Inhoudsopgave

Managementsamenvatting

Inleiding en aanpak

Het ministerie van Binnenlandse Zaken voert momenteel in opdracht van de Staatssecretaris een onderzoek uit met als doel om in beeld te brengen in hoeverre de invoering van een uniforme domeinnaamextensie voor websites en mail kan helpen om de herkenbaarheid van overheidswebsites en email te vergroten en de veiligheid van overheidswebsites en email te verbeteren. Aanleiding hiervoor zijn onderzoeken van Novay naar de kansen en risico's bij invoering van een uniforme domeinnaamextensie en onderzoek van Kantar naar de herkenbaarheid van overheidswebsites voor burgers. VNG heeft naar aanleiding van dit voorstel een impactanalyse laten uitvoeren naar de invoering van een uniforme domeinnaamextensie voor gemeentelijke websites en email. VNG Realisatie heeft deze opdracht uitgevoerd. Deze impactanalyse is uitgevoerd in de periode van september 2019 tot en met november 2019.In deze impactanalyse is gekeken naar de gevolgen voor gemeenten van het implementeren van een uniforme domeinnaamextensie. Het doel is om de uitvoerbaarheid en impact hiervan voor gemeenten in kaart te brengen. Hiervoor zijn gesprekken gevoerd met 12 gemeenten, is er onder de leden van de Vereniging Directeuren Publieksdiensten een enquête gehouden en heeft de Informatiebeveiligingsdienst voor Gemeenten een advies uitgebracht.

Huidige situatie

In de gesprekken is in kaart gebracht hoe gemeenten momenteel omgaan met de domeinnaam voor website en email. Gemeenten blijken gebruik te maken meer dan één website. Zowel voor digitale dienstverlening, informatieve onderwerpen als voor projecten zijn er verschillende sites en worden aparte domeinnamen gebruikt. Gemeenten werken ook vaak samen met andere publieke of private organisaties. Voor dergelijke samenwerkingen worden regelmatig aparte domeinnamen gebruikt.
Gemeenten blijken na een herindeling de domeinnamen van de oorspronkelijke gemeenten in stand te houden en via een re-direct aan de nieuwe site te koppelen. Tevens registreren gemeenten hun domeinnaam ook onder andere extensies dan *.nl om misbruik te voorkomen. Daarmee hebben gemeenten een groot aantal domeinnamen in hun bezit. Niet alle gemeenten hebben beleid voor het aanmaken van domeinnamen. Burgers blijken vooral via de zoekbalk van Google op de gemeentelijke site terecht te komen en niet via de domeinnaam.
Gemeenten gebruiken in de verbinding tussen website en achterliggende applicaties of servers de domeinnaam op de beveiligingscertificaten. Gemeenten hebben veel van dergelijke certificaten in gebruik. Beveiliging van de website en achterliggende servers is voor gemeenten van groot belang en in de onderzoeken van Forum Standaardisatie scoren gemeenten ook zeer hoog op het toepassen van de vereiste beveiligingsstandaarden voor website en email.

Impact invoering uniforme domeinnaam bij gemeenten

Het voorstel voor de invoering van een uniforme domeinnaamextensie is nog niet volledig uitgewerkt wat er toe leidt dat gemeenten de impact nog niet helemaal kunnen inschatten. De

impact hangt onder meer af van welke websites er onder dit voorstel gaan vallen. Voor het bereiken van het effect van herkenbaarheid bij burgers, zouden *alle* websites van gemeenten en overheidsorganisaties meegenomen moeten worden. Maar in dat geval is de impact bij gemeenten zeer groot. Tevens is nog de vraag of dit voorstel gaat gelden voor alleen website of ook voor email. Ook hier: alleen de website, dan is de impact te overzien, als het ook gaat om achterliggende systemen en email, dan is de impact zeer groot.

Gemeenten en de Informatiebeveiligingsdienst voor gemeenten vragen zich af of het inrichten van één overheidsdomein niet gaat leiden tot een single point of failure of een groter risico voor gemeenten om doelwit te worden van hackers.
Gemeenten ervaren niet dat burgers moeite hebben met het herkennen van de gemeentelijke website. Daarmee is dit een lastig voorstel om intern te verkopen en capaciteit voor los te krijgen. Gemeenten vragen zich af waarom de oplossing voor het herkenbaar maken van de overheid wordt gezocht bij een uniforme domeinnaamextensie. Ze vragen zich af of er geen betere manieren zijn om overheidswebsites herkenbaar te maken. Gemeenten denken dan aan eisen rondom toegankelijkheid en eenduidige vormgeving van websites. Deze alternatieven zijn in de impactanalyse niet nader onderzocht.

Kosten

Gemeenten zullen technische aanpassingen moeten doen, zoals het aanpassen van de certificaten, re-directs van emailadressen. Niet alleen ontstaan kosten door de aanschaf van nieuwe certificaten; ook moet worden geïnvesteerd in het installeren en testen van deze certificaten in de gemeentelijk architectuur en bij leveranciers en ketenpartners. Daarnaast moet worden geïnvesteerd in gemeentelijke communicatie rond de nieuwe domeinnamen en emailadressen naar burgers, ondernemers en betrokken ketenpartners en moeten communicatie-uitingen worden aangepast. Alleen de investering in de aanschaf van nieuwe certificaten bedraagt al minimaal € 7,5 miljoen euro. De kosten van installeren, testen, aanpassen communicatie-uitingen en communiceren over deze wijziging zijn op dit moment niet in te schatten. We gaan echter uit van een aanzienlijke kostenpost die daarmee samenhangt.

Conclusies en aanbevelingen

Invoering van een uniforme domeinnaamextensie gaat vooral gepaard met eenmalige werkzaamheden. Na de invoering veranderen de werkzaamheden niet of nauwelijks ten opzichte van de huidige situatie. De impact – zeker qua technische aspecten – kan echter wel heel groot zijn. Dit zal afhangen van de gekozen scope. Tevens zijn de aanpassingen dus niet beperkt tot de gemeenten, maar worden ook andere partijen hierdoor geraakt.

De kosten die met de invoering van een uniforme domeinnaamextensie gepaard gaan voor gemeenten zijn hoog. Hier staan nauwelijks besparingen tegenover. Ook dit leidt ertoe dat gemeenten niet positief staan tegenover de invoering van een uniforme domeinnaamextensie Indien gekozen wordt om een uniforme domeinnaamextensie in te voeren, dan is het wenselijk dat gemeenten voor deze kosten gecompenseerd worden op basis van artikel 2, Wet Financiële Verhoudingen.

Gemeenten herkennen niet dat de probleemstelling van beperkte herkenbaarheid overheidswebsites en verbeteren beveiliging voor de gemeentelijke websites opgelost kan worden door het invoeren van een uniforme domeinnaamextensie. Gemeenten zien wel dat er mogelijkheden zijn de herkenbaarheid en toegankelijkheid van gemeentelijke websites te verbeteren. Op het gebied van beveiliging nemen gemeenten hun verantwoordelijkheid al, gezien de hoge score op de toepassing van de juiste standaarden.

Gemeenten hebben verschillende risico's voor de implementatie van de uniforme domeinnaamextensie benoemd. Bij deze een opsomming:

- Het gaat hier om een ingrijpende verandering die naar inschatting van de gemeenten niet of onvoldoende tot het gewenste effect zal leiden
- Vermoedelijk is er weinig draagvlak bij raad, college en de interne organisatie omdat de meerwaarde van het voorstel onvoldoende is aangetoond.
- Gemeenten vrezen als niet alle overheidsorganisaties van dezelfde laag deze wijziging doorvoeren er juist onduidelijkheid voor burgers ontstaat.
- Gemeenten geven aan dat een bureaucratisch proces van aanvragen van websites bij centrale beheerorganisatie hen zal belemmeren.

Voor de implementatie van de uniforme domeinnaamextensie zijn de volgende randvoorwaarden benoemd:

- Er moet een uitgewerkt voorstel komen, waarin de scope helder is en het beoogde effect aantoonbaar wordt gemaakt voor gemeenten.
- De invoering moet uitgaan van een wettelijke verplichting, zodat alle gemeenten verplicht worden mee te doen
- Vanuit het Rijk dient er een landelijke communicatiecampagne ingericht te worden om deze naamswijzigingen toe te lichten.
- Er dient rekening gehouden te worden met de tijd die leveranciers nodig hebben om gemeenten te helpen met het doorvoeren van deze veranderingen.
- Gemeenten dienen voor deze invoering gecompenseerd te worden op basis van artikel 2 (Wet Financiële verhoudingen).

1. Inleiding

1.1. Introductie

VNG heeft in opdracht van het ministerie van Binnenlandse Zaken (BZK) een impactanalyse laten uitvoeren naar de invoering van een uniforme domeinnaamextensie voor gemeentelijke websites en email. VNG Realisatie heeft deze opdracht uitgevoerd. Deze impactanalyse is uitgevoerd in de periode van september 2019 tot en met november 2019.

In deze impactanalyse is gekeken naar de gevolgen voor gemeenten van het implementeren van een uniforme domeinnaamextensie. Het doel is om de uitvoerbaarheid en impact hiervan voor gemeenten in kaart te brengen.

Dit hoofdstuk schetst het voorstel voor het invoeren van een uniforme domeinnaamextensie op hoofdlijnen, de onderzoeksvragen voor deze impactanalyse en het gevolgde proces om te komen tot beantwoording van deze vragen.

1.2. Voorstel: Uniforme domeinnaamextensie

Momenteel zijn er geen afspraken over welke domeinnaamextensies overheidsorganisaties gebruiken voor hun websites en emailadressen. Uit onderzoek dat BZK heeft laten uitvoeren (Kantar, januari 2019[1]) is gebleken dat de *herkenbaarheid* van overheidswebsites niet optimaal is: burgers en bedrijven herkennen overheidswebsites niet altijd direct als zodanig. Daarnaast ziet BZK diverse risico's op het gebied van *veiligheid*.

Het ministerie van Binnenlandse Zaken voert momenteel in opdracht van de Staatssecretaris een onderzoek uit met als doel om in beeld te brengen in hoeverre de invoering van een uniforme domeinnaamextensie voor websites en mail kan helpen om de *herkenbaarheid van overheidswebsites en email te vergroten* en de *veiligheid van overheidswebsites en email te verbeteren*. Daarnaast kan het gebruiken van een uniforme domeinnaamextensie mogelijk leiden tot kwaliteitsverbetering van overheidswebsites en tot versterking van het overheidsimago. Er worden meerdere mogelijke domeinnamen en implementatiescenario's onderzocht.

