Forum Standaardisatie
Standaard Samenwerken

Adviesrapport internetdomeinbeleid: Een centrale aanpak met overheidsbreed bereik

Het aanpakken van de micro -en macroproblematiek van internetdomeinbeheer door decentrale verantwoordelijkheden centraal te faciliteren

Datum document: 26 april 2022

Status document: Definitief

Inhoudsopgave

1. Conclusie en managementsamenvatting

1.1. Conclusie

In het onderzoek ‘overheidsbreed internetdomeinbeleid’ is gezocht naar een antwoord op de vraag ‘Hoe ziet overheidsbreed internetdomeinbeleid er idealiter uit?’. Om deze vraag te beantwoorden is kwalitatief onderzoek verricht door het voeren van gesprekken met relevante stakeholders.

Uit analyse van de onderzoeksopbrengsten is gebleken dat internetdomeinbeheer zowel decentraal als centraal nog onvoldoende volwassen is ingericht. Hierdoor ontbreekt het aan een effectief sturingsinstrument om grip te krijgen op het portfolio van internetdomeinen van de overheid. Gevolg is dat de herkenbaarheid en veiligheid van de digitale overheid in het geding komt. Een herkenbare en veilige digitale overheid is cruciaal voor burgers en ondernemers.

Om internetdomeinbeheer binnen de gehele overheid naar een hoger volwassenheidsniveau te brengen, zijn in dit onderzoek tien oplossingsrichtingen geïdentificeerd en uitgewerkt:

1. Register Internetdomeinen Overheid (RIO).
2. Herkenbare overheidsextensie (.gov.nl/.overheid.nl)
3. Centrale overheidsregistrar
4. Centrale afspraken omtrent levenscyclusbeheer
5. Beleggen van verantwoordelijkheden en rollen
6. Eisen voor externe leveranciers
7. Intern verplichte periodieke kwaliteitscontroles
8. Centraal vormgeven van toezicht, monitoring en handhaving
9. Interbestuurlijke werkgroep waarbij iedere overheidslaag is gerepresenteerd
10. Intern interdisciplinair expertiseteam

De tien oplossingen spelen in op de geconstateerde knelpunten, behoeften en belangen van overheidsorganisaties. Uit het onderzoek blijkt dat het draagvlak voor deze oplossingen groot is: de stakeholders zien in het ideale internetdomeinbeleid het liefst alle oplossingen in onderlinge samenhang terugkomen. Dit ideaalplaatje is in dit adviesrapport uitgewerkt in het ideaalscenario, voor inrichting en implementatie van het internetdomeinbeleid. Naast het ideaalscenario zijn drie andere scenario’s uitgewerkt die een oplopende effectiviteit en complexiteit vertonen.

Op die manier worden afspraken centraal verankerd, wordt centraal een basis gelegd voor overheidsbrede dienstverlening, en worden overheidsorganisaties met betrekking tot het beheer van hun internetdomeinportfolio ontzorgd en ondersteund. Deze integrale aanpak zorgt overheidsbreed voor een volwassen inrichting van internetdomeinbeheer dat uiteindelijk resulteert in verbetering van de herkenbaarheid en veiligheid van de digitale overheid op decentraal én centraal niveau.

1.2. Managementsamenvatting

In 2021 is overheidsbrede inzet op het gebied van internetdomeinbeleid geagendeerd. De nota Herkenbare Digitale Overheid benoemt overheidsinzet voor eenduidig internetdomeinbeleid om de grip op internetdomeinen van de overheid te verhogen, en het Kamerstuk Informatieveiligheid agendeert overheidsbreed internetdomeinbeleid en stelt het belang van verankering van afspraken op dit gebied vast.

Dit adviesrapport sluit aan op dit belang. Het Forum Standaardisatie heeft op verzoek van Directie Digitale Samenleving van het Ministerie van Binnenlandse Zaken het onderzoek 'overheidsbreed internetdomeinbeleid' uitgevoerd, onderdeel van het traject 'Herkenbare en veilige digitale overheid', om de verankering van afspraken omtrent internetdomeinbeheer overheidsbreed vorm te geven. Dit adviesrapport, wat eind april 2022 is opgeleverd, geeft antwoord op de vraag 'Hoe ziet overheidsbreed internetdomeinbeleid er idealiter uit?'. Om antwoord te geven op de onderzoeksvraag is aan de hand van twee gespreksfases is inzicht verkregen in de stand van zaken omtrent internetdomeinbeheer binnen de overheid, zijn knelpunten in de beleidsvoering en in de praktijkuitvoering van internetdomeinbeheer geïdentificeerd, zijn behoeften en belangen van overheidsorganisaties onderzocht, en oplossingsrichtingen verkend. Dit heeft geleid tot tien oplossingen voor de geconstateerde knelpunten, waarover in dit rapport is geadviseerd met bijbehorend implementatieadvies. De oplossingen zijn opgenomen in vier scenario's, die de impact van implementatie weergeven en zo een beeld schetsen van hoe overheidsbreed internetdomeinbeleid ingevuld kan worden.

Het adviesrapport fungeert daarmee als basis voor overheidsbreed internetdomeinbeleid. Door het verankeren van kaders en richtlijnen in overheidsbreed internetdomeinbeleid brengen we de beheersbaarheid en kwaliteit van internetdomeinen en achterliggende online middelen binnen de gehele overheid naar een hoger volwassenheidsniveau. Het doel is dan ook om, door het gezamenlijk meer grip te krijgen op overheidsdomeinen, de herkenbaarheid en veiligheid van de overheid te verbeteren.

Dit onderzoek heeft verschillende knelpunten aan het licht gebracht die de relevantie van dit rapport benadrukken. De praktijk toont dan ook aan dat de behoefte aan een meer centrale aansturing op dit gebied groot is. De alsmaar voortdurende voortzetting van wildgroei leidt tot een gebrek aan overzicht en inzicht in overheidsdomeinen, waardoor het aansturen op en voldoen aan kwaliteitseisen steeds moeilijker wordt. Eveneens hebben overheidsorganisaties intern hun internetdomeinportfolio niet onder controle. Een onduidelijke governance-structuur en onvoldoende ingerichte beheerprocessen liggen hieraan ten grondslag. Door het ontbreken van toezicht, monitoring en handhaving worden de huidige afspraken en verplichte richtlijnen onvoldoende nageleefd. De afgelopen jaren hebben zich verschillende voorbeelden voorgedaan die ten gevolge van deze problematiek zijn voorgevallen, zoals fake-news, phishing en domein-spoofing. Kortom, kwetsbare internetdomeinen ondermijnen onze veiligheid. Tegelijkertijd

hebben zowel burgers als overheidsorganisaties, als gevolg van deze ontwikkelingen, steeds meer moeite met het herkennen van overheidswebsites en e-mails. Door gebrek aan herkenbaarheid hebben burgers steeds minder vertrouwen in de digitale overheid. De digitale overheid moet herkenbaar zijn voor burgers en ondernemers.

In het ideale internetdomeinbeleid wordt dan ook het ideaalscenario geadopteerd. Dit houdt in dat iedere oplossing waarover geadviseerd is in dit rapport overheidsbreed wordt geïmplementeerd. Dit zijn oplossingen gericht op zowel interne beheersing van de governance en beheerprocessen omtrent internetdomeinbeheer als het overkoepelend zorgen voor een stabiele basis om overheidsorganisaties te ontzorgen en te ondersteunen. Door centraal aan te sturen en decentraal in te richten pakken we gezamenlijk de huidige problematiek aan op zowel micro- als macro-niveau. Zo verbeteren we de herkenbaarheid en veiligheid van de overheid.

2. Scenario’s

In dit onderdeel zijn vier scenario’s opgesteld, waaronder een 0-scenario, een basisscenario, een ambitieus scenario, en het ideaalscenario. Deze representeren ieder een ander kader voor het inrichten van internetdomeinbeheer. Voor ieder scenario staat beschreven wat er in dat scenario wordt geïmplementeerd, en wat de impact daarvan is op de huidige situatie. Op die manier is een beeld geschetst van welke (maatschappelijke) veranderingen het betreffende scenario teweeg brengt. De oplossingen uit hoofdstuk 3 zijn in deze scenario’s ondergebracht. Deze worden in hoofdstuk 3 nader toegelicht. De scenario’s zijn opbouwend opgesteld, wat betekent dat het oploopt van een 0-scenario, die de huidige situatie beschrijft, tot een ideaalscenario, waarin de meest ideale situatie beschreven is. Uiteraard heeft het ideaalscenario de voorkeur. De mate van verplichting en het tempo van implementatie zijn variabel en daarom is het mogelijk om ieder scenario op de gewenste manier te implementeren.

Bovenal is het van belang te benadrukken dat ongeacht welk scenario wordt doorgevoerd, het internetdomeinbeleid met bijbehorende oplossingen bekrachtigd moet worden door de juiste communicatieuitingen te verzorgen die het beleid ondersteunen, en kennisdeling te stimuleren. Zonder het op de juiste manier uitdragen van het internetdomeinbeleid, is het onmogelijk om optimale effectiviteit te bereiken en de voordelen daarvan te kunnen benutten. Om die reden is eveneens het advies om bij implementatie van het beleid een communicatiestrategie te bepalen om uitwerking van het beleid te ondersteunen. Daarnaast moet er toegewerkt worden naar het centraliseren van kennis, zodat deze evenredig blijft aan de kwaliteit en verwachtingen van het beleid.

Geadviseerd wordt om Directie Digitale Samenleving (BZK) als eigenaar van het internetdomeinbeleid aan te stellen, en kaders en richtlijnen voor internetdomeinbeheer te laten opstellen. Zij kunnen eveneens dit beleid uitdragen.

Zoals benoemd is het 0-scenario een scenario waarin de keuze ligt bij het implementeren van geen enkele voorgestelde oplossing, waardoor de huidige situatie onveranderd blijft.

Vanaf het basisscenario wordt RIO (3.1) in ieder scenario als ingangseis geïmplementeerd, om de reden dat het andere oplossingen faciliteert en ondersteunt in implementatie.

In het basisscenario wordt een set aan minimumeisen geïmplementeerd, die beschouwd worden als basishygiëne voor goed internetdomeinbeheer. Deze set aan basiseisen draagt, door het maken van centrale afspraken, op een individueel organisatieniveau bij aan het verbeteren van de interne *governance* en beheerprocessen. Deze aanpak vereist centrale aansturing, en decentrale inrichting. Over het algemeen zijn dit eisen die relatief makkelijk implementeerbaar zijn, en pakken zo onderliggende problematiek op het gebied van internetdomeinbeheer op micro-niveau aan. Een goede uitvoering van internetdomeinbeheer verhoogt het

kwaliteitsniveau van de internetdomeinen, webtoepassingen en andere online middelen.

In het ambitieuze scenario zijn deze basiseisen aangevuld. De aanvullingen op de basiseisen die vanaf het ambitieuze scenario naar voren komen zijn oplossingen die centraal worden aangestuurd en overkoepelend werken. Dit zijn de oplossingen die het meest effectief de geconstateerde problemen op macro-niveau aanpakken en de meeste maatschappelijke impact hebben. Deze worden vanaf het basisscenario in ieder opeenvolgend scenario opgenomen.

De oplossingen die in het ideaalscenario aanvullend daarop zijn toegevoegd zijn oplossingen die ter ondersteuning werken van de rest van de oplossingen en kennisdeling stimuleren. In het ideaalscenario wordt iedere oplossing ter implementatie doorgevoerd. Uiteraard ligt de voorkeur bij het implementeren van het ideaalscenario.

In de onderstaande uitwerking van de scenario's is beschreven hoe het scenario eruitziet bij implementatie van de genoemde oplossingen. Dit is een globale beschrijving waarbij voor inhoudelijke toelichting gerefereerd wordt naar hoofdstuk 3. Met andere woorden, wat de oplossingen inhoudelijk betekenen, wat de voor -en nadelen van implementatie zijn, en wat het implementatieadvies per oplossing inhoudt, is onder hoofdstuk 3 uitgelijnd.

2.1. 0-Scenario

In het 0-scenario blijft de huidige situatie onveranderd, zonder dat er oplossingen geïmplementeerd worden om internetdomeinbeheer binnen de overheid te verbeteren.

Voordelen

Er hoeft geen extra capaciteit vrijgemaakt te worden om internetdomeinbeheer in te richten. Daarnaast zal het kosten die nodig zijn om bepaalde opties in te richten besparen. Allerlaatst geeft het overheidsorganisaties de vrijheid om zelf internetdomeinbeheer in te richten.

Nadelen

De huidige situatie blijft onveranderd. Dit betekent dat internetdomeinen niet overzichtelijk in kaart zijn gebracht, waardoor overheidsorganisaties onvoldoende grip blijven houden op hun internetdomeinportfolio. Hierdoor is er onvoldoende inzicht in de kwaliteit van internetdomeinen en achterliggende online middelen. Als gevolg daarvan is gerichte aansturing op kwaliteitseisen -en aspecten onmogelijk.

Zonder kaders, richtlijnen en randvoorwaarden blijft wildgroei een doorn in het oog. Dit leidt zowel op korte als op lange termijn tot steeds minder overzicht en inzicht in internetdomeinen, wat risicovolle situaties met zich meebrengt. Overheidsorganisaties verliezen steeds meer internetdomeinen uit het oog die niet (meer) geüpdatet worden aan de hand van kwaliteitseisen. Dit leidt tot kwetsbaarheden. Zonder duidelijke afspraken over het levenscyclusbeheer van internetdomeinen en centralisatie van dienstverlening, blijft versnippering van registraties een groot knelpunt en worden er

blijvend te veel internetdomeinen geregistreerd. Dat zorgt er eveneens voor dat wildgroei prominent aanwezig blijft.

Daarnaast worden internetdomeinen zonder het stellen van kaders, richtlijnen, en randvoorwaarden niet op tijd uitgefaseerd, waardoor deze onnodig online blijven staan en tot mogelijke veiligheidsrisico's leiden. En dan niet te vergeten dat het vrijgeven van internetdomeinen waar e-mail op gedraaid heeft e-mailspoofing mogelijk maakt. Ook worden internetdomeinen die te vroeg worden vrijgegeven overgenomen door een externe partij, terwijl de associatie met de overheid nog bij de burger aanwezig is. Zo zijn er tal van risicovolle situaties die blijven voortbestaan zonder voldoende aansturing van internetdomeinbeheer.