1.3. Vraagstelling

Deze impactanalyse geeft inzicht in de uitvoerbaarheid en de impact van de invoering van een uniforme domeinnaamextensie voor website en mail op gemeenten. Tevens geeft de impactanalyse aanbevelingen voor de implementatie van een uniforme domeinnaamextensie bij gemeenten wanneer ervoor wordt gekozen om dit daadwerkelijk in te voeren.

De onderzoeksvragen voor deze impactanalyse zijn:

[1] https://www.rijksoverheid.nl/documenten/rapporten/2019/01/31/herkenbaarheid-van-en-vertrouwen-in-websites-en-e-mails-van-de-overheid

1. Wat wijzigt er in de werkwijze van de gemeente door invoering van de uniforme domeinnaamextensie voor websites en email?
2. Wat betekent deze verandering voor de gemeentelijk organisatie? Hierbij wordt zowel gekeken naar de primaire processen als naar de ondersteunende processen en bedrijfsvoeringsaspecten.
3. Is de gemeente voldoende toegerust voor een doeltreffende uitvoering?
4. Welke kosten en besparingen voor de gemeentelijke uitvoering zijn aan de invoering van een uniforme domeinnaamextensie verbonden?
5. Wat zijn de verwachte effecten van de invoering van een uniforme domeinnaamextensie?
6. Hoe kan een uniforme domeinnaamextensie worden geïmplementeerd en wat zijn de randvoorwaarden en risico's? Ga hierbij uit van de door BZK benoemde implementatiescenario's.

1.4. Aanpak & methodologie

Voor het uitvoeren van deze impactanalyse is gebruik gemaakt van de methodiek met bijbehorend analysekader die VNG Realisatie hanteert voor het uitvoeren van impactanalyses. Het proces is begeleid door een begeleidingscommissie, bestaande uit vertegenwoordigers van het ministerie van Binnenlandse Zaken (Rob Ramdjilal, Dirk Maats), Vereniging Nederlandse Gemeenten (Peter van Dijk), VNG Realisatie (Pieter Pinxten) en de Vereniging Directeuren Publieksdiensten (Jan Fraanje).

Voor het beantwoorden van de onderzoeksvragen is een plan van aanpak opgesteld. Dit plan is in september 2019 door de begeleidingscommissie goedgekeurd. Tevens heeft de begeleidingscommissie nog suggesties gedaan voor de te betrekken gemeenten. Het onderzoek bestond uit vier onderdelen.

Ten eerste is een documentanalyse uitgevoerd, waarbij de volgende documenten bestudeerd zijn:
- projectvoorstel van BZK,
- onderzoeken van Novay en Kantar,
- diverse rapportages van Forum Standaardisatie.

Ten tweede zijn er met 12 gemeenten interviews gehouden. Het ging hierbij om gemeenten die verschillen qua grootte en ligging in het land. Daarnaast is er gekeken naar gemeenten die de afgelopen jaren een herindeling hebben meegemaakt, omdat zij een dergelijke wijziging van domeinnaam al eens hebben doorgevoerd. De laatste groep waren gemeenten die nu al een afwijkende domeinnaam hebben, zoals www.nijkerk.eu of gemeenten die hun domeinnaam delen met een VVV, zoals www.leiden.nl. De lijst met geïnterviewde gemeenten is te vinden in bijlage A. De gebruikte topiclijst is te vinden in bijlage B.

Ten derde is er een enquête uitgezet onder de leden van de Vereniging Directeuren Publieksdiensten. Deze enquête ging in op dezelfde onderwerpen als de interviews. De enquête is via de nieuwsbrief van de VDP verstuurd en heeft 1 week opengestaan. Er zijn 12 volledig ingevulde enquêtes ontvangen. Het beeld dat hieruit naar voren kwam, sloot aan bij het beeld van

de kwalitatieve interviews. De resultaten van de enquête zijn daarom in de bevindingen verwerkt en niet meer apart benoemd.

Ten vierde heeft de Informatie Beveiligingsdienst Gemeenten (IBD) van de VNG een advies uitgebracht. Zij hebben een advies gegeven over de mogelijkheden die een uniforme domeinnaam biedt om de beveiliging van websites en email te verbeteren.

De resultaten en bevindingen zijn via een schriftelijke ronde aan de geïnterviewde gemeenten voorgelegd en besproken met de begeleidingscommissie op 12 november 2019. Daarna is het eindrapport opgesteld. Dit is opgeleverd op 6 december 2019.

1.5. Leeswijzer

Dit rapport is als volgt opgebouwd:

- In hoofdstuk 2 wordt de achtergrond geschetst van het onderzoek van BZK naar een uniforme domeinnaamextensie, dat aanleiding vormt voor deze impactanalyse;
- In hoofdstuk 3 wordt de huidige situatie beschreven;
- In hoofdstuk 4 wordt de nieuwe situatie beschreven die ontstaat door de invoering van een uniforme domeinnaamextensie en de impact hiervan voor gemeenten;
- In hoofdstuk 5 worden de conclusies gegeven, door de onderzoeksvragen van deze impactanalyse te beantwoorden.

2. Achtergrond bij het onderzoek naar een uniforme domeinnaamextensie

In dit hoofdstuk wordt de achtergrond geschetst van het onderzoek van BZK naar de invoering van een uniforme domeinnaamextensie. Dit onderzoek vormt de aanleiding voor deze impactanalyse.

2.1. Aanleiding voor het onderzoek

Bij het ministerie van BZK is in de zomer van 2019 een project gestart om het invoeren van een uniforme domeinnaamextensie voor overheidswebsites en email te onderzoeken. Aanleiding hiervoor zijn onder meer twee onderzoeken geweest. Novay heeft in 2013 gekeken naar de mogelijkheden om een TopLevelDomein voor de gehele overheid in te voeren. Kantar heeft in 2019 een onderzoek onder burgers gedaan naar de herkenbaarheid van overheidswebsites en email. Hierna worden deze onderzoeken en de uitkomsten besproken.

2.1.1. Onderzoek Novay

Het onderzoek van Novay (februari 2013[2]) heeft verkend wat de kansen en risico's zijn van het inzetten een generiek TopLevelDomein (gTLD) voor overheidswebsites. Hierbij is gekeken naar de optie om *.overheidnl te registreren en te gaan gebruiken in plaats van *.nl. Doel was om overheidscommunicatie via het internet betrouwbaarder te maken. Een dergelijk gesloten en door de overheid gecontroleerd gTLD biedt potentiële mogelijkheden om invloed uit te oefenen op de beveiliging en betrouwbaarheid van de online overheidscommunicatie en deze daarmee naar een hoger niveau te brengen. Tevens is in dit onderzoek gekeken naar de mogelijkheid om *.overheid.nl te gebruiken. In de tabel hieronder staan de conclusies uit het Novay onderzoek samengevat.

Samengevatte uitkomsten uit onderzoek Novay
De absolute meerwaarde van de beveiligingsmogelijkheden die een gTLD biedt is ten opzichte van de andere situaties beperkt en te kenschetsen is als anders maar niet beter of slechter. Beschikbare beveiligingsmaatregelen om DNS veiliger te maken (DNSSEC) of om via DNS de communicatie te beveiligen (met bijvoorbeeld technologieën als DANE en DKIM) kunnen ook in de huidige situatie ingezet worden. Wel is er bij een gTLD meer controle over de beveiliging doordat er strengere eisen kunnen worden gesteld. In het geval van een *.overheid.nl situatie, is de overheid volledig in control over wie daaronder domeinen registreert en hoe de beveiliging ervan ingericht is. Vanuit communicatie-perspectief biedt een eigen gTLD beperkte meerwaarde betreffende de herkenbaarheid en de eenduidigheid van de overheidscommunicatie richting burgers of bedrijven. Hier hangt een prijskaartje aan dat mede bepaald wordt door te verwachten transitiekosten voor allerlei bestaande communicatieve uitingen.

[2] https://kennisopenbaarbestuur.nl/media/23353/een-top-level-domein-voor-betrouwbare-overheidscommunicatie.pdf

Een *.overheid.nl situatie biedt vanuit communicatieperspectief vergelijkbare meerwaarde tegen naar verwachting substantieel lagere kosten. Overheidswebsites worden t.o.v. de huidige .nl situatie herkenbaarder als ze vallen onder een gTLD of het *.overheid.nl domein. De acceptatie en het draagvlak onder burgers en bedrijfsleven zijn lastig te bepalen, maar lijken te worden ondermijnd door het ontbreken van duidelijke meerwaarde voor hen en de weinig intuïtieve naamgeving van de aangevraagde *.overheidnl gTLD naam. Met een overheidseigen gTLD vallen efficiency-slagen te behalen betreffende de vindbaarheid en authenticiteit van overheidscontent van de overheidswebsites. De grote mate van controle die een gTLD met zich meebrengt kan ten koste gaan van de flexibiliteit en vrijheid die overheidsorganisaties nu hebben om een domeinnaam aan te vragen.
Voordelen zijn te behalen met het inrichten van één centraal loket voor het aanvragen van domeinen. Dit vergroot de controle op registraties van domeinnamen en draagt bij tot een beter toezicht op het naleven van het gebruik van DNSSEC en de webrichtlijnen.

Op basis van dit onderzoek heeft de Rijksoverheid besloten om de aanvraag voor het gTLD *.overheidnl in te trekken[3]. Het onderzoek is vervolgens gericht op *.overheid.nl.

2.1.2. Onderzoek Kantar

In januari 2019 is een onderzoek uitgevoerd door Kantar[4] onder 1423 burgers. Aanleiding voor dit onderzoek was dat BZK een goed beeld wilde krijgen van de wensen, behoeften en verwachtingen van burgers op het gebied van online overheidscommunicatie. De uitkomsten van dit onderzoek staan in onderstaand kader samengevat.

Uitkomsten onderzoek Kantar

Uit de resultaten blijkt dat burgers slecht in staat zijn om onechte websites te herkennen. De vervalste websites worden niet herkend door 50% tot 60% (afhankelijk van het voorbeeld) van de deelnemers. Bij vervalste e-mails zijn de resultaten wat gunstiger: deze worden door 10% tot 30% van de respondenten niet ontmaskerd. Met het herkennen van echte (overheids-)websites en e-mailberichten is het niet beter gesteld. Slechts 30% tot 50% herkent de voorgelegde overheids-websites als echt. Ook hier worden de e mailberichten vaker juist beoordeeld (48% tot 74% correct).
Vervalste websites herkent men vooral aan de hand van de domeinnaam. De focus op de domeinnaam, zorgt er bij een aantal echte websites van overheidsdiensten voor dat men deze niet herkent, omdat men niet bekend is met de afzender van de overheidsdienst, bijvoorbeeld DUO.
Circa 63% van de deelnemers verwacht gemakkelijker websites en e mails van de overheid te herkennen wanneer deze zijn voorzien van een uniforme domeinextensie. Driekwart van de deelnemers (75%) is voorstander van zo'n uniforme extensie. Bijna negen op de tien ondervraagden (86%) geven hierbij de voorkeur aan de extensie "*.overheid.nl".