Naast gebrekkige sturing op internetdomeinbeheer van de overheid als geheel, blijft gebrek aan *governance* in overheidsorganisaties een groot knelpunt. Internetdomeinbeheer binnen overheidsorganisaties blijft versnipperd, waardoor verantwoordelijkheden niet duidelijk belegd zijn. Dit zorgt voor grote blinde vlekken binnen de organisatorische context. Hierdoor is aansturing van internetdomeinbeheer onmogelijk.

Deze versnippering vindt niet alleen intern plaats, maar ook bij uitbesteding van diensten aan externe leveranciers. Overheidsorganisaties besteden (te) veel diensten die betrekking hebben op internetdomeinbeheer uit aan verschillende externe leveranciers. Hierdoor blijft de overheid afhankelijkheid van externe leveranciers in de hand werken. Wanneer externe leveranciers daarnaast niet op de hoogte zijn van – of niet werken volgens – kaders en vereisten die voor overheden gelden, zullen de diensten die zij aan overheden leveren niet voldoen aan de kwaliteit die de burger mag verwachten. Kortom, onvoldoende sturing op het aangaan van contracten met externe leveranciers zorgt ervoor dat de gestelde kwaliteitseisen niet altijd ondersteund worden.

Het ontbreken van toezicht, monitoring en handhaving zorgt ervoor dat naleving van de gemaakte afspraken niet gecontroleerd kan worden. Hierdoor is aansturing en handhaving op naleving moeilijk en is het lastig om effectiviteit van het beleid te bepalen.

Omdat internetdomeinbeheer niet overheidsbreed is aangestuurd blijven er grote verschillen in internetdomeinbeheer tussen centrale overheidsorganisaties en decentrale overheidsorganisaties. Overheidsorganisaties zijn zelf verantwoordelijk voor het inrichten van interne beheerprocessen, waardoor de inrichting hiervan uiteenloopt. Daarnaast is er onvoldoende centrale aansturing vanuit de Rijksoverheid in de vorm van kaders en richtlijnen om de praktische uitvoering van internetdomeinbeheer beter in te richten. Dit zorgt ervoor dat er geen eenduidige overheid ontstaat, maar tot steeds meer divergentie tussen overheden leidt. Daarnaast ondervinden alle overheidsorganisaties de nadelen ervan wanneer het niet op orde is. Wanneer de burger de overheid niet herkent en niet als betrouwbaar acht, heeft dit impact op de gehele overheid.

Daarnaast blijft de overheid onherkenbaar voor de burger. Burgers kunnen moeilijk onderscheid maken tussen overheidswebsites en niet-overheidswebsites, omdat er

geen goede, niet kopieerbare, herkenningspunten zijn. Zonder grip te krijgen op overheidsdomeinen, verergert dit probleem. De burger ondervindt daar de problemen van. Dit ondermijnt het vertrouwen van de burger in de overheid[1]. De wildgroei aan internetdomeinen zorgt er ook voor dat relevante informatie van de overheid steeds moeilijker vindbaar wordt, of informatie op verschillende legitieme bronnen elkaar zelfs tegenspreekt.

Concluderend is er in dit scenario een gebrek aan beheersing, waardoor er risico's zijn voor de herkenbaarheid, vindbaarheid, betrouwbaarheid en veiligheid van de overheid.

2.2. Basisscenario

In het basisscenario wordt, naast implementatie van RIO (3.1), een set aan minimumeisen geïmplementeerd die overheidsorganisaties decentraal inrichten. Deze basiseisen ondersteunen inrichting van internetdomeinbeheer intern binnen organisaties.

Dit gaat om het maken van afspraken omtrent levenscyclusbeheer (3.4), het vastleggen van verantwoordelijkheden en rolverdeling (3.5), het stellen van eisen aan externe leveranciers (3.6), en het intern verplichten van periodieke kwaliteitscontroles (3.7). Deze oplossingen hebben betrekking op zowel de interne *governance* en procesinrichting van internetdomeinbeheer (3.4, 3.5) als op de achterliggende kwaliteit van internetdomeinen (3.6, 3.7).

Voordelen

Deze aanpak zorgt ervoor dat de geconstateerde problematiek omtrent internetdomeinbeheer intern vanuit overheidsorganisaties zelf bestreden wordt. Dit is een aanpak die duurzaam is op lange termijn, omdat overheidsorganisaties door goede procesinrichting en *governance* internetdomeinbeheer beter op orde kunnen houden. Tevens zorgt het inrichten van eenduidig internetdomeinbeheer voor een eenduidige overheid. Naast een verbeterde interne beheersing van processen (3.4) en inrichting van een werkende *governance*-structuur (3.5) binnen overheidsorganisaties, wordt ook de kwaliteit van overheidsdomeinen actief aangestuurd (3.6, 3.7), wat zorgt voor een verhoogde veiligheid.

Naast het inrichten van RIO, kosten de aanvullende oplossingen weinig extra capaciteit en middelen, omdat deze meer gericht zijn op aansturing van de mensen en middelen die al aanwezig zijn binnen overheidsorganisaties. Implementatie van deze oplossingen is relatief makkelijk realiseerbaar en kan snel worden ingezet. Wat dat betreft zijn het oplossingen waarbij op korte termijn effectiviteit zichtbaar is en bijsturing mogelijk is. Het tempo van implementatie en de mate van verplichting zijn variabel en kunnen naar wensen worden ingericht. Daarnaast zijn het duurzame oplossingen omdat deze aanpasbaar zijn aan actualiteiten die zich voordoen. Op die manier is het

[1] 'Herkenbaarheid van en vertrouwen in websites en e-mails van de overheid', Kantar (2019).

internetdomeinbeleid adaptief en kan gedurende de komende jaren makkelijk worden bijgesteld.

Nadelen

Ondanks dat het beter inrichten van internetdomeinbeheer binnen overheidsorganisaties vele voordelen met zich meebrengt, is er bij invoering van deze oplossingen geen sprake van extern toezicht, monitoring en handhaving op de gemaakte afspraken. Centraal toezicht is van belang om de naleving te monitoren en bij gebrek aan naleving te kunnen handhaven. Omdat dat in dit scenario niet centraal is ingeregeld, is het lastig hier actief op te controleren. Door kwaliteitscontroles enkel op decentraal niveau door overheidsorganisaties in te laten regelen, ligt de verantwoordelijkheid voor toezicht, monitoring en handhaving bij organisaties zelf. Hierdoor kan effectiviteit afnemen omdat naleving afhankelijk is van interne aansturing en zonder centrale aansturing consequenties ontbreken bij het niet voldoende naleven van afspraken in het internetdomeinbeleid.

Al met al wordt er in dit scenario enkel aangestuurd op decentrale inrichting van internetdomeinbeheer, waardoor geconstateerde knelpunten niet op macro-niveau worden aangepakt. Het aansturen van kwaliteitsaspecten als herkenbaarheid, vindbaarheid, veiligheid en beheersbaarheid vereisen naast een decentrale aanpak ook een centraal aangestuurde aanpak om onderliggende oorzaken overkoepelend aan te pakken.

2.3. Ambitieus scenario

In het ambitieuze scenario wordt er geadviseerd om aanvullend op de decentrale basiseisen een aantal diensten en voorzieningen te implementeren op centraal niveau. Dit gaat om de herkenbare overheidsextensie (3.2), de centrale overheidsregistrar (3.3), en vormgeving van toezicht, monitoring en handhaving (3.8). Deze diensten en voorzieningen zijn centraal aangestuurd en pakken overkoepelend problemen aan die voortkomen uit gebrekkig internetdomeinbeheer. De implementatie van deze diensten en voorzieningen vragen relatief meer tijd, kosten en capaciteit en worden daarom als ambitieus beschouwd.

Voordelen

Waar het basisscenario alleen inspeelt op de microproblematiek, pakt het ambitieuze scenario ook de achterliggende oorzaken op macro-niveau aan. Dit gebeurt door niet alleen op decentraal niveau aan te sturen op interne beheersing van internetdomeinbeheer en de daaraan grenzende governance-structuur, maar ook te zorgen voor een centrale aanpak.

Implementatie van een herkenbare overheidsextensie (3.2) en een centrale overheidsregistrar (3.3) vormen na RIO (3.1) een logische implementatievolgorde, en ondersteunen elkaar, wat voor optimale effectiviteit zorgt. Zo faciliteren zowel RIO als de centrale overheidsregistrar de transitie naar een herkenbare overheidsextensie. Dit is onder hoofdstuk 3 verder toegelicht. Het betreft oplossingen van een lange adem,

maar levert blijvende voordelen op. Onder andere pakt het invoeren van een herkenbare overheidsextensie op centraal niveau het herkenbaarheidsprobleem aan, en gaat een centrale overheidsregistrar versnippering van registraties tegen. De combinatie van deze richtingen zorgt voor een eenduidige inrichting van internetdomeinbeheer voor de gehele overheid, en daarmee het zijn van één digitale overheid. Het implementeren van deze oplossingen leidt overkoepelend tot een verbeterde beheersbaarheid, vindbaarheid en herkenbaarheid, én veiligheid van de overheid.

Daarnaast is het centraal inrichten van toezicht, monitoring en handhaving (3.8) op de gemaakte afspraken in internetdomeinbeleid cruciaal voor het stimuleren van naleving op decentraal niveau en draagt het bij aan een verhoogde effectiviteit van de geïmplementeerde oplossingen door processen te monitoren en bij te sturen.

De hierboven benoemde oplossingen dragen bij aan een duurzame en effectieve lange termijn aanpak voor goed internetdomeinbeheer en bieden de mogelijkheid om dit op centraal niveau te blijven aansturen. Kijkend vanuit een lange termijn perspectief biedt deze centrale aanpak meer zekerheid op het gebied van kwaliteitsaspecten als herkenbaarheid en beheersbaarheid, doordat de aanpak zowel op centraal als decentraal niveau ontzorgt en ondersteunt.

Nadelen

De bovenstaande aanpak zal op organisatorisch niveau grote veranderingen teweeg brengen. Allereerst is het een uitdaging om toezicht, monitoring en handhaving overheidsbreed in te richten. Ondanks dat de verantwoordelijkheid hiervoor belegd kan worden bij een bestaande overheidspartij, kost het inrichten van toezicht, monitoring en handhaving overheidsbreed tijd en capaciteit om in te richten op grote schaal. Echter zonder dat dit voldoende is ingericht is het moeilijk om overheidsorganisaties te controleren op de toepassing van afspraken op het internetdomeinbeheer binnen de organisatie. Ook het inrichten van een centrale overheidsregistrar kan belegd worden bij een bestaande overheidspartij, maar kost eveneens extra capaciteit door bestaande taken op overheidsbrede schaal in te richten. Daarnaast brengt het inrichten van dit pakket ook door implementatie van de generieke overheidsextensie de nodige tijd en kosten met zich mee. Al met al zijn het oplossingen waarin geïnvesteerd moet worden op lange termijn. Het zorgt met name op lange termijn voor veel effectiviteit, waardoor korte termijn effecten moeilijk zichtbaar zijn. Het beschikbaar stellen van voldoende capaciteit en middelen is cruciaal om volledige effectiviteit te benutten.

2.4. Ideaalscenario

In het ideaalscenario worden alle voorgaande oplossingen geïmplementeerd, met aanvullend twee oplossingen. Deze oplossingen zijn het inrichten van een interbestuurlijke werkgroep internetdomeinbeheer waarbij iedere overheidslaag is gerepresenteerd (3.9) en het intern inrichten van een interdisciplinair expertiseteam bij overheidsorganisaties (3.10). Beiden hebben betrekking op de stimulering van naleving en van kennisdeling op het gebied van internetdomeinbeheer.

Voordelen

Naast het implementeren van de basiseisen en aanvullende eisen op het gebied van *governance*, kwaliteit, procesinrichting en toezicht, is het van belang dat kennis en praktijkervaring wordt gedeeld en naleving van de gemaakte afspraken wordt gestimuleerd. Deze oplossingen dragen daaraan bij. Ook zorgt het ervoor dat het gat tussen de werkvloer en het bestuurlijke niveau wordt verkleind, doordat een overheidsbrede werkgroep praktijkervaring kan uitwisselen en hierover signalen kan afgeven op bestuursniveau. Het zorgt ervoor dat praktijkprocessen actief kunnen worden bijgestuurd aan de hand van behoeften en belangen van deelnemende organisaties. Tevens is het van belang dat er kennisdeling plaatsvindt, om houdbaarheid, optimalisatie en innovatie te stimuleren, en overheidsorganisaties bewust te houden van actualiteiten omtrent internetdomeinbeheer. Dit stimuleert adaptatie, actualisatie en groei op het gebied van internetdomeinbeheer, zonder het risico te lopen dat het beleid snel verouderd. Hiervoor is het belangrijk dat de overheid actief inspeelt op veranderingen, en daarvoor is interdisciplinaire samenwerking in combinatie met input vanuit verschillende overheidslagen en niveaus cruciaal.

Allerlaatst maken deze oplossingen het mogelijk om aanvullende afspraken te maken omtrent het inrichten van de basiseisen. Zo worden ook de basiseisen en de kaders eromheen beter verankerd in het internetdomeinbeleid. Al met al zorgt de combinatie van deze oplossingen voor een optimalisatie in beheersbaarheid, vindbaarheid, herkenbaarheid en veiligheid binnen de overheid.

Nadelen

De effectiviteit van de oplossingen is afhankelijk van de wil en motivatie van overheidsorganisaties om bij te dragen aan gezamenlijke processen en samenwerking op dit gebied.

2.5. Vergelijkingstabel scenario's

SCENARIO	AARD	TERMIJN	TEMPO	VERPLICHTING
0-SCENARIO	**N.v.t.**	**N.v.t.**	**N.v.t.**	**N.v.t.**
BASIS	**Decentraal**	**Korte termijn**	**Variabel**	**Variabel**
AMBITIEUS	**Decentraal en centraal**	**Lange termijn**	**Variabel**	**Variabel**
IDEAAL	**Decentraal en centraal**	**Lange termijn**	**Variabel**	**Variabel**

SCENARIO	IMPACT*	EFFECTIVITEIT*	MOEILIJKHEIDSGRAAD	KOSTEN	CAPACITEIT
0-SCENARIO	**0**	**0**	**0**	**0**	**0**
BASIS	**+**	**+**	**-**	**-**	**-**
AMBITIEUS	**++**	**++**	**+**	**+**	**+**
IDEAAL	**+++**	**+++**	**+**	**+**	**+**

***Het is mogelijk om criteria op te nemen om impact en effectiviteit meetbaar te maken na implementatie.**
****** Impact draait om maatschappelijke impact, effectiviteit draait om effectiviteit van implementatie voor de interne organisatie.**

3. Oplossingen en implementatieadvies

3.1. Register Internetdomeinen Overheid (RIO)

Algemeen

Op dit moment ontbreekt een overheidsbreed overzicht van internetdomeinen. Het Register Internetdomeinen Overheid (RIO) is een centraal, openbaar register dat overzicht biedt van overheidsdomeinen. RIO is gekoppeld aan de staatsalmanak (Register Overheidsorganisaties, ROO). Het register biedt de mogelijkheid voor burgers om te valideren of een website van de overheid is. Dit draagt bij aan de herkenbaarheid van de overheid en het vertrouwen van de burger in de overheid. Ook biedt het voor overheidsorganisaties zelf een overzicht van bestaande overheidsdomeinen, en voor welke hun eigen of andere overheidsorganisaties verantwoordelijk zijn.

Voordelen

Het grootste voordeel van een centraal overheidsregister is dat het de algehele herkenbaarheid van de overheid verbetert. Doordat overheidswebsites te valideren zijn heeft de burger minder moeite met onderscheid maken tussen wat een overheidswebsite is en wat niet. Dit vergroot het vertrouwen van de burger in de overheid, en helpt fraude voorkomen door bijvoorbeeld phishing of verspreiding van nepnieuws. Daarnaast helpt het overheidsorganisaties om grip te krijgen op hun portfolio van internetdomeinen doordat het overzicht en inzicht biedt.

Nadelen

Het nadeel kan zijn dat burgers niet de moeite nemen om een website op echtheid te controleren, waardoor zij nog steeds de problemen ondervinden van een onherkenbare overheid. Ook is een nadeel dat overheidsorganisaties zelf verantwoordelijk zijn om hun domeinnamen te registreren in het register, en dit actief bij te houden. Wanneer organisaties dit niet actief bijwerken wanneer er veranderingen plaatsvinden, behoudt het register niet haar actualiteit. Een niet actueel register gaat ten koste van de herkenbaarheid van de overheid, waar de burger de problemen van ondervindt.

Implementatieadvies

Het advies is om RIO als basis te implementeren ter ondersteuning van andere oplossingen. Hoe RIO de andere oplossingen ondersteunt is te vinden onder 3.1.5.

Een aansluitend advies is om criteria op te stellen om te bepalen wat onder een overheidsdomein valt. Dit kan (gedeeltelijk) aan de hand van het Register Overheidsorganisaties (ROO) geïdentificeerd worden. Zo kan er onderscheid gemaakt worden op basis van classificaties wat er in RIO wordt opgenomen, en kan bepaald worden of bijvoorbeeld een campagnewebsite als overheidsdomein telt, en of internetdomeinen van publiek-private samenwerkingen in RIO horen.

Tevens wordt geadviseerd om overheidsorganisaties te verplichten om veranderingen rondom internetdomeinen door te voeren in RIO. Overheidsorganisaties zijn dan verplicht om alle internetdomeinen waar zij verantwoordelijk voor zijn op te nemen in

RIO, en houden wijzigingen actief bij. Dit voorkomt dat het register niet actuele informatie bevat en het ten koste gaat van de herkenbaarheid van de overheid.

Daarnaast is het advies om in RIO op te nemen wie verantwoordelijkheid draagt voor een overheidsdomein, door bijvoorbeeld de rol van (website)eigenaar en van (portfolio)beheerder te verwerken bij een internetdomein. Hierdoor is het overzichtelijk waar verantwoordelijkheden voor een internetdomein belegd zijn, en wie het aanspreekpunt is. Dit bevordert overheidscommunicatie op het gebied van internetdomeinbeheer. Informatie over het invullen van de verantwoordelijkheden en rollen die hieraan gekoppeld kunnen worden is te vinden onder 3.5. Uiteraard is het van belang om bij het verwerken van persoonsgegevens rekening te houden met de AVG. Het advies is dan ook om deze gegevens af te schermen voor derden. Alleen contactpersonen van de overheid kunnen dan deze gegevens inzien. Wel is het mogelijk om, in plaats van het openbaar maken van directe contactpersonen, voor burgers een centrale mailbox als aanspreekpunt te verwerken in het register, die wel publiekelijk zichtbaar is.

Het advies is om deze afspraken op te nemen in het internetdomeinbeleid.

Combineren met andere oplossingen

3.2, Herkenbare overheidsextensie: RIO brengt overheidsdomeinen in kaart en biedt daarom een goede basis voor internetdomeinbeheer. Zo ondersteunt het de stap naar een herkenbare overheidsextensie. Door te classificeren wat overheidsdomeinen zijn, kan men vanuit RIO identificeren welke domeinnamen een herkenbare overheidsextensie krijgen. Zo vergemakkelijkt het de transitie naar deze extensie, omdat overheidswebsites al geïnventariseerd zijn. Anderzijds is het ook makkelijker om websites met een herkenbare overheidsextensie te traceren en in het RIO op te nemen. Echter is RIO niet meer een noodzakelijke oplossing om als validatieregister gebruiken wanneer álle overheidsdomeinen een herkenbare overheidsextensie hebben, omdat deze al herkenbaar zijn. Wel is het erg relevant om in RIO redirects met een overheidsextensie te verwerken, wanneer er een transitieperiode plaatsvindt voor de overgang naar de herkenbare overheidsextensie. Daarom is het advies om RIO als eerste stap te implementeren, zodat dit de transitie naar een herkenbare overheidsextensie kan ondersteunen.

3.3, Centrale overheidsregistrar: Door RIO te combineren met het aanstellen van een centrale overheidsregistrar, biedt het de mogelijkheid om betere controle te voeren op de actualiteit van het register. Een centrale overheidsregistrar kan bij registratie van een nieuw overheidsdomein deze registratie doorvoeren in het register, waardoor RIO gekoppeld blijft aan actualiteiten die zich bij de registrar voordoen. Andersom kan de registrar ook informatie ophalen uit het RIO, wanneer organisaties hierin wijzigingen doorvoeren.

3.4, Centrale afspraken omtrent levenscyclusbeheer: Doordat overheidsdomeinen overzichtelijk in kaart zijn gebracht, vermindert het de beheerlast van overheidsorganisaties in het beheren van internetdomeinen. Daardoor draagt het indirect bij aan levenscyclusbeheer. Door bijvoorbeeld het bestaan van verouderde of

overbodige internetdomeinen beter in beeld te brengen, kunnen organisaties deze tijdig uitfaseren.

3.7, Verplichte periodieke kwaliteitscontroles: Het overzicht van RIO kan gebruikt worden voor het uitvoeren van verplichte periodieke kwaliteitscontroles op open standaarden en andere verplichte richtlijnen. RIO maakt het overzichtelijk welke internetdomeinen er getoetst moeten worden.

3.8, Vormgeven van toezicht, monitoring en handhaving: Het overzicht van RIO kan gebruikt worden voor het houden van toezicht, monitoring en handhaving. Doordat door RIO al geclassificeerd is wat onder overheidsdomeinen vallen, is al geïdentificeerd welke internetdomeinen aan de gestelde eisen moeten voldoen. Dit maakt toezicht, monitoring en handhaving overzichtelijker.

3.2. Herkenbare overheidsextensie

Algemeen

Een herkenbare overheidsextensie is een eenduidige extensie die als 2nd level domain (.gov.nl/.overheid.nl) wordt toegepast op overheidsdomeinen. In onderstaande voorbeelden wordt .gov.nl als uitgangspunt genomen.

Voordelen

Het doorvoeren van een herkenbare overheidsextensie voor overheidsdomeinen bevordert de algehele herkenbaarheid en betrouwbaarheid van de overheid. Het maakt onderscheid tussen overheidsdomeinen en niet-overheidsdomeinen. Doordat alleen overheidsdomeinen de extensie krijgen, is het voor burgers direct duidelijk dat het om een overheidswebsite gaat, waardoor de burger de website niet meer hoeft te valideren en de overheid beter vindbaar is. Ook wordt de burger minder makkelijk misleid, doordat het phishing en oplichting tegengaat. Daarnaast centraliseert het aspecten van internetdomeinbeheer, wat de dienstverlening en beveiliging ervan vergemakkelijkt. Het rapport 'technische impactanalyse eenduidige domeinnaam'[2] biedt hierover meer informatie.

Nadelen

Bestaande domeinen moeten gewijzigd worden, wat voor grotere domeinen een (tijdelijke) beheerlast met zich meebrengt. Ook moeten communicatiemiddelen aangepast worden als het domein met de extensie het nieuwe hoofddomein wordt. Daarnaast is de dienst afhankelijk van de beschikbaarheid van DNS, omdat overheidswebsites anders niet bereikbaar zijn. Wanneer de DNS-dienst die de extensie ondersteunt offline gaat, betekent dat dat de overheidscommunicatie niet beschikbaar is. Ook brengt deze wijziging de nodige kosten met zich mee. Het rapport van de technische impactanalyse[2] gaat hier verder op in.

[2] Rapport technische impactanalyse eenduidige domeinnaam, ICTU. Definitieve versie. (2022).

Implementatieadvies

Het advies is om de herkenbare overheidsextensie door middel van een transitieperiode te implementeren. Voor grote overheidsdomeinen zal het een zwaardere beheerlast met zich meebrengen dan voor kleinere overheidsdomeinen. Daardoor verschilt de behoefte aan overgangstijd per organisatie. Door voor ieder overheidsdomein uit RIO een redirect met .gov.nl te registreren, creëert het ruimte om op eigen tempo over te gaan van het hoofddomein naar het domein met de extensie. RIO faciliteert de transitieperiode door redirects met een overheidsextensie op te nemen in het register. Dit geeft overheidsorganisaties de tijd om de overgang te maken. Zodra de domeinen volledig overgezet zijn naar het domein met de .gov.nl extensie, wordt dat domein de default. Het oude hoofddomein wordt uitgefaseerd en uit RIO gehaald, en het .gov.nl-domein het hoofddomein. Zo blijft het tijdens een transitieperiode in RIO overzichtelijk welke domeinen nog geen overheidsextensie hebben (bijv. alleen Rijksoverheid.nl in RIO), welke via een redirect in de transitieperiode zitten (bijv. Rijksoverheid.nl én Rijksoverheid.gov.nl in RIO), en welke volledig over zijn (bijv. enkel Rijksoverheid.gov.nl in RIO). Hierdoor blijft het in de transitieperiode ook voor burgers duidelijk welke domeinen van de overheid zijn, ook wanneer zij nog niet beschikken over een herkenbare extensie.

Om herkenbaarheid van de hele overheid te verbeteren, is het advies om gedurende een aantal jaar een verleidingsstrategie in te zetten en dan over te gaan tot verplichting. De keuze om eerst te verleiden zal minder weerstand oproepen, waardoor meer overheidsorganisaties zelf de keuze zullen maken om over te gaan. Uit het Buitenlandonderzoek Domeinnaambeleid blijkt dat veel landen kiezen voor een verleidingsstrategie[3]. Echter zal verplichting wel een optie moeten blijven wanneer dit niet voldoende blijkt te zijn. In het Buitenlandonderzoek Domeinnaambeleid[3] blijkt uit een praktijkvoorbeeld van Nieuw Zeeland dat bij de keuze om de extensie niet te verplichten maar op basis van vrijblijvendheid overheidsorganisaties de extensie te laten adopteren, niet iedere overheidsorganisatie meegaat. Hierdoor blijken burgers nog steeds de problemen van een onherkenbare overheid te ondervinden. Het verplichten zal uiteindelijk de herkenbaarheid van de overheid ten goede komen, omdat er uiteindelijk geen onderscheid meer zit in overheidsdomeinen. Er zijn echter voldoende middelen nodig om dit af dwingen. Door middel van de transitieperiode wordt het traject over een aantal jaar uitgesmeerd, wat de haalbaarheid vergroot en minder druk legt op organisaties om op korte termijn over te moeten. De Vlaamse overheid heeft voor deze transitie vier jaar uitgetrokken[3]. De Rijksoverheid kan gedurende deze periode de overgang faciliteren en bijdragen aan het ontzorgen en ondersteunen van organisaties. In de transitieperiode kan dus gebruik gemaakt worden van een verleidingsstrategie. Politiek-bestuurlijk draagvlak is echter cruciaal om tot verplichting over te gaan. Uiteraard is dit afhankelijk van het tempo en de mate van verplichting waarvoor gekozen wordt in een transitieperiode, deze zijn variabel.

Combineren met andere oplossingsrichtingen

3.2, Register Internetdomeinnamen Overheid (RIO): RIO biedt een goede basis om te classificeren wat overheidsdomeinen zijn. Zo kan men vanuit RIO identificeren welke

[3] Buitenlandonderzoek Domeinnaambeleid, PBLQ. (2019).

websites een herkenbare overheidsextensie krijgen. Andersom is het ook makkelijker om websites met een herkenbare overheidsextensie te traceren en in het RIO op te nemen. Echter is RIO niet meer een noodzakelijke oplossing om als validatieregister gebruiken wanneer overheidsdomeinen een herkenbare overheidsextensie krijgen. Wel is het RIO erg relevant om redirects met een overheidsextensie in te verwerken, wanneer er een transitieperiode plaatsvindt voor de overgang naar de herkenbare overheidsextensie.

3.3, Centrale overheidsregistrar: Doordat de herkenbare overheidsextensie afhankelijk is van een beschikbare DNS, kan het DNS-beheer van websites met een herkenbare overheidsextensie (deels) ondergebracht worden bij de centrale overheidsregistrar. Een herkenbare overheidsextensie impliceert dat het aantal registrars dat deze extensie mag uitgeven beperkt wordt. Hiermee verminder je externe afhankelijkheid omdat een registrar moet voldoen aan strikte voorwaarden, om te voorkomen dat de extensie misbruikt wordt. Een centrale overheidsregistrar kan deze voorwaarden ondersteunen.