[3] https://tweakers.net/nieuws/88010/overheid-trekt-reservering-in-voor-gtld-overheidnl.html
[4] https://www.rijksoverheid.nl/documenten/publicaties/2019/07/04/rapport-kantar-public-telemarketing-2019

Burgers krijgen vaak het advies ‘Let op domeinnaam’. De waarde van dit advies neemt toe, wanneer de overheid ervoor kiest om domeinnamen meer uniform vorm te geven, zodat het duidelijk is waar mensen op moeten letten.

Naar aanleiding van de uitkomsten van deze twee onderzoeken is het project Uniformering overheidsdomeinextensie gestart.

2.2. Project ‘Uniformering overheidsdomeinextensie’ van BZK

2.2.1. Scope van het project

Bij de start van het project heeft BZK vier onderwerpen geformuleerd waarop men mogelijke voordelen ziet van de invoering van een uniforme domeinnaamextensie[5]:

1. Communicatie:
   - Versterking overheidsimago: imago versterkend keurmerk, straalt betrouwbaarheid uit.
   - Herkenbaarheid door consistentie: voor burger wordt het makkelijker om overheidssites te herkennen.
   - Kwaliteitsverbetering: kwaliteitsslag in overheidscommunicatie (je mag alleen *.overheid.nl gebruiken als je voldoet aan webrichtlijnen); voorkomen van onwenselijke url’s.

2. Veiligheid:
   - Beveiligingsbeheer en standaarden: meer controle op veilige configuratie, invoering en controle op internetbeveiligingsstandaarden wordt eenvoudiger.
   - Betere waarborgen echtheid: extra controle voor burger naast https slotje.
   - Beperken mogelijkheden typosquatting[6] (alleen overheijd, overheit en overhijd).
   - Geen misbruik oude domeinnamen: alleen overheid kan domeinnamen zelf opnieuw registreren (en dus kunnen criminelen niet een oud overheidsdomein misbruiken).

3. Beheersbaarheid:
   - Beter overzicht: Overheid heeft zelf overzicht over alle domeinnamen. Dat overzicht is er nu niet.
   - Hogere kwaliteit: Door overzicht kan overheid beter zicht houden op kwaliteit van e-dienstverlening.
   - Meer grip: Meer grip op websites vanuit AVG compliance.
   - Centraal domeinbeheer: mogelijk om aanvragen, beheren en beveiligen van domeinnamen binnen een gestandaardiseerde omgeving te organiseren.
   - Gebruiksvoorwaarden: mogelijk om gebruiksvoorwaarden te stellen, zoals verplicht gebruik van standaarden, naamgevingsconventies etc.
   - Naamswijziging eenvoudiger: beoogde domeinnamen kunnen niet in handen zijn van partijen buiten de overheid.
   - Inactieve domeinen verwijderen: momenteel is afstoten domeinnamen een risico op misbruik, dit levert een blijvende beheerlast op. Probleem wordt opgelost met uniforme

[5] Bron: Presentatie Voordelen 1 uniforme overheidsdomeinextensie, BZK, April 2019
[6] [6] https://nl.wikipedia.org/wiki/Typosquatting: het opzetten van een valse website met typfouten in de domeinnaam.

domeinnaam.

4. Overig
    - Lagere operationele kosten: verminderen aantal te beheren (inactieve) domeinen, verminderen contacten Klant contact centrum ivm spoofing[7]/phishing[8].
    - Conform best practice: aansluiten bij wat in buitenland al vaker gebruikt wordt.

2.2.2. Verschillende sporen

BZK heeft in dit project meerdere sporen lopen:

- Een onderzoek naar het gebruik van een (second of top level) domeinextensie in het buitenland. Dit onderzoek is uitgevoerd door PBLQ, de resultaten zijn in november 2019 opgeleverd.
- Een onderzoek op de samenvoeging van meerdere sites tot onder meer www.politie.nl en *.postnl.
- Daarnaast is aan verschillende (koepels van) overheidspartijen (onder andere provincies, waterschappen en gemeenten) gevraagd om de impact voor hun organisaties te bepalen. De VNG heeft naar aanleiding hiervan de voorliggende impactanalyse uitgevoerd om de impact voor gemeenten in kaart te brengen.

Op basis van deze verschillende sporen brengt de projectgroep van BZK een advies uit aan de Staatssecretaris voor een eventueel vervolg.

[7] https://nl.wikipedia.org/wiki/Spoofing: het vervalsen van kenmerken met als doel om tijdelijk een valse identiteit aan te nemen. Dit kan bijvoorbeeld met een emailadres.
[8] https://nl.wikipedia.org/wiki/Phishing: het vervalsen van een website om zo inloggegevens te verkrijgen.

3. Huidige situatie

In dit hoofdstuk wordt de huidige werkwijze van gemeenten beschreven met betrekking tot de domeinnaam voor website en email. We kijken eerst naar de situatie rondom domeinnamen bij gemeenten, vervolgens naar de vindbaarheid van websites, het gebruik van certificaten en tenslotte naar de toepassing van beveiligingsstandaarden door gemeenten.

3.1. Domeinnamen

Onder gemeenten is een grote variatie in het aantal geregistreerde domeinnamen. Dit varieert van enkele tientallen tot meer dan 300. Dit zijn deels actieve en deels inactieve domeinnamen; de laatste categorie is vaak het grootst. In figuur 1 is voor enkele gemeenten te zien hoeveel websites die gemeenten gebruiken voor hun digitale dienstverlening. Deze gegevens komen uit een onderzoek van VNG Realisatie[9]. In de interviews heeft een G4 gemeente overigens aangegeven dat ze veel meer sites gebruiken dan de hier genoemde 31. Naast de websites gericht op digitale dienstverlening kunnen gemeenten dus nog allerlei andere websites hebben, bijvoorbeeld informatieve sites, campagnesites en projectsites.

Figuur 1. Onderzoek VNG Realisatie aantal sites voor digitale dienstverlening per gemeente en sites van Utrecht als voorbeeld.

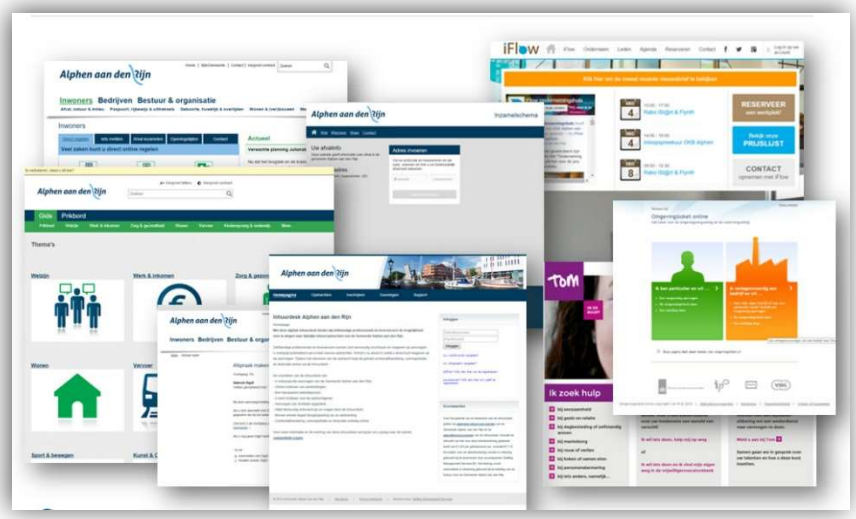
3.1.1. Websites van samenwerkende organisaties

De meeste gemeenten geven aan dat er meerdere sites zijn waarop de gemeente samenwerkt met organisaties in de gemeente of regio. Dit kunnen zowel publieke als private organisaties zijn. Daarvoor is vaak een aparte website met eigen domein aangemaakt. Deze websites worden soms

[9] https://publicaties.vngrealisatie.nl/2017/koken-met-data/recept-6-exploratief-onderzoek-naar-bezoek-gemeentelijke-websites/, April 2017.

door de gemeente en soms door één van de partnerorganisaties beheerd. Hier is geen sprake van sec een gemeentelijke website, en afhankelijk van de samenstelling van de samenwerking is de vraag of gesproken kan worden van een overheidswebsite. Zeker bij samenwerkingen met private organisaties is deze grens niet altijd zuiver te trekken. In figuur 2 is te zien op welke sites je via de site van de gemeente Alphen aan den Rijn terecht kan komen.

Voor bouw- of tijdelijke projecten worden vaak aparte sites aangemaakt. Soms door de gemeente, soms door de projectontwikkelaar. Soms draagt een gemeente de domeinnaam over aan een bewonersorganisatie als de wijk gebouwd is.



Figuur 2. Sites gekoppeld aan gemeentelijke site Alphen aan de Rijn.

3.1.2. Herindelingen

Gemeenten die een herindeling hebben meegemaakt, houden de domeinnamen van de oorspronkelijke gemeenten vaak in eigen bezit. Meestal worden de oude domeinnamen voor een periode van meerdere jaren via een re-direct naar de nieuwe domeinnaam doorgezet. Maar een re-direct kost ook geld en dat kan voor kleinere gemeenten een reden zijn om na verloop van tijd de re-direct te stoppen. De oude domeinnamen blijven dan wel in het bezit van de gemeente om misbruik te voorkomen.
In de voorbereiding op herindelingen worden vaak meerdere mogelijke domeinnamen van de toekomstige fusiegemeente geregistreerd. Dit wordt niet altijd opgeschoond na een definitieve keuze voor de nieuwe gemeentenaam.

3.1.3. Andere extensies

Gemeenten registreren hun domeinnaam ook vaak nog met *.com, *.info, *.org of *.eu. Dit om misbruik tegen te gaan. Dit domein wordt dan meestal niet actief gebruikt, maar is wel in eigendom van de gemeente.