3.4, Afspraken omtrent levenscyclusbeheer: Een herkenbare overheidsextensie faciliteert levenscyclusbeheer, waardoor het afspraken omtrent dit beheer kan ondersteunen. Bij het implementeren van een herkenbare overheidsextensie is het mogelijk om afspraken vast te leggen onder afspraken omtrent levenscyclusbeheer. Bijvoorbeeld wanneer een nieuw domein geregistreerd wordt onder de herkenbare overheidsextensie (en wanneer niet), of over het vrijgeven van een domein dat onder de herkenbare overheidsextensie valt. Op deze manier kunnen er afspraken over de levenscyclus van een overheidsdomein gemaakt worden wanneer deze geregistreerd worden onder de herkenbare overheidsextensie. Het dient dan al vanaf het registratieproces als een stok achter de deur, waardoor het wildgroei beperkt.

3.3. Centrale overheidsregistrar

Algemeen

Een centrale overheidsregistrar vervult de functie van registrar overheidsbreed. Het kan gezien worden als een uitbreiding van de rol die DPC nu heeft voor de Rijksoverheid. Een registrar is verantwoordelijk voor de registraties van overheidsdomeinnamen, bewaakt overzicht van geregistreerde internetdomeinen en adviseert over levenscyclusbeheer en toepassing van open standaarden en verplichte richtlijnen.

Voordelen

Het centraliseren van domeinnaamregistraties zorgt voor meer overzicht van en inzicht in overheidsdomeinen. Doordat registraties op één plek gebeuren, voorkomt het versnippering van registraties en daarmee het uit het oog verliezen van domeinnamen. Dat is cruciaal om wildgroei tegen te gaan. Daarnaast komt er door het centraliseren van deze dienstverlening ook meer duidelijkheid over het eigenaarschap van een domein. Periodieke controle op de actualiteit van de gegevens (is een domein nog actief en is het nog bij de juiste eigenaar belegd) is dan makkelijker en houdt het overzicht actueel. Ook verkleint het centraliseren de afstand tussen decentrale overheden en de Rijksoverheid in internetdomeinbeheer, en draagt het bij aan het toewerken naar eenduidig internetdomeinbeheer. Door decentrale overheden dezelfde

diensten te bieden als die DPC aan de Rijksoverheid verleent, ontzorgen en ontlasten we decentrale overheden.

Nadelen

Een nadeel is dat er capaciteit en middelen beschikbaar gesteld moet worden om dit overheidsbreed in te richten. Afhankelijk van waar capaciteit beschikbaar gemaakt kan worden, kan er gekozen worden voor het beleggen bij een bestaand organisatieonderdeel, of kan er een nieuw organisatieonderdeel in het leven geroepen worden die deze dienstverlening op zich neemt. Beide gevallen vereisen capaciteit.

Implementatieadvies

Het advies is om de rol van centrale overheidsregistrar te beleggen bij een centrale overheidspartij die hier capaciteit voor beschikbaar stelt. Dit zou bijvoorbeeld bij DPC belegd kunnen worden. Het is ook de dienstverlening elders te beleggen, bijvoorbeeld bij een partij als Logius. De centrale overheidsregistrar is een uitbreiding van de rol van DPC. Het advies is om het takenpakket van de centrale overheidsregistrar uit te breiden, zodat deze niet alleen verantwoordelijk meer is voor het registratieproces, het bewaken van overzicht van geregistreerde internetdomeinen en het adviseren over procesgerichte zaken en kwaliteit van internetdomeinen, maar ook een meer toezichthoudende, monitorende, en handhavende rol op zich neemt. Door de centrale overheidsregistrar het mandaat te geven om controles uit te voeren en hierop te handhaven, kan de centrale overheidsregistrar centraal internetdomeinbeheer en de kwaliteit ervan beter aansturen. Geadviseerd wordt om de centrale overheidsregistrar het internetdomeinbeleid te laten uitdragen. Aansluitend kunnen ze controleren op naleving van het beleid. Op die manier wordt bij één partij centraal het internetdomeinbeleid aangestuurd.

Tevens is het advies om alleen de centrale overheidsregistrar de herkenbare extensie te laten uitgeven. Hiermee verminder je externe afhankelijkheid omdat een registrar moet voldoen aan strikte voorwaarden om te voorkomen dat de extensie misbruikt wordt. Een centrale overheidsregistrar kan deze voorwaarden overheidsbreed ondersteunen. Ook voorkomt het dat overheidsorganisaties buiten de centrale overheidsregistrar om registreren, omdat het op één plek gecentraliseerd is. Dat voorkomt versnippering van registraties, en zorgt voor meer overzicht en inzicht in overheidsdomeinen, wat wildgroei beperkt. Ook kan het DNS-beheer van de herkenbare overheidsextensie ondergebracht worden bij de centrale overheidsregistrar. Voor een herkenbare overheidsextensie is een goed functionerende DNS cruciaal. Een centrale overheidsregistrar kan overheidsbreed DNS-beheer onderbrengen, waardoor er minder externe afhankelijkheid ligt bij externe leveranciers. Dit kan op een verleidende manier gestimuleerd worden.

Combineren met andere oplossingen

3.1, Register Internetdomeinnamen Overheid: Een centrale overheidsregistrar kan goed gecombineerd worden met RIO. RIO is een overheidsbreed register, en door een centrale overheidsregistrar aan te stellen die overheidsbreed registraties op zich neemt, kan de centrale overheidsregistrar de registratiedata en wijzigingen doorvoeren in RIO. Ook kan de centrale overheidsregistrar input vergaren vanuit RIO, wanneer er

wijzigingen direct zijn doorgevoerd vanuit de organisatie in RIO, die nog niet bekend zijn bij de centrale overheidsregistrar. Het dient als een wederzijdse relatie waar voordeel uit gehaald kan worden betreffende het bewaken van overzicht en inzicht in internetdomeinen, overheidsbreed.

3.2, Herkenbare overheidsextensie: Voor een herkenbare overheidsextensie is een goed functionerende DNS cruciaal. Een centrale overheidsregistrar kan overheidsbreed DNS-beheer faciliteren, waardoor overheidsorganisaties voor wat betreft DNS ontzorgd worden en er minder afhankelijk is van externe leveranciers.

3.4, levenscyclusbeheer: Een centrale overheidsregistrar adviseert over levenscyclusbeheer. Wanneer er centrale afspraken zijn omtrent levenscyclusbeheer, kan een centrale overheidsregistrar de naleving van de gemaakte afspraken bevorderen.

3.5, Beleggen van rollen en verantwoordelijkheden: De centrale overheidsregistrar kan adviseren over het toekennen van (vastgestelde) verantwoordelijkheden aan rollen binnen de organisatie en zo de naleving van deze verantwoordelijkheden bevorderen.

3.8, Vormgeving van toezicht, monitoring en handhaving: Een centrale overheidsregistrar heeft een minimale effectiviteit als er geen toezicht ingeregeld is. In de huidige situatie wordt er niet toegezien op de gemaakte afspraken met DPC (registrar), waardoor deze lang niet altijd worden nageleefd. Omdat DPC momenteel geen toezichthoudende rol op zich neemt, maar enkel een adviserende, is de registrar niet verantwoordelijk voor de naleving van deze afspraken. Toezicht is daarom cruciaal om de voordelen van beleid te benutten.

3.4. Centrale afspraken omtrent levenscyclusbeheer

Algemeen

Centrale afspraken omtrent het levenscyclusbeheer van internetdomeinen omvatten de registratie, verhuizen, uitfaseren/offline halen en vrijgeven van domeinen. Momenteel zijn er geen centrale afspraken rondom het beheren van de levenscyclus.

Voordelen

Door het bieden van een centrale set aan afspraken hebben overheidsorganisaties de handvatten om de activiteiten rondom levenscyclusbeheer van hun internetdomeinen beter te reguleren. Het stellen van randvoorwaarden en het begrenzen van keuzemogelijkheden zorgt voor een minder ‘grijs gebied’ over het omgaan met internetdomeinen. Dit maakt het makkelijker voor decentrale (portfolio)beheerders of (website)eigenaren om te bepalen wat ze met hun internetdomeinen moeten doen, wat risico’s kan voorkomen. Daarnaast zorgt het meer grip krijgen op het internetdomeinportfolio dat wildgroei wordt beperkt. Het maken van centrale afspraken draagt zo niet alleen bij aan het zijn van een eenduidige overheid, maar ook aan de herkenbaarheid, veiligheid en betrouwbaarheid van de overheid. Zo kunnen afspraken omtrent de naamgeving van domeinen zorgen voor een verbeterde herkenbaarheid, en

zorgen afspraken omtrent het tijdig offline halen van een domein voor meer veiligheid. Dit zorgt voor meer vertrouwen van de burger in de (digitale) overheid.

Nadelen

Het hebben van centrale afspraken biedt minder flexibiliteit en vrijheid voor organisaties om dit proces in te richten en ervan af te wijken. Op deze manier kost het maken van uitzonderingen meer tijd, omdat er formele goedkeuring nodig is om andere processtappen te nemen dan in de regelgeving beschreven staan.

Implementatieadvies

Het advies is om centraal concrete afspraken te maken met betrekking tot levenscyclusbeheer, wat de veiligheid, herkenbaarheid en betrouwbaarheid bevordert en wildgroei beperkt. Dit geeft overheidsorganisaties meer handvatten voor het beheren van hun domeinportfolio en voorkomt het voortbestaan van kwetsbare internetdomeinen. Er zijn een aantal concrete oplossingen gedaan om in deze afspraken op te nemen. Deze zijn uitgewerkt in de bijlage. Hieronder volgen een aantal voorbeelden van afspraken die de herkenbaarheid en veiligheid van overheidsdomeinen verbeteren.

Onder andere is het gewenst om registratiecriteria op te stellen, zodat er minder makkelijk nieuwe domeinnamen worden geregistreerd. Dit beperkt wildgroei van internetdomeinen en bevordert de herkenbaarheid en vindbaarheid van de overheid. In de bijlage is een voorstel gedaan voor een registratieproces. Ook zijn richtlijnen voor naamgeving van internetdomeinen cruciaal, zodat de naamgeving herleidbaar is naar de desbetreffende overheidsorganisatie. Dit zorgt ervoor dat burgers beter herkennen welke internetdomeinen van de overheid zijn. In de bijlage is in de procesrichtlijnen voor levenscyclusbeheer verduidelijkt wat hieronder verstaan wordt.

Om op kwaliteit en veiligheid in te spelen, wordt aanbevolen om een CISO of CIO het mandaat te geven om internetdomeinen offline te halen wanneer deze na een bepaalde periode en een oproep tot verbetering nog niet volledig voldoen aan veiligheidseisen. Dit zorgt ervoor dat er geen kwetsbare internetdomeinen voor langere tijd online blijven staan. Ook is het advies om een internetdomein van de overheid niet meer vrij te geven wanneer hier e-mail op heeft gedraaid, om te voorkomen dat internetdomeinen van de overheid misbruikt worden voor e-mail spoofing. Echter is dit afhankelijk van de herkenbaarheid van de domeinnaam. Bijvoorbeeld met de verandering van ‘minvenj’ naar ‘minjenv’ is het niet wenselijk om ‘minvenj’ vrij te geven, terwijl een minder herkenbare domeinnaam wellicht wel na 10 jaar vrijgegeven kan worden volgens de richtlijnen van Z-Cert[4]. In de bijlage zijn deze veiligheidsafspraken verder uitgewerkt, en is er een voorstel voor procesinrichting opgesteld om levenscyclusbeheer beter in te bedden. Naast de concrete oplossingen in de bijlage, bieden ook de handreiking verlopen domeinnamen[4] en de handreiking

[4] Handreiking verlopen domeinnamen, Z-CERT. (2021). Geraadpleegd via Z-CERT_Handreiking2021.pdf

beheer internetdomeinen Rijksoverheid[5] suggesties voor een meer concrete en aansturende procesinrichting omtrent levenscyclusbeheer.

Er wordt geadviseerd om de afspraken centraal vast te leggen in het internetdomeinbeleid, maar de interne inrichting ervan decentraal te beleggen bij overheidsorganisaties. Op deze manier hebben overheidsorganisaties zelf de vrijheid om de afspraken te beleggen als verantwoordelijkheid bij rollen in de organisatie. De centrale overheidsregistrar kan deze afspraken uitdragen. Zij adviseren over hoe de afspraken intern belegd kunnen worden en welke rollen hiervoor geschikt zijn.

Combineren met andere oplossingen

3.1, Register Internetdomeinnamen Overheid (RIO): Door overheidsdomeinen te inventariseren met RIO, is het overzichtelijk voor welke internetdomeinen deze afspraken gelden. Dit maakt het makkelijker binnen een organisatie om te sturen op afspraken omtrent levenscyclusbeheer. Anderzijds kunnen wijzigingen die plaatsvinden als gevolg van deze afspraken gelijk gecommuniceerd worden naar het beheer van RIO, wat het mogelijk maakt om wijzigingen direct door te voeren. Dit zorgt ervoor dat het overzicht actueel blijft.

3.2, Herkenbare overheidsextensie: Een herkenbare overheidsextensie faciliteert levenscyclusbeheer, waardoor het afspraken omtrent dit beheer kan ondersteunen. Bij het implementeren van een herkenbare overheidsextensie is het mogelijk om afspraken vast te leggen onder afspraken omtrent levenscyclusbeheer. Bijvoorbeeld wanneer een nieuw domein geregistreerd wordt onder de herkenbare overheidsextensie (en wanneer niet. Op deze manier kunnen er afspraken over de levenscyclus van een overheidsdomein gemaakt worden wanneer deze geregistreerd worden onder de herkenbare overheidsextensie. Het dient dan al vanaf het registratieproces als een stok achter de deur, waardoor het wildgroei beperkt.

3.3, Centrale overheidsregistrar: Een centrale overheidsregistrar adviseert over levenscyclusbeheer. Wanneer er centrale afspraken zijn omtrent levenscyclusbeheer, kan een centrale overheidsregistrar de naleving van de gemaakte afspraken bevorderen door dit proces te ondersteunen.

3.5, Beleggen van rollen en verantwoordelijkheden: Door het maken van centrale afspraken omtrent levenscyclusbeheer te combineren met het beleggen van rollen en verantwoordelijkheden, is het mogelijk om bepaalde afspraken te beleggen bij vastgestelde verantwoordelijkheden of toebedeelde rollen. Door te verankeren welke afspraken onder welke verantwoordelijkheid vallen, krijgt men meer grip op het beheren van internetdomeinen.