3.1.4. Beleid voor het aanmaken van domeinnamen

Sommige van de geïnterviewde gemeenten hebben beleid op het mogen aanmaken van domeinnamen. Die gemeenten hebben goed zicht op welke domeinnamen er zijn en op de toe te passen beveiligingsmaatregelen, eisen aan lay-out en toegankelijkheid en het verlopen van certificaten. Vaak wordt het aanmaken en beheren van domeinnamen in deze gemeenten gecoördineerd vanuit een webteam waarin met name expertise rond communicatie, ICT en online dienstverlening vertegenwoordigd is. Veel gemeenten geven aan steeds meer te werken met subdomeinen in plaats van nieuwe domeinnamen: *.gemeentenaam.nl of www.gemeentenaam.nl/*.

Maar bij veel andere gemeenten is het beleid voor het aanmaken van domeinnamen niet heel strak geregeld en kunnen medewerkers zelf namen registreren.

3.1.5. Relatie website met achterliggende systemen

De gemeentelijke website heeft vaak een verregaande integratie tussen de website en achterliggende systemen (Basisregistraties, pre-fill van formulieren en dergelijke). Voor het beveiligen van deze verbindingen worden certificaten gebruikt waarop de domeinnaam staat.

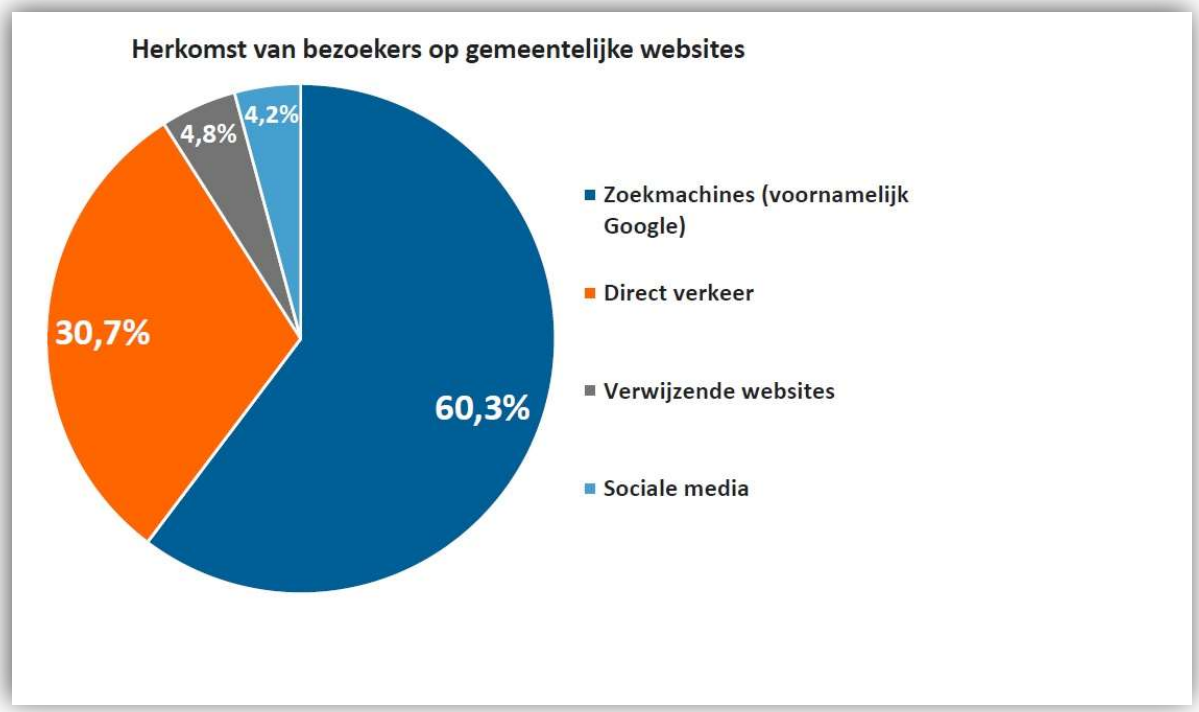
3.2. Vindbaarheid

De geïnterviewde gemeenten geven aan dat burgers vooral via Google op de gemeentelijke website terechtkomen en niet via het intypen van de url in de adresbalk van de internetbrowser. Dit komt ook doordat burgers steeds vaker internet gebruiken op hun smartphone. Het intypen van een url – en dan zeker een lange url - op een smartphone is lastig en deze wordt onleesbaar. Dus gebruiken burgers het zoekopdrachtveld van Google (bijvoorbeeld “paspoort Den Haag”) en komen dan direct op de juiste subpagina uit. Burgers gebruiken ook steeds vaker voice search.

GBBO[10] heeft voor deze impactanalyse uitgezocht hoe bezoekers op de gemeentelijke website terecht komen. In dit onderzoek aan de hand van de webstatistieken van 20 gemeenten blijken bezoekers in ruim 60% van de gevallen via een zoekmachine op de gemeentelijke website te komen. Het merendeel daarvan (meer dan 95%) gebruikt hiervoor Google. Ongeveer 30% van de bezoekers komt via direct verkeer op de site. In onderstaand figuur 3 is de verdeling te zien hoe bezoekers op de gemeentelijke site terecht komen. Ook komen bezoekers via een verwijzende website op de gemeentelijke site terecht.

Soms hebben burgers favorieten-linkjes in hun browser die ze aanklikken om de gemeentelijke site te bezoeken. Bij de gemeenten die een herindeling hebben meegemaakt, blijkt dat burgers jaren na de herindeling nog steeds via de oude favorietenlinkjes binnen komen op de nieuwe website. Het kost dus tijd om burgers deze linkjes te laten veranderen en gemeenten hebben hier geen directe invloed op.

[10] https://www.gbbo.nl/



Figuur 3. Herkomst bezoekers op gemeentelijke websites (Bron: GBBO, november 2019)

3.3. Certificaten

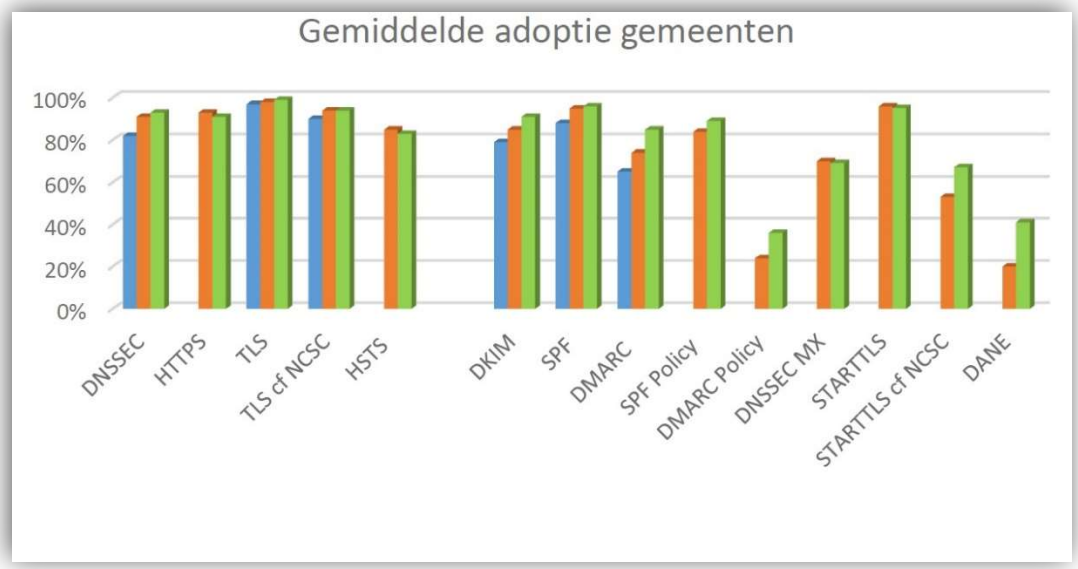
Gemeenten gebruiken certificaten om de website, email en devices (laptops, telefoons) te beveiligen. Ook worden er certificaten gebruikt in de verbindingen die met andere partijen worden gelegd of met applicaties in de cloud of op servers van leveranciers. Op deze certificaten wordt de gemeente geïdentificeerd aan de hand van de domeinnaam. Het aantal certificaten dat gemeenten hebben varieert sterk en hangt af van de keuzes die een gemeente maakt om de beveiliging van servers en werkplekken te regelen. Het aantal certificaten dat een gemeente in gebruik heeft, loopt sterk uiteen van zo'n 75 tot enkele honderden certificaten. De kosten per certificaat variëren tussen de € 250 en € 900 per certificaat, afhankelijk van het soort certificaat en de leverancier van het certificaat.

3.4. Toepassing beveiligingsstandaarden voor web en email

Het Forum Standaardisatie heeft op haar "Lijst open standaarden"[11] (gebaseerd op het 'pas toe of leg uit'-beleid) standaarden opgenomen voor web en email die gemeenten moeten toepassen. Door het gebruik van deze standaarden wordt de beveiliging van websites en overheidscommunicatie verbeterd. Over bepaalde standaarden zijn nadere afspraken gemaakt wat betreft het moment waarop overheidspartijen die standaarden verplicht moeten toepassen. Het Forum voor Standaardisatie doet twee keer per jaar (in maart en september) een meting naar de adoptie van deze standaarden bij de verschillende overheidspartijen. Voor gemeenten wordt dan gekeken naar

[11] https://www.forumstandaardisatie.nl/open-standaarden/lijst/verplicht

de hoofdwebsite (www.gemeentenaam.nl) en het bijbehorende emaildomein (@gemeentenaam.nl). In maart 2019 heeft het Forum haar meest recente rapport[12] uitgebracht. Ook in de aankomende wet Digitale Overheid wordt het gebruik van bepaalde beveiligingsstandaarden verplicht gesteld[13].

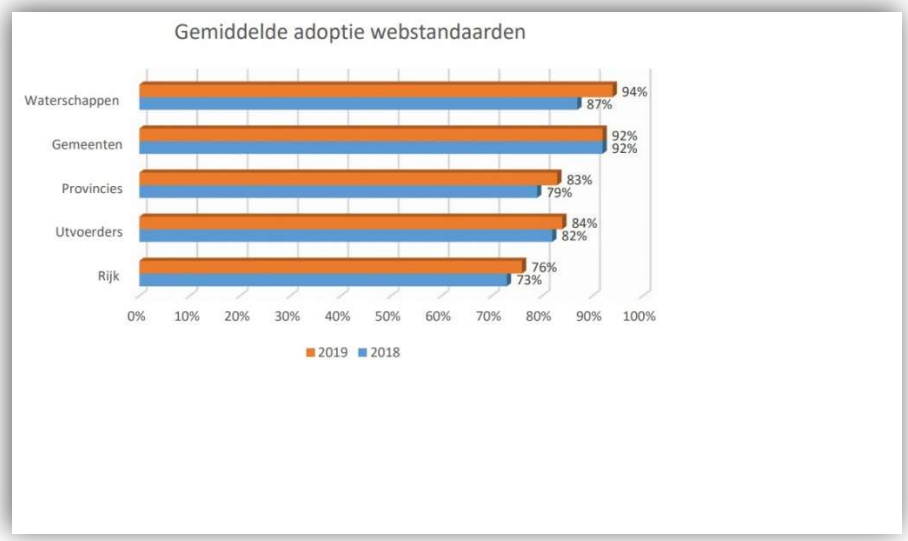


Figuur 4. Adoptie standaarden door gemeenten (onderzoek Forum Standaardisatie, maart 2019). De kleuren zijn de jaren 2017 (blauw), 2018 (oranje) en 2019 (groen). De eerste 5 standaarden zijn voor web, de overige standaarden voor email.

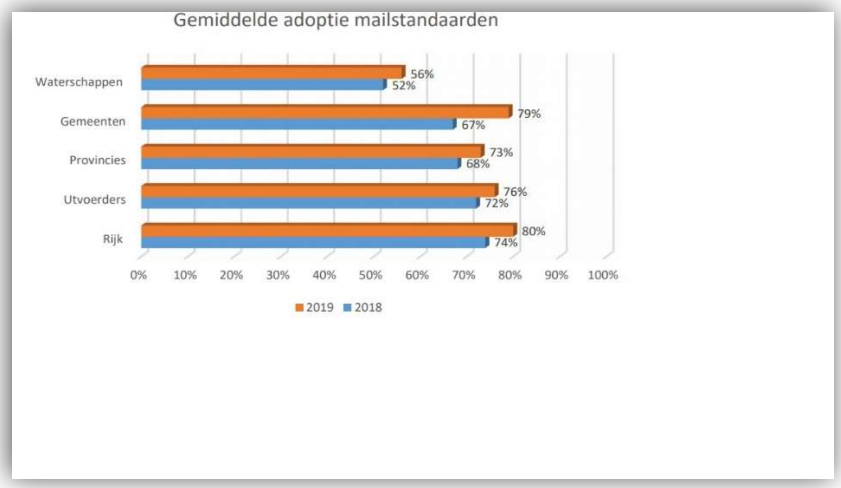
Uit figuur 4 wordt duidelijk dat de adoptiegraad van de beveiligingsstandaarden voor web bij gemeenten heel erg hoog is. De adoptie voor email is iets lager. Dat heeft ermee te maken dat de eisen hiervoor korter geleden zijn gesteld dan voor web. Ook speelt mee dat veel gemeenten Office 365 gebruiken en dat Microsoft niet alle standaarden ondersteunt. Dit wil overigens niet zeggen dat het maildomein daarmee niet veilig is, alleen wordt de veiligheid op een andere wijze geregeld dan door het toepassen van de door het Forum voor Standaardisatie vastgestelde standaarden.

Als we kijken naar de gemiddelde adoptie van de web- en mailstandaarden binnen de gehele Rijksoverheid, dan zien we dat gemeenten daarop hoog scoren. Zie figuren 5 en 6.

[12] https://www.forumstandaardisatie.nl/sites/bfs/files/190424%20Rapport%20IV-meting%20maart%202019%20v1.01.pdf
[13] https://www.tweedekamer.nl/kamerstukken/wetsvoorstellen/detail?cfg=wetsvoorsteldetails&qry=wetsvoorstel%3A34972



Figuur 5. Gemiddelde adoptie webstandaarden door de verschillende overheidslagen.



Figuur 6. Gemiddelde adoptie mailstandaarden door de verschillende overheidslagen.

4. Nieuwe situatie en impact voor gemeenten

In dit hoofdstuk wordt de nieuwe situatie beschreven die ontstaat als gekozen zou worden om een uniforme domeinnaamextensie voor de gehele overheid in te voeren. Ook wordt aangegeven welke impact dit heeft voor gemeenten. Eerst kijken we naar de scope van dit voorstel, dan naar de benodigde technische en overige aanpassingen, de communicatie, zaken rondom beheer en herkenbaarheid. En als laatste naar de implementatie en mogelijke alternatieven.

4.1. Scope

Het onderzoek van BZK bevindt zich nog in een verkennende fase. Dit betekent dat het voorstel voor een uniforme domeinnaamextensie nog niet tot in detail is uitgewerkt. Voor het bepalen van de nieuwe situatie voor gemeenten betekent dit dat er nog veel vragen leven, waarvan het antwoord bepalend kan zijn om de impact volledig in te kunnen schatten. Dit speelt onder andere bij de scope van het voorstel.

4.1.1. Alleen gemeentelijke hoofdsite of ook breder?

De impact voor gemeenten hangt sterk af van de keuze voor welke sites het voorstel gaat gelden. Gaat het *alleen* om de hoofdsite of ook *alle andere* sites die de gemeente beheert of waarin zij participeert? De impact wordt *groter* naarmate er *meer* sites onder vallen, maar voor de herkenbaarheid voor burgers ligt het voor de hand om alle sites mee te nemen. Anders gaat het effect verloren. Duidelijkheid over welke sites wel of niet onder de wijziging vallen is nodig om de exacte impact te kunnen bepalen.

4.1.2. Alleen sites voor inwoners of ook interne domeinnamen?

Een tweede vraag is of dit voorstel alleen geldt voor de buitenkant (dus de site voor de burger) of ook voor de interne domeinnamen voor de bedrijfsvoeringssoftware (werkplek.gemeenteX.nl, koppeling met basisregistraties etc.). Als ook de interne domeinnamen moeten worden aangepast, dan wordt de impact erg groot en de kosten stijgen substantieel (zie verderop in hoofdstuk 4).

4.1.3. Alleen website of ook maildomein?

Gaat het hier alleen om de website of ook om het emaildomein? Ook hier neemt de impact toe als het ook voor emaildomein gaat gelden, maar voor de herkenbaarheid voor de burgers zou het emaildomein ook meegenomen moeten worden. Zo niet, dan kan het verschil tussen de website (gemeentenaam.overheid.nl) en de mail (info@gemeentenaam.nl) verwarrend zijn voor burgers.

4.2. Technische aanpassingen

Gemeenten hebben aangegeven dat de huidige domeinnamen via een re-direct doorgestuurd zullen worden naar de nieuwe domeinnaam. Dat moet door de ICT-afdeling worden ingesteld. Daarnaast zijn er technische aanpassingen nodig (afhankelijk van de scope, zie hiervoor) aan certificaten. Voor het aanpassen van certificaten moet zowel de versturende partij (de gemeente) als de ontvangende partij (leverancier, ketenpartner) een aanpassing doen: er moet een nieuw

certificaat bij de gemeente geïnstalleerd worden, de ontvanger moet dit certificaat herkennen en deze verbinding moet getest worden.

De kosten voor het vervangen van certificaten kunnen we inschatten. Er moeten nieuwe certificaten aangevraagd worden, dit kost ongeveer 250 tot 900 euro per certificaat. Het aantal certificaten per gemeente hangt af van de manier waarop de gemeente de beveiliging heeft ingericht. Er zijn helaas geen cijfers over het aantal certificaten dat een gemeente heeft. In de tabel hieronder wordt een schatting gemaakt van hoeveel het landelijk vervangen van certificaten zal kunnen kosten.

Kosten voor vervangen certificaten
Voor elke e-overheidsvoorziening moeten er een certificaten zijn (ongeveer 15), voor koppelingen met backoffice applicaties, voor beveiliging van werkplekken, servers etc. De inschatting van de Informatiebeveiligingsdienst (IBD) is dat het om ongeveer 75-100 certificaten[14] per gemeente gaat. Op basis van 355 gemeenten gaat het om ongeveer 25.000 certificaten in Nederland. Gemeenten geven aan dat ze 250-900 euro per certificaat per jaar uitgeven. De inschatting van de IBD is dat dit bedrag verlaagd kan worden door certificaten in grotere hoeveelheden tegelijk aan te schaffen. In deze berekening wordt uitgegaan van 300 euro per certificaat. De kosten bedragen dan: 25.000 certificaten*300 euro = 7.5 miljoen euro voor het vervangen van de certificaten. Hier komen nog personeelskosten bij om certificaat te installeren en te testen (bij gemeente en ontvangende partij). Dit alles is een *inschatting* en hangt af van de manier waarop de gemeente de beveiliging van bijvoorbeeld werkplekken heeft geregeld (1 certificaat per werkplek of meerdere werkplekken achter een beveiliging).

4.3. Overige aanpassingen

Uiteraard moeten gemeenten ook communicatie-uitingen aanpassen waar de domeinnaam op wordt gebruikt. Denk hierbij aan printwerk (folders, flyers etc), visitekaartjes, soms belettering van auto's of gebouwen, drukwerk voor de bekendmakingen in lokale media. Maar ook aan het aanpassen van briefsjablonen in diverse systemen. Daarvoor moeten leveranciers inspanningen verrichten en die zullen daar kosten voor in rekening brengen.

Gemeentelijke medewerkers zullen ook hun digitale handtekening onderaan mails moeten aanpassen en communiceren met hun relaties over een aangepast emailadres.

Daarnaast is een belangrijke aanpassing dat ook partijen die verwijzen naar de gemeentelijke sites hun verwijzing moeten aanpassen naar de nieuwe domeinnaam. Hier zal ook over

[14] Overigens geeft de G4 gemeente in het onderzoek aan dat zij honderden certificaten in gebruik hebben. Die hier genoemde 75-100 certificaten zijn dus voor een grote gemeente een onderschatting.

gecommuniceerd moeten worden en het is de vraag of gemeenten weten welke partijen naar gemeentelijke sites verwijzen.

Gemeenten geven aan dat “vergeten worden door Google” lastig is en inspanning vereist: oude domeinnamen zullen nog vrij lang in de zoekresultaten omhoog komen. Tevens moet je met een nieuwe site weer bovenaan komen in de zoekresultaten en dat vereist inspanning.

Een lange domeinnaam is niet wenselijk in de schriftelijke communicatie, maar ook mondeling lastiger te communiceren. Dit is nog sterker het geval bij gebruik van subdomeinnamen, bijvoorbeeld: www.belastingen.gemeenteX.overheid.nl.

Ook bij deze zaken gaat het om eenmalige wijzigingen, maar die zijn wel fors en kosten geld en tijd.