3.6, Leverancierseisen: Centrale afspraken omtrent levenscyclusbeheer kunnen doorgevoerd worden bij het stellen van leverancierseisen als internetdomeinbeheer

[5] Inhoudelijke informatie met betrekking tot de verplichte richtlijnen online middelen zijn te vinden op de pagina 'Handreiking Verplichte richtlijnen websites en andere online middelen', UBR (2019). Deze dient geactualiseerd te worden.

wordt uitbesteed. Op deze manier blijven externe leveranciers op één lijn met overheidsorganisaties en loopt men niet tegen uiteenlopende beheerprocessen aan.

3.7, Verplicht periodieke kwaliteitscontroles: Verplichte periodieke kwaliteitscontroles gaan met name om de controle op het toepassen van open standaarden en andere verplichte richtlijnen, maar kunnen ook afspraken omtrent levenscyclusbeheer omvatten. Een voorbeeld hiervan is het controleren of een domein nog online staat na het voor langere periode niet voldoen aan veiligheidseisen.

3.8, Vormgeving van toezicht, monitoring en handhaving: Bij het vormgeven van toezicht, monitoring en handhaving is het mogelijk om toezicht op de naleving van de gemaakte afspraken omtrent levenscyclusbeheer in te bedden. Zoals het controleren of een registratie bij de (centrale) overheidsregistrar is geregistreerd, en of een domein is uitgefaseerd bij het behalen van het (communicatie)doel van het domein.

3.9, Interbestuurlijke werkgroep waarbij iedere overheidslaag gerepresenteerd is: In het centrale Interbestuurlijke werkgroep kunnen 'best practices' gedeeld worden met betrekking tot levenscyclusbeheer van internetdomeinen, waardoor overheidsbrede kennisdeling en kwaliteitsverbetering wordt gestimuleerd.

3.10, Interdisciplinair expertiseteam: Doordat het mogelijk is om centrale afspraken omtrent levenscyclusbeheer bij zowel een communicatiedirectie als een IT-directie te beleggen, is het voordelig om een interdisciplinair expertiseteam te creëren waarin men over het beleggen en naleven van deze afspraken kan communiceren. Als afspraken op een versplinterde manier verdeeld zijn over verschillende afdelingen en/of disciplines, is het extra van belang hier duidelijkheid over te creëren. Zo voorkom je dat er afspraken op de verkeerde plek belegd zijn of deze niet worden nageleefd.

3.5. Beleggen van rollen en verantwoordelijkheden

Algemeen

Om internetdomeinbeheer beter aan te sturen, is het van belang dat de *governance* omtrent internetdomeinbeheer duidelijk belegd is. Hiervoor is het cruciaal dat verantwoordelijkheden en rollen rondom internetdomeinbeheer vastgelegd zijn. Denk hierbij aan het vastleggen van verantwoordelijkheden als het voldoen aan kwaliteitseisen van internetdomeinen, het vastleggen van eigenaarschap, of het actueel houden van het domeinportfolio.

Voordelen

Internetdomeinbeheer kan beter aangestuurd worden als rollen en verantwoordelijkheden duidelijk belegd zijn. Als rollen en verantwoordelijkheden intern vastgelegd zijn, bevordert het de communicatie op het gebied van internetdomeinbeheer en zorgt het voor het hebben van centrale aanspreekpunten, wat zowel intern als extern zijn voordelen heeft. Door het bieden van kaders en/of randvoorwaarden in beleid biedt het organisaties handvatten om beheer zelf beter in te richten, maar behouden zij wel hun autonomie om dit toe te passen op hun eigen organisatiestructuur. Ook bevordert dit de nazorg bij overdracht van verantwoordelijkheden bij het verlaten van een functie.

Nadelen

Het is nadelig om het niet te verplichten. Naleving is zonder verplichting nog steeds de verantwoordelijkheid van de organisatie zelf. Als het blijft bij kaderstellende richtlijnen en er geen verplichtingen aan zitten, zitten er geen consequenties aan bij het niet naleven van de belegde verantwoordelijkheden en het toebedelen aan rollen. Als organisaties de verantwoordelijkheden niet (voldoende) naleven en rolverdeling onduidelijk blijft, gaat het ten koste van de actualiteit van informatie en van internetdomeinbeheer in zijn geheel. Een ander risico is dat organisaties het mogelijk suboptimaal inrichten in de eigen organisatie, waardoor de uitvoering ervan niet effectief is.

Implementatieadvies

Het advies is om verantwoordelijkheden rondom internetdomeinbeheer centraal vast te leggen in het internetdomeinbeleid en het beleggen ervan decentraal in te laten richten door de organisaties zelf. De vastgestelde verantwoordelijkheden (een voorzet is gedaan in bijlage 2) die vallen onder internetdomeinbeheer kunnen zo door de desbetreffende organisatie zelf verdeeld worden onder relevante rollen die zij intern hanteren. Over het algemeen zijn dit rollen als (functioneel) beheerder, portfoliobeheerder/liaison, (web)eigenaar, of communicatieadviseur. De CISO of CIO kan de verantwoordelijkheden die vastgelegd zijn delegeren onder deze rollen. Beleid kan hiervoor kaders of randvoorwaarden bieden zonder rollen bij voorbaat in te vullen. Bijvoorbeeld door verantwoordelijkheden vast te leggen, maar de rolinvulling ervan open te laten en er enkel advies over uit te brengen. Zo kunnen rollen en verantwoordelijkheden centraal worden aangestuurd, maar worden toegepast op de organisatiestructuur van de desbetreffende organisatie. De centrale overheidsregistrar kan hierbij helpen door te adviseren over de rolverdeling.

De organisatie dient de verantwoordelijkheid -en rolverdeling schriftelijk vast te leggen in de organisatie en deze te communiceren naar de centrale overheidsregistrar en het beheer van RIO. Op deze manier is het voor iedere overheidspartij inzichtelijk waar verantwoordelijkheden belegd zijn, en wie aanspreekpunten zijn met betrekking tot internetdomeinbeheer. Bijvoorbeeld wie eigenaarschap van een internetdomein draagt, wie het centrale aanspreekpunt is, of wie verantwoordelijk is voor levenscyclusbeheer. Dit bevordert de dienstverlening van de centrale overheidsregistrar richting overheidsorganisaties, maar het bevordert ook intern beheer en communicatie tussen overheidspartijen. Doordat intern is vastgelegd en overzichtelijk is gemaakt waar verantwoordelijkheden belegd zijn, voorkomt het *governance*-problemen. Denk hierbij aan overlap in taken, het dubbel uitvoeren van taken of het vergeten van taken. Ook voorkomt het dat vragen op de verkeerde tafel terecht komen, doordat duidelijk gecommuniceerd is waar verantwoordelijkheden liggen. Al met al zorgt het voor een betere beheersing van internetdomeinen doordat *governance* binnen overheidsorganisaties beter is ingericht.

In de bijlage zijn suggesties gedaan met betrekking tot welke verantwoordelijkheden belegd moeten zijn in een organisatie, en welke rollen hier relevant voor zijn. Het

advies is om deze suggesties nader te bepalen voor vaststelling. Eveneens moet nagedacht worden over het verdelen van verantwoordelijkheden in (publiek-private) samenwerkingsverbanden. Directie Digitale Samenleving (BZK) kan deze verantwoordelijkheden en rollen nader definiëren met behulp van andere overheidsorganisaties (zoals de betrokken organisaties in dit onderzoek), en opnemen in het internetdomeinbeleid.

Combineren met andere oplossingen

3.3, Centrale overheidsregistrar: De centrale overheidsregistrar kan adviseren over het toekennen van verantwoordelijkheden aan rollen binnen de organisatie en zo de naleving van deze verantwoordelijkheden bevorderen.

3.4, Centrale afspraken omtrent levenscyclusbeheer: Het beleggen van rollen en verantwoordelijkheden in combinatie met het maken van centrale afspraken omtrent levenscyclusbeheer maakt het mogelijk om bepaalde afspraken te beleggen bij vastgestelde verantwoordelijkheden of toebedeelde rollen. Door te verankeren welke afspraken onder welke verantwoordelijkheid vallen, krijgt men meer grip op het beheren van internetdomeinen.

3.6, Leverancierseisen: Het beleggen van verantwoordelijkheden en rollen met betrekking tot externe leveranciers kan divergentie tussen de overheidsorganisatie en de externe partij tegengaan. Door het aanstellen van een aanspreekpunt voor de externe leverancier verbetert het communicatie tussen de leverancier en de overheidsorganisatie. Ook kan de verantwoordelijkheid bij dit centrale aanspreekpunt belegd worden om aan te sturen op leverancierseisen, wat naleving ervan bevordert.

3.7, Verplicht periodieke kwaliteitscontroles: Afhankelijk van of periodieke kwaliteitscontroles intern of extern belegd worden, kan het als verantwoordelijkheid belegd worden. Als periodieke kwaliteitscontroles verplicht worden om intern in te richten, is het functioneel om dit als verantwoordelijkheid te beleggen in beleid. Zo kan de desbetreffende organisatie deze verantwoordelijkheid toekennen aan een rol binnen de organisatie. Deze rol is dan verantwoordelijk voor het uitvoeren van periodieke kwaliteitscontroles en voor het aansturen op de kwaliteit. Anderzijds, als periodieke kwaliteitscontroles extern worden belegd, is het eveneens van belang om verantwoordelijkheden en rollen te beleggen. Het beleggen van verantwoordelijkheden zorgt ervoor dat een externe partij de verantwoordelijke rol kan aanspreken op het niet naleven van kwaliteitseisen. Dit werkt effectiever wanneer hier een persoon aan gekoppeld is dan wanneer de organisatie verantwoordelijk wordt gesteld. Als verantwoordelijkheden niet zijn vastgelegd, is het moeilijker om iemand aan te spreken op het niet naleven van verantwoordelijkheden.

3.8, Vormgeving van toezicht, monitoring en handhaving: In het vormgeven van toezicht, monitoring en handhaving kan opgenomen worden om te controleren of de vastgestelde verantwoordelijkheden (schriftelijk) vastgelegd en toegekend zijn, of de rolverdeling actueel is, en of de verantwoordelijkheden worden nageleefd in een organisatie. Zo kunnen zij bepaalde rollen aansturen wanneer de toegekende verantwoordelijkheden niet (voldoende) nageleefd zijn.

3.9, Interbestuurlijke werkgroep waarin iedere overheidslaag gerepresenteerd is: Door een centraal Interbestuurlijke werkgroep in te richten waarin iedere overheidslaag gerepresenteerd is, is het mogelijk om 'best practices' te delen. Bijvoorbeeld het delen van processen omtrent het naleven van verantwoordelijkheden en de rolverdeling die intern belegd is om deze verantwoordelijkheden na te komen.

3.10, Interdisciplinair expertiseteam: Als er een interdisciplinair expertiseteam is ingericht, biedt het de mogelijkheid om binnen dit team rolverdeling te bespreken, verantwoordelijkheden toe te schrijven, en te communiceren over het opvolgen van deze verantwoordelijkheden. Het zorgt voor convergentie tussen relevante functies, maar ook voor convergentie tussen betrokken afdelingen, wat naleving van verantwoordelijkheden en communicatie daarover bevordert.

3.6. Eisen bij uitbesteden van dienstverlening aan externe leveranciers

Algemeen

Er worden leverancierseisen gesteld bij het uitbesteden van dienstverlening op basis van open standaarden en verplichte richtlijnen[6] van de Rijksoverheid. Wanneer een externe leverancier diensten verleent aan overheidsorganisaties, is het cruciaal dat deze (blijven) voldoen aan de gestelde eisen en richtlijnen. Echter voldoen nog steeds veel (Rijks)overheidswebsites niet aan deze verplichtingen. In het websiteregister van de Rijksoverheid is bijvoorbeeld te zien welke Rijkswebsites hier nog niet (volledig) aan voldoen. Omdat veel (Rijks)overheidsorganisaties dienstverlening uitbesteden, is het van cruciaal belang dat externe leveranciers deze eisen ondersteunen.

Voordelen

Door overheidsbreed leverancierseisen te stellen en op aan te sturen voorkomt men dat contractuele afspraken met een externe leverancier na een bepaald termijn niet meer voldoen aan de eisen van de Rijksoverheid. Het is cruciaal dat externe leveranciers de verplichte richtlijnen ondersteunen om (Rijks)overheidswebsites (blijvend) te laten voldoen aan kwaliteitseisen.

Nadelen

Zonder toezicht is het moeilijk te controleren of er daadwerkelijk eisen worden gesteld in contracten met externe leveranciers en of deze worden nageleefd.

Implementatieadvies

Allereerst is het advies om de verplichte richtlijnen online middelen[6] te actualiseren. Als deze geactualiseerd zijn, wordt geadviseerd om open standaarden en andere verplichte richtlijnen als basiseisen op te nemen voor leverancierseisen. Als een overheidsorganisatie voor een externe leverancier kiest, is het cruciaal dat de externe

[6] Inhoudelijke informatie met betrekking tot de verplichte richtlijnen online middelen zijn te vinden op de pagina 'Handreiking Verplichte richtlijnen websites en andere online middelen', UBR (2019). Deze dient geactualiseerd te worden.

leverancier voldoet aan de gestelde kwaliteitseisen vanuit de Rijksoverheid en deze kan ondersteunen. Dit moet een ingangseis zijn bij het aangaan van een contract.

Echter houden externe leveranciers zich lang niet altijd aan de gestelde eisen of kunnen deze niet ondersteunen. Hier moet beter op aangestuurd worden. Wanneer een contract voor een langere periode is vastgelegd en eisen later worden aangepast, is het erg lastig dit bij te stellen. Het is daarom van belang dat een contract bijgesteld kan worden wanneer kwaliteitseisen veranderen, zodat externe leveranciers blijven voldoen aan de eisen die de Rijksoverheid stelt. Dit draagt bij aan de kwaliteit van dienstverlening van externe leveranciers aan overheidsorganisaties. Hoe dit juridisch mogelijk is, dient nader bepaald te worden aan de hand van juridische kaders en wat de impact van een contractwijziging gaat betekenen. Hiervoor is het advies om juridische experts te raadplegen voor opname in het internetdomeinbeleid.

Verplichte richtlijnen en gestelde leverancierseisen moeten vertaald worden naar een overheidsbrede richtlijn om vanaf het startpunt in offerteaanvragen en aanbestedingen door te voeren en voor organisaties het makkelijker te maken om dit bij ingang van het contract vast te leggen. Dit heeft echter actualiteit nodig, maar valt buiten de scope van dit onderzoek.

Combineren met andere oplossingen

3.4, Afspraken omtrent levenscyclusbeheer: Centrale afspraken omtrent levenscyclusbeheer kunnen doorgevoerd worden bij het stellen van leverancierseisen als internetdomeinbeheer wordt uitbesteed. Op deze manier blijven externe leveranciers op één lijn met overheidsorganisaties en loopt men niet tegen uiteenlopende beheerprocessen aan.

3.5, Beleggen van rollen en verantwoordelijkheden: Het beleggen van verantwoordelijkheden en rollen met betrekking tot externe leveranciers kan divergentie tussen de overheidsorganisatie en de externe partij tegengaan. Door het aanstellen van een aanspreekpunt voor de externe leverancier verbetert het communicatie tussen de leverancier en de overheidsorganisatie. Ook kan de verantwoordelijkheid bij dit centrale aanspreekpunt belegd worden om aan te sturen op leverancierseisen, wat naleving ervan bevordert.

3.7, Verplicht periodieke kwaliteitscontroles: Als periodieke kwaliteitscontroles op toepassing van open standaarden en andere verplichte richtlijnen vereist zijn, is het mogelijk om leveranciers waaraan dienstverlening is uitbesteed mee te nemen in controle en op de hoogte te brengen bij het niet (volledig) voldoen aan de eisen van de Rijksoverheid. Op deze manier worden leveranciers vaker gealarmeerd en meer bewust van het ondersteunen van de leverancierseisen.

3.8, Vormgeving van toezicht, monitoring en handhaving: Afhankelijk van of toezicht, monitoring en handhaving centraal of decentraal wordt ingericht, kan controle op leverancierseisen ingebed worden. Bij decentrale inrichting van toezicht, monitoring en handhaving, kan er intern binnen organisaties een toezichtsrol worden opgenomen om controle op externe leveranciers te voeren.

3.7. Interne controle via verplichte periodieke controlechecks

Algemeen

Het verplicht stellen van interne periodieke kwaliteitscontroles op toepassing van open standaarden en andere verplichte richtlijnen[7]. Deze dienen intern ingericht te worden per overheidsorganisatie. Ook moet er een termijn vast komen te staan over de frequentie dat de checks uitgevoerd dienen te worden.

Voordelen

Door periodiek kwaliteitscontroles uit te voeren op toepassing van open standaarden en andere verplichte richtlijnen komt er meer grip op de kwaliteit van internetdomeinen en achterliggende online middelen. Het draagt bij aan het voorkomen dat er gebreken voor een langere periode blijven sudderen, en mogelijk voor ernstige gevolgen zorgen, zoals veiligheidslekken of domein-spoofing. Op deze manier kan een organisatie sneller inspelen op risicovolle omstandigheden, en ligt er meer druk op het voldoen aan de (veiligheids)eisen. Dit bevordert te veiligheid van de overheid en het vertrouwen van de burger in de overheid. Ook zijn de kwaliteitscontroles vrij makkelijk van aard om vorm te geven. Dit kan bijvoorbeeld (gedeeltelijk) door gebruik te maken van het internet.nl[8] dashboard.

Nadelen

Het kost extra tijd en mogelijk capaciteit om de periodieke kwaliteitscontroles in te richten wanneer dit nog niet is ingericht binnen een organisatie. Om dit decentraal in te richten is capaciteit vereist om dit bij elke overheidsorganisatie te beleggen. Ook is het van belang te sturen op de uitkomsten van de kwaliteitscontroles, omdat alleen de checks zelf niet zorgen voor naleving. Daarom is nazorg van belang en dient er verantwoordelijkheid te worden gedragen om de kwaliteit op basis van de resultaten aan te sturen en de acties na te leven. Allerlaatst is het een nadeel dat zonder vormgeving van centraal toezicht het onduidelijk is in welke mate het wordt nageleefd en hoe effectief het werkt.

Implementatieadvies

Het advies is dat overheidsorganisaties verplicht worden om intern periodieke controlechecks uit te voeren op toepassing van open standaarden en verplichte richtlijnen[7]. Dat betekent dat een organisatie zelf dit in beheer kan nemen en aan de hand van eigen organisatiestructuur kan inregelen. Geadviseerd wordt om dit op te nemen als verantwoordelijkheid en aan een rol binnen de organisatie te koppelen (zie 3.5). Eveneens dient een organisatie een eindverantwoordelijke aan te stellen, dit kan bijvoorbeeld de CISO of CIO zijn. Op deze manier is de verantwoordelijkheidsverdeling duidelijk, en kan er makkelijker intern gecontroleerd worden op naleving van de

[7] Inhoudelijke informatie met betrekking tot de verplichte richtlijnen online middelen zijn te vinden op de pagina 'Handreiking Verplichte richtlijnen websites en andere online middelen', UBR (2019). Deze dient geactualiseerd te worden.

[8] Op de testtool www.internet.nl kun je eenvoudig testen of je internet up-to-date is door het testen van je website, e-mail en internetverbinding op toepassing van internetstandaarden.

verplichting. Ook kan de kwaliteit van internetdomeinen zo beter centraal aangestuurd worden en inzichtelijk worden gemaakt. Doordat door middel van RIO overheidsdomeinen al in kaart zijn gebracht is het internetdomeinportfolio meer op orde, en kost het minder tijd en moeite om de kwaliteitscontroles uit te voeren. Er is dan al inzichtelijk gemaakt op welke overheidsdomeinen de kwaliteitscontrole uitgevoerd moet worden. Geadviseerd wordt om de kwaliteitscontroles per kwartaal of halfjaarlijks in te richten, zodat er bij afwijkingen tijdig bijgestuurd kan worden, maar de organisatie genoeg tijd heeft om te voldoen aan de eisen voor de volgende controle. Als binnen een bepaald termijn het internetdomein nog niet voldoet (aan veiligheidseisen), kan de CISO/CIO het internetdomein offline halen (zoals benoemd bij 3.4). Kwaliteitscontroles zijn dus tevens goed toe te passen op afspraken omtrent levenscyclusbeheer.

Combineren met andere oplossingen

3.1, Register Internetdomeinnamen Overheid (RIO): Het overzicht van RIO kan gebruikt worden voor het uitvoeren van verplichte periodieke kwaliteitscontroles op open standaarden en andere verplichte richtlijnen.

3.3, Centrale overheidsregistrar: Het is een mogelijkheid om toezicht op de periodieke kwaliteitscontroles te beleggen bij de centrale overheidsregistrar als de voorkeur ligt bij het centraal inrichten ervan. De centrale overheidsregistrar moet dan wel een meer toezichthoudende, monitorende rol aannemen, in plaats van enkel adviserend.

3.4, Afspraken omtrent levenscyclusbeheer: Verplichte periodieke kwaliteitscontroles gaan met name om de controle op het toepassen van open standaarden en andere verplichte richtlijnen, maar kunnen ook afspraken omtrent levenscyclusbeheer omvatten. Bijvoorbeeld of een domein nog online staat na het voor langere periode niet voldoen aan veiligheidseisen.

3.5, Beleggen van rollen en verantwoordelijkheden: Afhankelijk van of periodieke kwaliteitscontroles intern of extern belegd worden, kan het als verantwoordelijkheid belegd worden. Als periodieke kwaliteitscontroles verplicht worden om intern in te richten, is het functioneel om dit als verantwoordelijkheid te beleggen in beleid. Zo kan de desbetreffende organisatie deze verantwoordelijkheid toekennen aan een rol binnen de organisatie. Deze rol is dan verantwoordelijk voor het uitvoeren van periodieke kwaliteitscontroles en voor het aansturen op de kwaliteit. Anderzijds, als periodieke kwaliteitscontroles extern worden belegd, is het eveneens van belang om verantwoordelijkheden en rollen te beleggen. Het beleggen van verantwoordelijkheden zorgt ervoor dat een externe partij de verantwoordelijke rol kan aanspreken op het niet naleven van kwaliteitseisen. Dit werkt effectiever wanneer hier een persoon aan gekoppeld is dan wanneer de organisatie verantwoordelijk wordt gesteld. Als verantwoordelijkheden niet zijn vastgelegd, is het moeilijker om iemand aan te spreken op het niet naleven van verantwoordelijkheden.

3.6, Leverancierseisen: Als periodieke kwaliteitscontroles op toepassing van open standaarden en andere verplichte richtlijnen vereist zijn, is het mogelijk om leveranciers waaraan dienstverlening is uitbesteed mee te nemen in controle en op de hoogte te brengen bij het niet (volledig) voldoen aan de eisen van de Rijksoverheid. Op deze manier worden leveranciers vaker gealarmeerd en meer bewust van het

ondersteunen van de leverancierseisen.

3.8, Vormgeving van toezicht, monitoring en handhaving: Het is mogelijk om periodieke kwaliteitscontroles in te bedden op de plek waar toezicht, monitoring en handhaving met betrekking tot internetdomeinbeheer wordt ingericht.

3.8. Centraal vormgeven van toezicht, monitoring en handhaving

Algemeen

Het beleggen van toezicht, monitoring en handhaving op naleving van gemaakte afspraken omtrent internetdomeinbeheer. Op dit moment zijn toezichthoudende taken nergens formeel vastgelegd, en is toezicht en handhaving niet ingeregeld. Er kan overwogen worden om dit centraal in te regelen, of decentraal te laten inrichten. Bij het centraal beleggen kan men ervoor kiezen toezichthoudende taken toe te wijzen aan een bestaande overheidsorganisatie. Bij decentrale inrichting kan vastgelegd worden dat desbetreffende organisaties zelf toezicht beleggen, intern of extern. Tevens is het mogelijk om toezicht gedeeltelijk te automatiseren, waar dat makkelijk kan.

Voordelen

Toezicht, monitoring en handhaving zorgen voor een verbetering in naleving van gemaakte afspraken. Voor veel organisaties biedt het een stok achter de deur om actief bezig te zijn met het blijven voldoen aan gestelde eisen. Dit komt internetdomeinbeheer bij overheidsorganisaties ten goede. Doordat afspraken beter worden nageleefd, verbetert dit de herkenbaarheid, veiligheid en betrouwbaarheid van de overheid. Overheidsorganisaties hebben vaak weinig capaciteit voor internetdomeinbeheer, dus het centraal inrichten van toezicht, monitoring en handhaving zal overheidsorganisaties ontzorgen en ondersteunen.

Nadelen

Het inrichten van een toezichthoudende rol vereist extra capaciteit. Als toezichthoudende taken worden belegd bij een bestaande overheidsorganisatie, dient deze te worden uitgebreid om dit overheidsbreed te kunnen dekken. Wanneer er een nieuw overheidsorgaan opgericht dient te worden, moet hier ook capaciteit voor beschikbaar gesteld worden. Maar ook als het decentraal wordt belegd, moeten overheidsorganisaties intern capaciteit vergroten om deze taken te kunnen beleggen. Er zal dus structureel capaciteit moeten vrijkomen om dit blijvend vorm te geven.

Implementatieadvies

Het advies is om toezicht, monitoring en handhaving centraal te beleggen bij één overheidsorganisatie. De centrale overheidsregistrar kan dit inbedden. Als de centrale overheidsregistrar toezicht, monitoring en handhaving opneemt in het takenpakket, kan de toezichtsrol uitgebreid worden naar het monitoren van en handhaven op de gemaakte afspraken in het internetdomeinbeleid.

Zo is het relevant om toezicht te houden op afspraken omtrent levenscyclusbeheer door organisaties te laten terugkoppelen over vastlegging van procesinrichting, om op die manier bijvoorbeeld te monitoren of registratieprocessen en uitfaseringsprocessen

volgens de gestelde regels verlopen (zie bijlage 1). Dit geldt eveneens voor schriftelijke vastlegging van verantwoordelijkheden en rollen. Overheidsorganisaties dienen dit intern in te regelen, en bij controle de vastlegging te kunnen aantonen. Ook is het van belang om erop toe te zien of overheidsorganisaties hun (nieuwe) internetdomeinen registreren in RIO, en het interne overzicht aansluit bij de actualiteit van het register. Op deze manier kan voor iedere oplossing een vorm van toezicht ingeregeld worden.

Als toezicht bij een centrale partij is belegd krijgen bevindingen hoogstwaarschijnlijk meer prioriteit dan wanneer het intern belegd is. Toezicht, monitoring en handhaving moet expliciet vastgelegd worden op de gemaakte afspraken die in het internetdomeinbeleid worden opgenomen. Overheidsorganisaties moeten aantonen dat ze het internetdomeinbeheer volgens de afspraken op orde hebben aan de centrale overheidsregistrar. Momenteel ontbreekt centraal toezicht, waardoor overheidsorganisaties lang niet altijd afspraken nakomen. Het is daarom gewenst om sancties te binden aan gemaakte afspraken in het internetdomeinbeleid, zodat er gehandhaafd wordt wanneer er structureel niet wordt voldaan aan de gestelde eisen. Sancties kan de centrale overheidsregistrar opleggen door de CISO/CIO aan te sturen om internetdomeinen tijdelijk offline te halen (zoals benoemd in 3.4), zelf een internetdomein offline te halen, of te werken met een *naming & shaming* proces dat in RIO getoond wordt wanneer een overheidsdomein niet (volledig) voldoet aan de gestelde (veiligheids)eisen na een bepaald termijn.

Combineren met andere oplossingen

3.1, Register Internetdomeinnamen Overheid (RIO): Het overzicht van RIO kan gebruikt worden voor het houden van toezicht, monitoring en handhaving. Doordat door RIO al geclassificeerd is wat onder overheidsdomeinen vallen, is al geïdentificeerd welke internetdomeinen aan de gestelde eisen moeten voldoen. Dit maakt toezicht, monitoring en handhaving overzichtelijker.

3.3, Centrale overheidsregistrar: Een centrale overheidsregistrar heeft een minimale effectiviteit als er geen toezicht ingeregeld is. In de huidige situatie wordt er niet toegezien op de gemaakte afspraken met de registrar, waardoor deze lang niet altijd worden nageleefd. Toezicht is daarom cruciaal om de voordelen te benutten.