4.4. Communicatie richting inwoners

Het doel van de invoering van een uniforme domeinnaamextensie is onder andere dat burgers overheidswebsites beter kunnen herkennen. Daarvoor is het volgens gemeenten van belang dat, als dit voorstel doorgevoerd wordt, alle overheidspartijen van dezelfde overheidslaag meedoen en dat er een landelijke campagne komt om burgers hierover te informeren. Door een landelijke campagne op te zetten waar gemeenten lokaal op kunnen aansluiten, worden gemeenten enigszins ontlast in het communiceren over deze verandering richting hun inwoners. Tevens wordt er dan namens de gehele overheid één boodschap uitgezonden.

4.5. Beheer *.overheid.nl

Het is van belang om te weten welke partij *.overheid.nl gaat registreren en beheren. Bij die partij moeten gemeenten namelijk het verzoek indienen om een eigen site aan te maken. Nu kunnen gemeenten bij commerciële partijen een domeinnaam aanvragen. Gemeenten geven aan dat de procedure voor het aanvragen van een domein snel en efficiënt moet verlopen. Bij centraal beheer van *overheid.nl zullen er eisen gesteld worden aan het mogen aanvragen van een domein op *.overheid.nl. Voor gemeenten is van belang om te weten wat deze eisen zijn.

De IBD ziet mogelijke voordelen wanneer er een centrale DNS provider wordt ingericht met multifactorauthenticatie en controle op de persoon die de aanvraag voor een nieuw subdomein mag indienen. Tevens zal door de strengere selectie van domeinnamen typo-squatting lastiger worden. Hier ziet de IBD kansen om de beveiliging te verbeteren; door strenge regulatie, selectie en mogelijk zelfs herkeuring elke paar jaar bepaalt de overheid welke organisatie het *.overheid.nl domein mag gebruiken en mogelijk ook wie weer moet vertrekken bij het niet nakomen van afspraken.
Het invoeren van een uniforme domeinnaamextensie vereist bij gemeenten echter behoorlijk wat resources (geld, personeel), waarbij de vraag is of deze niet beter voor andere maatregelen (die meer security impact hebben) kunnen worden ingezet.

De vraag is ook of het samenvoegen van alle overheidswebsites onder *.overheid.nl niet gaat leiden tot een *single point of failure* en een aantrekkelijke manier voor hackers om de gehele overheid in één keer aan te vallen. Ook de Informatiebeveiligingsdienst wijst op dit risico:

gemeenten vormen op dit moment nog nauwelijks een doelwit voor bepaalde (statelijke) actoren. Dit in tegenstelling tot bepaalde rijkspartijen. Een deels centrale en goed herkenbare infrastructuur zou gemeenten opeens ook zo'n doelwit kunnen maken.

4.6. Herkenbaarheid

Gemeenten herkennen het beeld dat burgers valse overheidswebsites niet kunnen onderscheiden van echte niet voor hun eigen gemeentelijke websites. Dit lijkt in tegenspraak te zijn met het onderzoek van Kantar. In dat onderzoek wordt echter aangegeven dat burgers vooral twijfelen aan de echtheid van overheidswebsites als ze niet bekend zijn met die naam van de organisatie die de dienst aanbiedt. De naam van de gemeente waar de burger woont of zaken mee doet, is echter bij die burgers wel bekend. Daarmee is het invoeren van een uniforme domeinnaamextensie voor veel gemeenten een oplossing voor een niet bestaand probleem. Met dit project zijn echter wel flinke kosten gemoeid. De gemeenten die we hebben gesproken zijn over het algemeen niet positief over dit voorstel. Een goed onderbouwde probleemstelling en financiële compensatie vanuit het Rijk is nodig om binnen de gemeente ambtelijk en bestuurlijk akkoord te krijgen om deze wijziging door te voeren.

Uit de gesprekken:

"Onze inwoners zijn gewend aan onze domeinnaam, ook als die afwijkt van de gebruikelijk www.gemeentenaam.nl."

"Dit voorstel tot uniformeren van de domeinnaam komt eigenlijk 20 jaar te laat en is nu niet zinvol meer voor de gemeentelijke wereld."

"Het invoeren van een andere domeinnaam gaat veel geld kosten en gaat, naar onze mening, te weinig opleveren voor onze burgers qua herkenbaarheid en beveiliging. We besteden het hiervoor benodigde geld liever aan zaken waar burgers echt mee geholpen zijn."

"Als gemeente hebben we onze eigen verantwoordelijkheid met betrekking tot beveiliging van onze website en achterliggende systemen. We nemen die verantwoordelijkheid heel serieus en we denken niet dat de invoering van een uniforme domeinnaamextensie hier iets aan bijdraagt."

4.7. Implementatie

Gemeenten zijn niet positief over het voorstel. In de gesprekken zijn we ingegaan op de vraag wat er nodig zou zijn voor een landelijke implementatie als dit voorstel toch wordt doorgezet. Gemeenten hebben randvoorwaarden benoemd voor een succesvolle implementatie van de uniforme domeinnaamextensie:

- Invoering van een uniforme domeinnaamextensie moet op basis van een *wettelijke verplichting*: alle overheidspartijen, in ieder geval alle partijen binnen dezelfde overheidslaag (dus bijvoorbeeld alle gemeenten), moeten meedoen, anders gaat niet iedereen mee doen en wordt het doel rondom herkenbaarheid niet gehaald
- Deze invoering moet gepaard gaan met een *landelijke campagne* richting de burgers. Dit heeft als consequenties dat alle overheidspartijen in een korte periode over moeten gaan, dus een soort *Big Bang*.

- Zorg ervoor dat softwareleveranciers *tijd* krijgen om de technische aanpassingen te doen voor al hun klanten. Dit kan ook een knelpunt zijn in de doorlooptijd.
- Gemeenten hebben behoefte aan een goede *probleemstelling* over de *noodzaak en het beoogde effect* van deze maatregel om dit aan college en raad (en ook breder binnen hun eigen organisatie) te 'verkopen'. Het project zal gemeenten geld en tijd kosten, dit moet goed onderbouwd en financieel gecompenseerd worden.
- Gemeenten willen de domeinnaam *centraal registreren*, maar wel *lokaal* kunnen *beheren* (anders verwachten zij veel vertraging bij het aanvragen van wijzigingen).
- Er moeten *handreikingen* komen voor technische aanpassingen, communicatie etc.

4.8. Keuze voor domeinnaamextensie

Het ministerie van Binnenlandse Zaken heeft nog geen definitieve keuze gemaakt voor de domeinnaamextensie die mogelijk gebruikt gaat worden. In de interviews en enquête is aan de gemeenten gevraagd welke extensie hen het meest aanspreekt. In de tabel hieronder staat een overzicht van de benoemde voordelen en nadelen per mogelijke extensie.

Naam	Voordeel	Nadeel
*.overheid.nl	Uniform en herkenbaar	Erg lang.
*.gov.nl	Kort	Te amerikaans, .gov bij ons niet gebruikelijk,
*.gemeente.nl	Localiteit	Lang; Onderscheid in overheidslaag, dan ga je doel voorbij van een herkenbare overheid.
Genoemd: *.gem of *.gemeente	Kort, herkenbaar	Ook hiermee onderscheid overheidslaag en dus ga je het doel herkenbare overheid voorbij.

Tabel 1. Overzicht voor- en nadelen per mogelijke extensie.

Uit dit overzicht blijkt dat gemeenten niet willen dat de domeinnaam te lang wordt en ook dat het niet wenselijk is dat er voor de gemeentelijke laag een aparte naam komt.

4.9. Alternatieve (en mogelijk effectievere) oplossingen

Gemeenten vragen zich af waarom de oplossing voor het herkenbaar maken van de overheid wordt gezocht bij een uniforme domeinnaamextensie. Ze vragen zich af of er geen betere manieren zijn om overheidswebsites herkenbaar te maken. Gemeenten denken dan aan eisen rondom toegankelijkheid en eenduidige vormgeving van websites. Deze alternatieven zijn in deze impactanalyse niet nader onderzocht, maar werden wel door meerdere gemeenten in de interviews genoemd. Ook gaven de meeste gemeenten die we hebben gesproken aan dat ze zelf al bezig zijn met het verbeteren van de herkenbaarheid en toegankelijkheid en beveiliging van hun websites.

5. Conclusies

In dit hoofdstuk worden de resultaten van deze impactanalyse gegeven: welke impact heeft het invoeren van een uniforme domeinnaamextensie voor gemeenten? In elke paragraaf wordt een onderzoeksvraag beantwoord.

5.1. Wijzigingen in de werkwijze van gemeenten

Als gemeenten worden gevraagd om de domeinnaam voor website en email aan te passen, dan brengt dit voor een groot deel eenmalige aanpassingen met zich mee. Het beheren van de nieuwe domeinnaam zal niet anders zijn dan het huidige beheer van de domeinnaam. Voor het beheren veranderen de werkzaamheden niet.
Het zou wel kunnen dat het aanvragen van een domeinnaam via een andere partij gaat verlopen dan nu het geval is, namelijk de eigenaar van *.overheid.nl. Gemeenten willen graag dat het uitgangspunt is dat deze aanvraag snel en efficiënt verloopt en dat daar geen tijd wordt verloren door lange wachttijden of procedures.
Ook het aanpassen van de communicatie-uitingen waarop de website of emailadressen worden genoemd is eenmalig en daarna niet anders dan in de huidige situatie. Dat geldt ook voor het beheren van de certificaten.
Gemeenten zullen voor het aanpassen van de domeinnaam een project moeten inrichten om dit te organiseren. Hiervoor moet geld en personeel beschikbaar gesteld worden voor een bepaalde periode.

Conclusie onderzoeksvraag 1
Invoering van een uniforme domeinnaamextensie gaat vooral gepaard met eenmalige werkzaamheden. Na de invoering veranderen de werkzaamheden niet of nauwelijks ten opzichte van de huidige situatie.

5.2. Impact van deze wijzigingen voor gemeenten

In de interviews is met gemeenten besproken welke impact het wijzigingen van de domeinnaam voor website en email heeft. Hieronder worden de relevante aspecten toegelicht.

5.2.1. Impact op gemeentelijk beleid

Niet alle gemeenten hebben nu beleid voor het aanmaken van domeinnamen. Daardoor hebben gemeenten onvoldoende zicht op welke domeinnamen er geregistreerd zijn, welke nog actief zijn, welke beveiligingsmaatregelen er worden toegepast en of de toegankelijkheid op orde is.
Onafhankelijk van het traject rondom uniforme domeinnaamextensie is het wenselijk dat gemeenten hierop beleid ontwikkelen.