3.4, Afspraken omtrent levenscyclusbeheer: Bij het vormgeven van toezicht, monitoring en handhaving is het mogelijk om toezicht op de naleving van de gemaakte afspraken omtrent levenscyclusbeheer in te bedden. Zoals het controleren of een registratie bij de centrale overheidsregistrar is geregistreerd, en of dat een domein is uitgefaseerd bij het (langdurig) niet voldoen aan veiligheidseisen.

3.5, Beleggen van rollen en verantwoordelijkheden: In het vormgeven van toezicht, monitoring en handhaving kan opgenomen worden om te controleren of de vastgestelde verantwoordelijkheden (schriftelijk) vastgelegd en toegekend zijn, of de rolverdeling actueel is, en of de verantwoordelijkheden worden nageleefd in een organisatie. Zo kunnen zij bepaalde rollen aansturen wanneer de toegekende verantwoordelijkheden niet (voldoende) nageleefd zijn.

3.6, Leverancierseisen: Afhankelijk van of toezicht, monitoring en handhaving centraal of decentraal wordt ingericht, kan controle op leverancierseisen ingebed worden. Bij

decentrale inrichting van toezicht, monitoring en handhaving, kan er intern binnen organisaties een toezichtsrol worden opgenomen om controle op externe leveranciers te voeren.

3.7, Verplicht periodieke kwaliteitscontroles: Het is mogelijk om periodieke kwaliteitscontroles in te bedden op de plek waar toezicht, monitoring en handhaving met betrekking tot internetdomeinbeheer wordt ingericht.

3.9. Interbestuurlijke werkgroep waarbij iedere overheidslaag gerepresenteerd is

Algemeen

Het inrichten van een interbestuurlijke werkgroep gericht op internetdomeinbeheer, waarbij iedere overheidslaag gerepresenteerd is. Op deze manier is het mogelijk om informatie uit te wisselen tussen overheden op het gebied van internetdomeinbeheer, en stimuleert het kennisdeling overheidsbreed.

Voordelen

Het is mogelijk om het internetdomeinbeleid op deze manier actief te onderhouden, door doorontwikkeling van het internetdomeinbeleid en advisering over de implementatie van het beleid te stimuleren in de werkgroep. Stimulering van kennisdeling zorgt voor convergentie tussen overheden, doordat zij op de hoogte gesteld worden van ontwikkelingen op het gebied van internetdomeinbeheer. Tevens biedt het draagvlak voor het internetdomeinbeleid, en/of de invulling daarvan. Het delen van ‘best practices’ en knelpunten draagt bij aan de verbetering van overheidsbreed internetdomeinbeheer en het zijn van een eenduidige overheid.

Nadelen

Het succes van het overleg is afhankelijk van de toewijding van overheden.

Implementatieadvies

Geadviseerd wordt om het overheidsbrede, interbestuurlijke werkgroep in te richten, waarbij relevante rollen met betrekking tot internetdomeinbeheer (zoals beschreven in 3.5) van alle overheidslagen samenkomen. In het overleg kunnen zij kennis en ideeën uitwisselen over internetdomeinbeleid en de praktijkuitvoering ervan, maar ook over aanvullende maatregelen die getroffen dienen te worden in doorontwikkeling van het internetdomeinbeleid. Het overleg is niet vrijblijvend, maar heel actiegericht en gericht op het actueel houden en beter geïmplementeerd krijgen van het internetdomeinbeleid. De werkgroep BIO biedt een format voor de invulling ervan. Het overleg kan ingericht worden in een vergelijkbare structuur. Een periodieke herhaling is mogelijk, afhankelijk van de behoeften van de gerepresenteerde partijen. Geadviseerd wordt om dit eens per kwartaal te doen. Tevens helpt het overheidsorganisaties om samen afspraken te distribueren en na te komen. Ook is het mogelijk om via het Interbestuurlijke werkgroep signalen af te geven naar het bestuurlijk niveau vanuit de praktijkomgeving. Het CIP (werkgroep BIO) of ICTU (NORA) zouden geschikte partijen kunnen zijn om dit overleg te trekken.

Combineren met andere oplossingen

3.4, Centrale afspraken omtrent levenscyclusbeheer: In het centrale Interbestuurlijke werkgroep kunnen 'best practices' gedeeld worden met betrekking tot levenscyclusbeheer van internetdomeinen, waardoor overheidsbrede kennisdeling en kwaliteitsverbetering wordt gestimuleerd.

3.5, Beleggen van rollen en verantwoordelijkheden: Door een centraal Interbestuurlijke werkgroep in te richten waarin iedere overheidslaag gerepresenteerd is, is het mogelijk om 'best practices' te delen. Bijvoorbeeld het delen van processen omtrent het naleven van verantwoordelijkheden en de rolverdeling die intern belegd is om deze verantwoordelijkheden na te komen.

3.10. Intern interdisciplinair expertiseteam

Algemeen

Het samenstellen van een interdisciplinair expertiseteam binnen een organisatie om internetdomeinbeheer te verbeteren. Internetdomeinbeheer is een onderwerp dat meerdere disciplines kruist. Doordat zowel communicatiedirecties als IT gerelateerde afdelingen (en soms aanvullend nog andere disciplines) betrokken zijn in internetdomeinbeheer, is het van belang de communicatie en samenwerking tussen deze betrokkenen te bevorderen door middel van een interdisciplinair expertiseteam.

Voordelen

Het inzetten van een interdisciplinair expertiseteam bevordert internetdomeinbeheer op verschillende fronten. Het zorgt ervoor dat het onderwerp niet vanuit één perspectief wordt benaderd. Hierdoor voorkom je dat een communicatievraag bij een IT-afdeling komt te liggen, en andersom. Op deze manier ontstaat er meer grip op internetdomeinbeheer en bevordert het interne communicatie en samenwerking. Er is sneller in te spelen op behoeften en veranderingen, en verantwoordelijkheden en rollen zijn duidelijk belegd.

Nadelen

Het vergt capaciteit, die kleinere organisaties niet altijd voldoende hebben om dit in te richten. Ook zitten bij kleine organisaties verschillende disciplines in elkaar verweven.

Implementatieadvies

Het advies is om overheidsorganisaties te adviseren een interdisciplinair expertiseteam intern in te richten op het gebied van internetdomeinbeheer. Organisaties moeten dit zelf intern inregelen. Over de invulling ervan kan de centrale overheidsregistrar adviseren, op basis van de rollen in de organisatie. Als rolverdeling door middel van verantwoordelijkheid -en rolverdeling belegd is, is het inzichtelijk welke rollen relevant zijn voor het interdisciplinair expertiseteam. Dit hoeft niet vastgelegd te worden als een formeel team, maar gaat om het intern bevorderen van communicatie en samenwerking tussen verschillende afdelingen en disciplines. De CIO of CISO kan dit team opstellen en de rollen daarbinnen delegeren. Dit advies is meer relevant voor grotere overheidsorganisaties, omdat die over meer capaciteit beschikken om dit in te richten en er daar vaak een kloof bestaat tussen verschillende afdelingen. Kleinere overheidsorganisaties kampen vaker met een capaciteitsprobleem op het gebied van

internetdomeinbeheer. Ondanks het capaciteitsprobleem blijft internetdomeinbeheer een interdisciplinair onderwerp. Daarom kan het als streng advies worden opgenomen om, als er meerdere disciplines binnen een organisatie elkaar kruisen op het gebied van internetdomeinbeheer, dit intern in te richten. Dit zal de invulling van de andere oplossingen, zoals het beleggen van verantwoordelijkheden en het nakomen van afspraken omtrent levenscyclusbeheer, bevorderen.

Combineren met andere oplossingen

3.4, Centrale afspraken omtrent levenscyclusbeheer: Doordat het mogelijk is om centrale afspraken omtrent levenscyclusbeheer bij zowel een communicatiedirectie als een IT-directie te beleggen, is het voordelig om een interdisciplinair expertiseteam te hebben waarin men over het beleggen en naleven van deze afspraken kan communiceren. Als afspraken op een versplinterde manier verdeeld zijn over verschillende afdelingen en/of disciplines, is het van belang hier duidelijk over te communiceren. Zo voorkom je dat er afspraken op de verkeerde plek belegd zijn of deze niet worden nageleefd.

3.5, Beleggen van rollen en verantwoordelijkheden: Als er een interdisciplinair expertiseteam is ingericht, biedt het de mogelijkheid om binnen dit team rolverdeling te bespreken, verantwoordelijkheden te toebedelen, en te communiceren over het opvolgen van deze verantwoordelijkheden. Het zorgt voor convergentie tussen relevante functies, maar ook voor convergentie tussen betrokken afdelingen, wat naleving van verantwoordelijkheden en communicatie daarover bevordert.

4. Onderbouwing

In het onderstaande stuk zijn de bevindingen uit de eerste en tweede fase van het onderzoek in hoofdlijnen beschreven. De eerste fase was gericht op het verkrijgen van inzicht in de stand van zaken van internetdomeinbeheer binnen de overheid, het identificeren van knelpunten in beleid en praktijkuitvoering van internetdomeinbeheer, en het identificeren van de behoeften en belangen van verschillende overheidsorganisaties. Hierdoor is context gecreëerd. In de tweede fase is gezocht naar oplossingen voor de geconstateerde knelpunten, rekening houdend met de behoeften en belangen van overheidsorganisaties. Verschillende oplossingsrichtingen zijn eveneens besproken met gesprekspartners in de tweede fase. Hieronder zijn de bevindingen die voortkomen uit beide fases ondergebracht. Het eerste onderdeel (4.1.) geeft een beeld van de knelpunten in beleidsvoering en in de uitvoering van internetdomeinbeheer, waarna het tweede onderdeel (4.2) draagvlak voor de opgestelde oplossingen toont[9].

Belangrijk is om hierbij in ogenschouw te nemen dat we spreken van 'internetdomeinbeleid' in plaats van 'domeinnaambeleid'. Wanneer er gesproken wordt van 'domeinnaambeleid' verwijst dit naar het domeinnaambeleid van de Rijksoverheid (2011)[10]. De oplossingen in dit onderzoek dekken een bredere scope, waardoor we spreken van 'internetdomeinbeleid'. Met andere woorden, de oplossingen richten zich op toekomstig internetdomeinbeleid.

4.1. Probleemschets van de knelpunten in beleidsvoering en uitvoering van internetdomeinbeheer

De behoefte van overheidsorganisaties om de oplossingen in dit rapport in te richten komt voort uit geconstateerde knelpunten in beleidsvoering en uitvoering van internetdomeinbeheer. De uitkomsten van de eerste fase duiden op deze knelpunten. Er zit geen onderscheid tussen Rijksorganisaties en decentrale overheden in de erkenning van deze knelpunten – allen kampen met dezelfde problemen in internetdomeinbeheer. In de gesprekken is ingegaan op onderwerpen met betrekking tot de beleidsvoering en uitvoering van internetdomeinbeheer in de desbetreffende organisatie, en het perspectief van de organisatie op de knelpunten die zij ondervinden. Het onderstaande stuk beschrijft de uitkomsten van de gesprekken, aan de hand van een aantal hoofdlijnen. De rapportage van de eerste fase van het onderzoek overheidsbreed internetdomeinbeleid[11] gaat hier meer verdiepend op in en

[9] Voor een meer gedetailleerde uitwerking van de bevindingen, wordt verwezen naar de rapportage van de eerste fase, en de rapportage van de tweede fase van het onderzoek 'overheidsbreed internetdomeinbeleid' (Forum Standaardisatie, 2021; 2022). Deze zijn niet online te raadplegen, maar worden op verzoek intern gedeeld.

[10] Domeinnaambeleid, Rijksoverheid (2011). www.domeinnaambeleid.nl

[11] Rapportage fase een: onderzoek overheidsbreed internetdomeinbeleid, Forum Standaardisatie (2021). Niet online te raadplegen.

toont een meer gedetailleerde weergave van de gesprekken. Hieronder volgen zeven conclusies die voortkomen uit de gesprekken.

4.1.1. Er is onvoldoende centrale aansturing. Vanuit zowel de Rijksoverheid als vanuit decentrale overheden speelt er de behoefte aan een meer centrale aansturing door middel van overheidsbreed internetdomeinbeleid, mits het de ruimte biedt om de uitvoering ervan in te laten richten door de organisaties zelf.

Rijksoverheid

Rijksorganisaties nemen vaak het huidige domeinnaambeleid[12] als uitgangspunt voor internetdomeinbeheer. Echter ervaren zij dit als onvoldoende, omdat er naast het huidige domeinnaambeleid nog andere eisen en verplichtingen[13] zijn waaraan voldaan moet worden, die raakvlak hebben met het huidige domeinnaambeleid, zo stelt BZK. Om die reden worden er aanvullende afspraken of beleid gevoerd. Zo is BZK bezig met een project om huidig beleid aan te vullen met verplichte richtlijnen, integreert UWV het beleid in eigen URL-beleid, en houden VWS en RVO aanvullende opschoonacties. Kortom, het huidige domeinnaambeleid dekt niet de volledige lading van wat er komt kijken bij internetdomeinbeheer in de praktijk. Allen zijn van mening dat het op orde krijgen van internetdomeinen en het voldoen aan kwaliteitseisen van belang is om de veiligheid, betrouwbaarheid en herkenbaarheid van de overheid te vergroten. Daarom is er vanuit Rijksorganisaties behoefte aan een overkoepelend beleid gericht op internetdomeinbeheer, dat actueel is en gericht is op zowel domeinen als domeinnamen, achterliggende online middelen, en verplichte richtlijnen van dien. Idealiter wordt dit overheidsbreed ingericht. Decentrale overheden tonen wel initiatief in het beheren van internetdomeinen en kwaliteit, maar aansluiting met de Rijksoverheid ontbreekt vaak, aldus RVO. Het is hierbij wel van belang dat het beleid richtlijnen en kaders biedt voor de praktijk, maar de uitvoering ervan ingericht kan worden door de organisatie zelf. DPC benadrukt dat het van belang is dat het beleid niet voor belemmering zorgt voor organisaties die het nu op orde hebben, maar juist ondersteuning biedt. Het centraal beleggen van beheer zorgt mogelijk voor meer orde in naleving van het beleid.