Aanbeveling
Ontwikkel als gemeente beleid op het aanvragen en beheren van domeinnamen. Bepaal wie een domeinnaam mag aanvragen, in welke situaties een nieuwe domeinnaam toegestaan is, welke eisen je stelt aan toegankelijkheid, herkenbaarheid en beveiliging. Hierin is een rol voor de ICT afdeling en voor communicatie weggelegd. Deze aanbeveling staat los van de vraag of er een uniforme domeinnaamextensie ingevoerd zal worden.

5.2.2. Personele impact

Zoals eerder geconstateerd, gaat het hier vooral om eenmalige aanpassingen. Er zal een projectteam geformeerd moeten worden en dat kost dus incidenteel extra inzet van personeel. Dit team zal de technische aspecten moeten regelen, de communicatie-uitingen moeten (laten) aanpassen en een communicatiecampagne moeten starten. Hiervoor is budget nodig en een financiële compensatie vanuit het Rijk. De omvang van deze personele impact is op dit moment moeilijk te bepalen, omdat een concreet uitgewerkt voorstel nog ontbreekt.

Aanbeveling
Zorg vanuit het ministerie voor een duidelijke probleemstelling en beschrijving van de noodzaak van deze aanpassing, zodat gemeenten bestuurlijk geld en capaciteit kunnen regelen. Tevens is financiële compensatie gewenst.

5.2.3. Impact op de techniek en informatievoorziening

De impact op techniek en informatievoorziening hangt af van de vraag wat de scope is van deze wijziging (zie paragraaf 3.2). Gaat het alleen om de hoofdwebsite, dan is de impact beperkt. Maar als het ook gaat om alle andere gemeentelijke websites en de email, dan is de impact groot. Wederom gaat het om vooral eenmalige aanpassingen, maar dat kunnen er – afhankelijk van de scope – veel zijn.

Bij een brede scope (alle gemeentelijke websites en email) moeten in elk geval de volgende zaken aangepast worden:

- Intern moeten alle certificaten aangepast worden (zowel aan kant van de gemeente als kant van leverancier/ketenpartner; dit moet ook door beide partijen getest worden). Het aantal certificaten verschilt per gemeente, maar dit kan een aanzienlijk aantal zijn.
- Mailadressen en active directory (emailadres wordt vaak ook als inlognaam gebruikt) aan passen.
- Instellen van een re-direct naar de nieuwe website (kost geld).

Het aantal domeinnamen dat een gemeente heeft, zal door de invoering van een uniforme domeinnaamextensie *niet* minder worden. Om misbruik te voorkomen (en tijdelijk een re-direct te kunnen doen), zullen gemeenten de oude domeinnaam lange tijd en misschien wel permanent behouden.

5.2.4. Impact op de communicatie door gemeenten

Gemeenten zullen op meerdere plekken communicatie-uitingen moeten aanpassen, zowel op papier alsook digitaal. Ook externe partijen die op hun website verwijzen naar de gemeentelijke site moeten hun verwijzing aanpassen.
Gemeente en hun medewerkers zullen moeten communiceren naar externe partners over aangepaste mailadressen (die staan vaak in adresboek en moeten worden aangepast). Uit de ervaring van gemeenten na een herindeling blijkt dat het nog jaren kan duren voor mensen emailadressen aan hebben gepast. Gedurende langere tijd zullen gemeenten dus moeten werken met 2 emailadressen.
In aanloop naar de overgang zal een goede communicatiecampagne nodig zijn om inwoners te informeren over de wijziging. Het heeft de voorkeur van gemeenten als deze campagne landelijk georganiseerd wordt.

Aanbeveling
Om gemeenten te ontlasten in de communicatie is het wenselijk dat er een landelijke communicatiecampagne wordt gestart die de herkenbaarheid en betrouwbaarheid van een *.overheid.nl website toelicht en onderstreept. Houd ook rekening met andere partijen die op hun site verwijzen naar de gemeentelijke site. Ook deze partijen zullen aanpassingen moeten doen.

Conclusie onderzoeksvraag 2
De impact van de invoering van een uniforme domeinnaamextensie betreft vooral eenmalige werkzaamheden. De impact – zeker qua technische aspecten – kan echter wel heel groot zijn. Dit zal afhangen van de gekozen scope. Tevens zijn de aanpassingen dus niet beperkt tot de gemeenten, maar worden ook andere partijen hierdoor geraakt.

5.3. Doeltreffende uitvoering door gemeenten

Gemeenten hebben veel vragen bij nut en noodzaak van dit voorstel. Mocht BZK er desondanks voor kiezen om over te gaan tot invoering van een uniforme domeinnaamextensie, dan zien gemeenten een aantal belangrijke voorwaarden om het voorstel doeltreffend te kunnen uitvoeren.

Als ervoor wordt gekozen om deze maatregel door te voeren, dan moet het ook een wettelijke verplichting moet zijn: alle overheidsorganisaties in dezelfde laag moeten mee doen, anders ontstaat alsnog veel onduidelijkheid doordat bijvoorbeeld het ene deel van de gemeenten wel meedoet en een ander deel niet. Hierbij trekken veel gemeenten de parallel met de implementatie van het 14+ netnummer, waar momenteel een deel van de gemeenten wel aan deelneemt en een deel niet. Dit leidt tot onduidelijkheid voor burgers.

Als dit voorstel daadwerkelijk wordt doorgevoerd, hebben gemeenten de wens uitgesproken voor een landelijke campagne waar lokaal op aangesloten kan worden. Dit zorgt voor een eenduidige

communicatie, geeft naar burgers een gelijk beeld voor de gehele overheid en voorkomt dat iedere organisatie zelf moet communiceren.
Gemeenten geven daarbij wel het volgende aan: als je kiest voor een landelijke campagne, dan kan de overgangsperiode niet al te groot zijn. Dan verdwijnt namelijk het effect van die landelijke campagne. Hierbij zien gemeenten als risico dat als alle overheidspartijen tegelijk over gaan (of in een beperkte periode), dit een grote impact heeft voor leveranciers om dit te ondersteunen (als je kiest voor: ook intern domeinnamen aanpassen). Het tempo waarin overheden de nieuwe domeinnaam in gebruik kunnen nemen, hangt dan vermoedelijk af van de capaciteit die de leveranciers hebben om de certificaten te installeren en te testen, aanpassingen aan systemen te kunnen doen (aanpassen brief sjablonen etc), etc. Om dit risico te beperken is een ruime voorbereidingstijd voor leveranciers van belang.

Gemeenten willen de domeinnaam centraal registreren bij de eigenaar van *.overheid.nl, maar ze willen het beheer van hun subdomein wel lokaal kunnen doen om snel te kunnen schakelen als er een nieuwe subsite nodig is.

Als het voorstel doorgaat, dan hebben gemeenten behoefte aan stappenplannen, handreikingen voor technische aanpassingen, communicatie etc.

Conclusie onderzoeksvraag 3

Voor een eventuele invoering van de uniforme domeinnaamextensie noemen gemeenten de volgende zaken als randvoorwaardelijk voor een doeltreffende uitvoering:

- Wettelijke verplichting
- Landelijke campagne
- Ruime voorbereidingstijd, ook voor leveranciers en ketenpartners
- Centrale registratie, lokaal beheer
- Duidelijke informatie in de vorm van handreikingen en stappenplannen

5.4. Mogelijke kosten en besparingen voor de gemeentelijke uitvoering

De aanpassingen (technisch en communicatief) brengen kosten met zich mee, onder andere door de benodigde extra personele capaciteit om de wijzigingen door te voeren. Deze inzet is zowel aan de kant van de gemeente nodig als aan de kant van ketenpartners of leveranciers (voor aanpassingen verwijzingen en invoeren en testen nieuwe certificaten). Er zijn geen algemene uitspraken gedaan over hoe hoog deze kosten zijn. Een goede inschatting kan gemaakt worden zodra er meer duidelijkheid is over de scope en de concrete invulling van het voorstel.

De kosten rondom certificaten hebben we in dit onderzoek ingeschat op minimaal 7,5 miljoen euro. Dit is exclusief de bijkomende personele kosten.

Het invoeren van een uniforme domeinnaamextensie levert voor de gemeenten *geen besparingen* op. Het aantal domeinnamen zal niet minder worden, omdat de huidige domeinnamen toch aangehouden worden door de gemeente om misbruik te voorkomen (zie ook de huidige werkwijze na een herindeling). Ook is er *geen verlichting van de beheer-werkzaamheden*.

Gemeenten vinden de beoogde voordelen van de maatregel niet opwegen tegen de kosten die met de maatregel gepaard gaan. Dit maakt het een lastige keuze om aan college en raad voor te leggen, met name gezien de financiële tekorten in het sociaal domein. Een financiële compensatie vanuit het Rijk is wenselijk.

Conclusie onderzoeksvraag 4
De kosten die met de invoering van een uniforme domeinnaamextensie gepaard gaan voor gemeenten zijn hoog. Hier staan nauwelijks besparingen tegenover. Ook dit leidt ertoe dat gemeenten niet positief staan tegenover de invoering van een uniforme domeinnaamextensie.

Aanbeveling
Indien gekozen wordt om een uniforme domeinnaamextensie in te voeren, dan is het wenselijk dat gemeenten voor deze kosten gecompenseerd worden op basis van artikel 2, Wet Financiële Verhoudingen.

5.5. Bereiken beoogde effecten

De vraag is of gemeenten verwachten dat het beoogde effect, herkenbaarheid en betere beveiliging, door het invoeren van een uniforme domeinnaamextensie wordt bereikt. Dit is de vijfde onderzoeksvraag.

5.5.1. Herkenbaarheid

Gemeenten herkennen de probleemstelling dat burgers een overheidswebsite niet als zodanig herkennen **niet** voor hun eigen gemeentelijke website(s). Gemeenten geven aan dat er *geen* signalen zijn dat hun burgers/ondernemers problemen hebben met de herkenbaarheid van de huidige domeinnaam, ook niet bij de gemeenten met een afwijkende domeinnaam. Burgers zijn bij gemeenten met afwijkende domeinnamen (anders dan ‘gemeentenaam.nl’) daar inmiddels aan gewend en komen überhaupt voor het grootste deel via Google binnen.

Gemeenten erkennen dat de herkenbaarheid van (gemeentelijke) sites vergroot kan worden, maar zien meer mogelijkheden in bijvoorbeeld het uniformeren van de lay-out of het aanbieden van standaardprocessen via overheid.nl en alleen lokale informatie en maatwerk via de eigen site. Aandachtspunt hierbij is wel dat er voldoende ruimte blijft voor de *couleur locale*, dit is met name politiek/bestuurlijk van belang. Deze alternatieven zijn in deze impactanalyse als suggestie opgetekend, maar niet nader onderzocht.

Een gemeentelijke site verwijst naar tientallen applicaties en andere sites: daar moet je (ook) de herkenbaarheid regelen. Eén domeinnaamextensie helpt daar niet bij.

Inwoners hebben soms jaren nodig om te wennen een nieuwe domeinnaam/mailadres. Dit blijkt onder andere uit het feit dat inwoners van heringedeelde gemeenten soms nog jaren na de herindeling via de url van één van de voormalige gemeenten binnenkomen op de website.

Aanbeveling
Het is wenselijk met gemeenten in gesprek te gaan over de manier waarop de herkenbaarheid van gemeentelijke sites voor burgers verbeterd kan worden. Hier is mogelijk een rol voor de VNG, Kenniscentrum Dienstverlening VNG Realisatie en de VDP.

5.5.2. Beveiliging

Gemeenten zien dat het goed beveiligen van de website als hun eigen verantwoordelijkheid. De meeste gemeenten noemen ook concreet maatregelen die ze hiervoor genomen hebben. Zowel gemeenten als de IBD geven aan dat door op *.overheid.nl bepaalde standaarden toe te passen, de beveiliging van de achterliggende applicaties en servers nog niet is gegarandeerd. Dat moet een gemeente toch zelf organiseren. Het is dus slechts beperkt mogelijk om een betere beveiliging af te dwingen via een uniforme domeinnaamextensie. Daarbij is in de gemeentelijke wereld het toepassen van beveiligingsstandaarden in het algemeen erg goed op orde. De vraag is of het invoeren van een uniforme domeinnaamextensie met als doel het verbeteren van de veiligheid voor gemeentelijke websites effectief is.

Conclusie onderzoeksvraag 5
Gemeenten herkennen niet dat de probleemstelling van beperkte herkenbaarheid overheidswebsites en verbeteren beveiliging voor de gemeentelijke websites opgelost kan worden door het invoeren van een uniforme domeinnaamextensie. Gemeenten zien wel dat er mogelijkheden zijn de herkenbaarheid en toegankelijkheid van gemeentelijke websites te verbeteren. Op het gebied van beveiliging nemen gemeenten hun verantwoordelijkheid al, gezien de hoge score op de toepassing van de juiste standaarden.

5.6. Randvoorwaarden en risico’s

Gemeenten hebben verschillende risico’s voor de implementatie van de uniforme domeinnaamextensie benoemd. Bij deze een opsomming:

- Het gaat hier om een ingrijpende verandering die naar inschatting van de gemeenten niet of onvoldoende tot het gewenste effect zal leiden
- Vermoedelijk is er weinig draagvlak bij raad, college en de interne organisatie omdat de meerwaarde van het voorstel onvoldoende is aangetoond
- Gemeenten vrezen als niet alle overheidsorganisaties van dezelfde laag deze wijziging doorvoeren er juist onduidelijkheid voor burgers ontstaat.
- Gemeenten geven aan dat een bureaucratisch proces van aanvragen van websites bij centrale beheerorganisatie hen zal belemmeren.

Voor de implementatie van de uniforme domeinnaamextensie zijn de volgende randvoorwaarden benoemd:

- Er moet een uitgewerkt voorstel komen, waarin de scope helder is en het beoogde effect aantoonbaar wordt gemaakt voor gemeenten.
- De invoering moet uitgaan van een wettelijke verplichting, zodat alle gemeenten verplicht worden mee te doen
- Vanuit het Rijk dient er een landelijke communicatiecampagne ingericht te worden om deze naamswijzigingen toe te lichten.

- Er dient rekening gehouden te worden met de tijd die leveranciers nodig hebben om gemeenten te helpen met het doorvoeren van deze veranderingen.
- Gemeenten dienen voor deze invoering gecompenseerd te worden op basis van artikel 2 (Wet Financiële verhoudingen).

Aanbeveling
Mocht het ministerie BZK dit traject willen doorzetten, dan is het wenselijk dat de VNG het draagvlak voor dit voorstel via de bestuurlijke commissies nader gaat onderzoeken.

Conclusie onderzoeksvraag 6
Voor een eventueel vervolg dient rekening te worden gehouden met de benoemde randvoorwaarden en dienen de risico's aangepakt te worden.

Bijlage A – Gesprekspartners

Voor deze impactanalyse is gesproken met de volgende organisaties en personen:

Organisatie	Naam
Gemeente Best	senior communicatie, beveiligingsfunctionaris, senior adviseur informatie, ICT-coördinator
Gemeente ‘s-Hertogenbosch	ICT-coördinator, online strateeg communicatie, afdelingshoofd ICT, ICT beheerder
Gemeente Leiden	Webmaster
Gemeente Nijkerk	Medewerker communicatie, Beheerder website, Ciso.
Gemeente Krimpenerwaard	Informatiemanager, Communicatie, Adviseur I&A, KCC
Gemeente Noordoostpolder	Projectleider informatie dienstverlening, Webbeheer en Kabinetszaken
Gemeente Súdwest Fryslân	Informatiemanager, eindredacteur website, ICT architect, projectleider nieuwe website.
Gemeente Midden-Delfland	Communicatieadviseur/webmaster, Backoffice-medewerker KCC, adviseur informatievoorziening en -beveiliging
Gemeente Molenlanden	adviseur informatievoorziening en -beveiliging, strategisch informatieadviseur
Gemeente Leidschendam-Voorburg	Programmamanager Moderne overheid, Eindredacteur website, communicatie adviseur, informatiemanager.
Gemeente Den Haag	Product owner website, Adviseur CIO office, solution architect van website
Gemeente Goeree-Overflakkee	Communicatieadviseur, beleidsadviseur I&A
Informatiebeveiligingsdienst Gemeenten	Team coördinator IBD, adviseur informatiebeveiliging

Leden van de begeleidingscommissie:

Organisatie	Naam
Ministerie van Binnenlandse Zaken	Rob Ramdjilal (projectleider), Dirk Maats (secretaris)
Vereniging Nederlandse Gemeenten (VNG)	Peter van Dijk, Roxane Daniels
VNG Realisatie	Pieter Pinxten
Vereniging Directeuren Publieksdiensten	Jan Fraanje

Bijlage B - Vragenlijst interviews

Achtergrond:

- Hoeveel gemeentelijke domeinnamen en hoeveel websites heeft deze gemeente?
- Hoe vaak komen er domeinnamen/websites bij en hoe vaak worden ze opgeheven?
- Heeft gemeente beleid voor het aanmaken van websites en de naamgeving?
- Welke inspanningen moet een medewerker verrichten om een website/domeinnaam te creëren?
- Welke kosten zijn hiermee gemoeid?
- Op welke producten/locaties staat een verwijzing naar een website? Digitaal en analoog.
- Heeft de gemeente (recent) ervaring met het wijzigen van de domeinnaam, bijvoorbeeld door herindeling of naamswijziging van de gemeente? Hoe is dat verlopen?
- Ervaart de gemeente momenteel wel eens nadelen van het niet hebben van een uniforme domeinnaam: domeinnaam die al door een (commerciële) partij in gebruik is (vb Nijkerk, Best), andere domeinnamen die sterk lijken op de domeinnaam van de gemeente, etc.?
- Heeft de gemeente ervaringen waaruit blijkt dat inwoners of bedrijven last hebben van de huidige domeinnaam, door onherkenbaarheid, verkeerde verwijzing door typefouten, etc.?

Voorstel: 1 uniforme domeinnaamextensie voor alle overheidswebsites en mogelijk ook voor emailadressen. Daarmee eenduidiger beeld van de overheid, minder risico's qua beveiliging etc.

- Welke voordelen zien gemeenten in gebruik van een uniforme domeinnaamextensie en welke nadelen?
- Op welke plekken heeft dit voorstel impact?
- Wat betekent dit voorstel voor het werk van de functioneel beheerder? En van vakafdelingen, communicatie etc?
- Gebruiken de gemeente emailadressen als inlognamen voor andere systemen?
- Wat kost het wijzingen van certificaat en domeinnaam?
- Welke kosten denkt de gemeenten dat dit voorstel met zich meebrengt op korte termijn? En op lange termijn?
- Welke baten ziet de gemeente?
- Hoeveel tijd zou de gemeente nodig hebben om over te gaan naar nieuwe domeinnaamextensie?
- Welke ondersteuning zou de gemeente nodig hebben?

Voorkeur extensie en scenario:

- Er is nog geen keuze gemaakt in de mogelijk te gebruiken domeinnaam: overheid.nl of gov.nl of een andere optie. Mogelijk kan er ook gekozen worden voor .gemeente.nl. Dus amsterdam.overheid.nl of amsterdam.gemeente.nl. Welke voorkeur heeft deze gemeente?
- Er zijn nu verschillende scenario's voorzien om over te gaan naar een uniforme domeinnaam: 'big bang' (alle overheidsorganisaties tegelijk over), overgang per type overheidsorganisatie, organische overgang (nog aanscherpen welke scenario's dit zijn). Welk scenario heeft de gemeentelijke voorkeur?

Overige:

- Zien gemeenten kansen om zaken gezamenlijk te organiseren?
- Aanvragen domeinnaam: wil gemeente dat zelf doen of gaat dit lopen via de eigenaar van overheid.nl/gov.nl? Welke voorkeur heeft de gemeente?
- Beheer van certificaten zal niet centraal worden geregeld en ook DNS wordt niet centraal aangeboden. Daarmee is de vraag of de beheerlast voor gemeenten gaat veranderen. Hoe schat de gemeente dit in?

XXXXXXXX

Bijlage C – Gebruikte bronnen

Voor deze impactanalyse is gebruikgemaakt van de volgende bronnen:

Internet

- Onderzoek Kantar, https://www.rijksoverheid.nl/documenten/rapporten/2019/01/31/herkenbaarheid-van-en-vertrouwen-in-websites-en-e-mails-van-de-overheid.
- Onderzoek Novay, https://kennisopenbaarbestuur.nl/media/23353/een-top-level-domein-voor-betrouwbare-overheidscommunicatie.pdf
- Koken met Data, VNG Realisatie, https://publicaties.vngrealisatie.nl/2017/koken-met-data/recept-6-exploratief-onderzoek-naar-bezoek-gemeentelijke-websites/, April 2017.
- Lijst verplichte open standaarden, Forum Standaardisatie, https://www.forumstandaardisatie.nl/open-standaarden/lijst/verplicht
- Rapport IVmeting, Foum Standaardisatie, maart 2019, https://www.forumstandaardisatie.nl/sites/bfs/files/190424%20Rapport%20IV-meting%20maart%202019%20v1.01.pdf