Decentrale overheden

Decentrale overheden hanteren zelden beleid op het gebied van internetdomeinbeheer. Zij zijn hier zelf verantwoordelijk voor, omdat dit niet centraal wordt aangestuurd. Zowel Provincies als Waterschappen hanteren geen specifiek beleid, centrale afspraken of richtlijnen, zo stellen de Unie van Waterschappen en provincie Noord Holland. Gemeenten voeren ook zelden beleid op dit gebied. Gemeente Tilburg is een gemeente die zelf een beleid 'webtoepassingen' hanteert, wat internetdomeinbeheer dekt, maar er zijn nog weinig gemeenten die volgen, stellen gemeente Tilburg en Parkstad IT

[12] Domeinnaambeleid, Rijksoverheid (2011). www.domeinnaambeleid.nl

[13] Inhoudelijke informatie met betrekking tot de verplichte richtlijnen online middelen zijn te vinden op de pagina 'Handreiking Verplichte richtlijnen websites en andere online middelen', UBR (2019).

(registrar van een aantal gemeenten). Kortom, er zijn nauwelijks afspraken omtrent het beheren van internetdomeinen. Volgens decentrale overheidsorganisaties heeft dit oorzakelijk vaak betrekking tot een gebrek aan kennis, bewustzijn en capaciteit. Daarnaast is het vaak een gebrek aan prioriteit op de agenda. Decentrale overheidsorganisaties stellen om deze redenen dat centrale aansturing op dit gebied in de vorm van een overheidsbreed internetdomeinbeleid zou helpen. De voorwaarde is wel dat het niet voor belemmering zorgt, maar het ontzorgt en steun biedt. Organisaties hebben tevens de behoefte om het beleid te kunnen toepassen op eigen organisatiestructuur.

4.1.2. Gebrek aan herkenbaarheid is een groot knelpunt in de praktijk, voor zowel de Rijksoverheid als voor decentrale overheden.

Rijksoverheid

Het zijn van een veilige, herkenbare en eenduidige overheid is voor veel Rijksorganisaties een belangrijk doel. Echter is het voor zowel overheidsorganisaties als voor burgers niet inzichtelijk wat een overheidsdomein is, aldus het NCSC. Er bestaan veel websites die lijken op overheidswebsites, waar de burger het onderscheid niet kan maken. Nergens kan geverifieerd worden of het om een overheidswebsite gaat. Volgens het NCSC zou herkenbaarheid een meer verplicht karakter moeten krijgen, zodat overheidsorganisaties verplicht zijn om duidelijk te maken dat het een overheidswebsite is. Ook UWV stelt dat de herkenbaarheid van de overheid en herleidbaarheid naar de overheidsinstantie in domeinen belangrijk is. Momenteel is er nog geen publieke lijst voor overheidsdomeinen om dit te controleren. Echter begint dit bij beheersbaarheid van internetdomeinen. Bij veel organisaties is nog te weinig grip op overzicht van domeinen en hun registraties. Dit is nodig om kwaliteitsaspecten als herkenbaarheid, maar ook veiligheid en betrouwbaarheid aan te sturen. Het generiek maken van een internetdomeinbeleid voor de gehele overheid draagt vanuit maatschappelijk punt ook bij aan een eenduidige overheid voor de burger, stelt RVO.

Decentrale overheden

Ook voor decentrale overheden is onherkenbaarheid een doorn in het oog. Volgens gemeente Tilburg heeft dit mede te maken met generieke naamgeving, die niet overheid-specifiek is. Overheden hebben een hoop domeinen waarbij je niet kunt aflezen dat het van een overheidsorganisatie is. Hierdoor is een domein niet herleidbaar naar de overheid, en herkent de burger de afzender niet. Ook Parkstad IT stelt dat herkenbaarheid een kwaliteitsaspect is waar bij gemeenten veel te winnen valt. Nu beschikken weinig gemeenten over overzicht en inzicht in hun domeinnamen, en besteden zij geen aandacht aan achterliggende kwaliteitseisen. Echter is het van belang dat een website herkenbaar is als overheidswebsite, aldus Parkstad IT. Decentrale overheden zien veiligheid, eenduidigheid en herkenbaarheid als de belangrijkste doelen voor overheidsbreed internetdomeinbeleid.

4.1.3. Interne *governance* omtrent internetdomeinbeheer ontbreekt: Rolverdeling en verantwoordelijkheden zijn onduidelijk en versnipperd bij zowel de Rijksoverheid als bij decentrale overheden.

Rijksoverheid

Bij Rijksoverheidsorganisaties is er sprake van een versnipperde rol -en verantwoordelijkheidsverdeling op het gebied van internetdomeinbeheer. Tevens verschilt het per organisatie hoe verantwoordelijkheden en rollen belegd zijn. Echter beargumenteert het NCSC dat organisaties niet altijd hun verantwoordelijkheid nemen. VWS stelt dat het lastig is de verantwoordelijkheidsgrens te bepalen, omdat er geen richtlijnen voor zijn. Organisaties moeten zelf intern verantwoordelijkheden gaan invullen, terwijl deze niet formeel in beleid vastgelegd zijn. DPC stelt dat het goed zou zijn om op centraal niveau na te denken over de *governance* van internetdomeinbeheer. Volgens DPC is het grootste knelpunt dan ook de ontbrekende governance bij organisaties in de uitvoering van beheer, met daaraan gekoppeld de onvoldoende duidelijke rol van liaison (of portfoliobeheerder). BZK bevestigt dit, en stelt dat de liaison (of portfoliobeheerder) nu verantwoordelijk is voor meer taken dan wat in beleid is opgenomen, en deze op uiteenlopende manieren worden ingevuld, omdat deze niet geconcretiseerd zijn. Daarnaast is het voor DPC duidelijk wie liaisons (of portfoliobeheerders) zijn bij Rijksorganisaties, maar vaak weten de liaisons zelf niet wie centrale aanspreekpunten zijn bij andere organisaties. RVO bevestigt dit, en stelt dat het voor RVO onduidelijk is wie het centrale aanspreekpunt is op het gebied van internetdomeinbeheer bij andere organisaties. Een betere aansturing in governance zou volgens DPC bijdragen aan het signaleren, corrigeren en bijsturen van organisaties die zich aan het (internetdomein)beleid onttrekken. VWS sluit zich hierbij aan, en stelt dat door verantwoordelijkheid te verbinden aan rollen er uitleg gevraagd kan worden bij het niet voldoen aan de eisen. Ook stelt DPC dat wie er verantwoordelijk is voor internetdomeinbeheer verschilt per organisatie. Daarom is het goed om verantwoordelijkheden vast te leggen in beleid, maar de rolinrichting ervan over te laten aan de organisaties zelf. Wat noodzakelijk is, is dat organisaties duidelijk communiceren over hoe deze rolverdeling is belegd, en welke verantwoordelijkheden daaronder vallen. Volgens RVO is het intern nu lang niet altijd te achterhalen wie de eigenaar of beheerder is van een website/domeinnaam, omdat dit vaak volledig ontbreekt of niet meer up-to-date is. Verantwoordelijkheden moeten daarom eenduidig belegd worden, beargumenteren zowel RVO, UWV, BZK als VWS. BZK stelt dat de invulling van rol -en taakverdeling ontbreekt in huidig beleid, en dat door de onduidelijkheid omtrent deze invulling naleving niet goed gehandhaafd kan worden binnen organisaties. Zo kan een verantwoordelijkheid vastgesteld worden onder andere voor het uitvoeren van periodieke controles en het beheren van de levenscyclus van een internetdomein, stelt VWS. Rollen als (functioneel/technisch) beheerder, (web/domeinnaam)eigenaar, en registrar moeten daarom duidelijk belegd zijn bij overheidsorganisaties, stellen RVO, BZK en UWV. Een eindverantwoordelijke (bijvoorbeeld CISO) kan het beheer verder delegeren. Als in grote lijnen rollen en bijbehorende taken vastgelegd zijn in beleid, helpt dat met het toezicht houden en handhaven wanneer er niet wordt nageleefd. Volgens alle Rijksorganisaties die gesproken zijn is het daarom van belang om verantwoordelijkheden en rollen vast te

leggen en te bekrachtigen in beleid. Het op orde hebben van de governance is het meest belangrijk, anders is stimulering van goed internetdomeinbeheer nutteloos, stelt DPC.

Decentrale overheden

Ook decentrale overheden herkennen de versnipperde rolverdeling binnen organisaties. Daarnaast zijn verantwoordelijkheden vaak zowel intern als extern belegd, waardoor versnippering verergert, zo stelt de Unie van Waterschappen. SIDN beargumenteert dat doordat decentrale overheden vaak verantwoordelijkheden uit handen geven er meer wildgroei ontstaat en veel domeinen niet bekend zijn.

Daarnaast wordt herkend dat verantwoordelijkheden en rolverdeling op het gebied van internetdomeinbeheer vaak niet aangestuurd bij decentrale overheden, en deze dan ook niet intern zijn vastgelegd. Ook ontbreekt er een centraal aanspreekpunt, en is het eveneens onduidelijk of centrale aanspreekpunten ingericht zijn bij andere overheidsorganisaties. Volgens zowel gemeente Tilburg als de Unie van Waterschappen zou het aanstellen van centrale aanspreekpunten helpen om internetdomeinbeheer beter in te richten. Gemeente Tilburg stelt dat een gebrek aan kennis vaak de oorzaak is van het ontbreken van beleid en/of centrale afspraken.

4.1.4. Wildgroei blijft een doorn in het oog.

Rijksoverheid

Voor Rijksorgansaties blijft wildgroei een doorn in het oog, zo erkennen RVO, VWS en het NCSC. Oorzakelijk heeft dit te maken met een aantal zaken. Zo blijft wildgroei voortbestaan doordat afspraken niet worden nageleefd, stelt RVO. Daarnaast blijft het aantal registraties hoger dan het aantal uitfaseringen, wat wildgroei in de hand werkt, beargumenteert DPC. Ook is er wildgroei volgens het RVO door versnippering van registraties bij externe leveranciers, en is het vaak niet bekend bij wie en of domeinen in beheer zijn. De impact hiervan is dat veel overheidsorganisaties overzicht verliezen, waardoor domeinen buiten beheer vallen en uit het oog verloren raken. Als gevolg hiervan voldoen niet alle domeinen aan kwaliteitseisen, zo stellen het NCSC en het RVO. Volgens DPC is de consequentie hiervan dat er te veel potentiële probleemgevallen en/of kwetsbaarheden zijn. Tevens gaat dit ten koste van de herkenbaarheid van de overheid. Al met al brengt wildgroei complexiteit in beheer, onnodige kosten, en veiligheidsrisico’s met zich mee, beargumenteert DPC.

DPC zegt dat de impact van wildgroei duidelijk te zien is, maar het onvoldoende prioriteit krijgt. Ook het NCSC zegt dat huidig beleid niet genoeg inspeelt op het tegengaan van wildgroei. Overheidsorganisaties zetten wel opschoonacties in, maar volgens VWS is dit enkel een bestrijding van het probleem aan de voorkant, en niet aan de achterkant. Doordat de oorzaken van wildgroei niet worden aangepakt, komen domeinen er aan de achterkant weer bij en blijft het probleem voortbestaan. Volgens het UWV zou wildgroei gedeeltelijk aangepakt worden wanneer er sancties hangen aan het niet voldoen aan kwaliteitseisen. DPC stelt dat een herkenbare overheidsextensie wildgroei tot een halt kan brengen.

Decentrale overheden

Decentrale overheden ervaren wildgroei eveneens als een doorn in het oog. Volgens Parkstad IT en gemeente Tilburg hebben gemeenten weinig zicht hierop. Vaak worden domeinen geregistreerd, waarna niemand er zicht meer op heeft, stelt Parkstad IT. Eveneens worden verantwoordelijkheden met betrekking tot internetdomeinen vaak uit handen gegeven, waardoor er meer wildgroei ontstaat en veel domeinen niet bekend zijn, zegt SIDN. Parkstad IT benoemt dat het aanstellen van centrale aanspreekpunten op het gebied van internetdomeinbeheer wildgroei zou beperken. Volgens gemeente Tilburg moet beleid handvatten bieden om wildgroei te beperken.

4.1.5. Er is een gebrek aan overzicht en inzicht in internetdomeinen, waardoor de achterliggende kwaliteitsaspecten niet voldoende worden aangestuurd.

Rijksoverheid

Er is een gebrek aan (centraal) overzicht van overheidsdomeinen, en onvoldoende inzicht in de kwaliteit van internetdomeinen. Bij veel organisaties is nog te weinig grip op overzicht van domeinen en hun registraties. Dit is nodig om kwaliteitsaspecten aan te sturen, stelt het NCSC. Ook volgens SIDN beschikken overheidsorganisaties nu over niet genoeg inzicht in hun domeinen. Eveneens beargumenteert AZ dat er weinig overzicht en inzicht is in overheidsdomeinen, en dat het verschil in volwassenheidsniveau groot is tussen overheidsorganisaties. Een van de grootste knelpunten is dat iedereen domeinnamen kan registreren, en dat dit vaak buiten de regel om gebeurt bij een externe leverancier in plaats van bij DPC. Intern loopt de registratie ook niet via de lijn, waardoor overzicht verloren raakt, beargumenteert het NCSC. Volgens UWV is het naast het hebben van overzicht ook het *behouden* van overzicht een groot knelpunt. Sommige (web/domeinnaam)eigenaren hebben na verloop van tijd niet meer in beeld welke domeinnamen zij in hun bezit of beheer hebben. RVO erkent het behouden van overzicht als een groot knelpunt. Zo stelt RVO dat een website vaak niet bekend is bij RVO, waardoor overzicht verloren raakt. Mede door wildgroei is overzicht behouden een groot knelpunt volgens RVO. Het gevolg is dat een domein buiten beheer valt en dan niet voldoet aan alle kwaliteitseisen. Ook volgens het NCSC is de impact van het ontbreken van overzicht dat er ‘vergeten’ domeinen ontstaan die niet voldoen aan verplichte standaarden. VWS stelt dat door een niet actueel, gebrekkig of niet volledig internetdomeinbeleid een gebrek aan overzicht en inzicht in internetdomeinen blijft voortbestaan, waardoor kwaliteit niet wordt aangestuurd. Het NCSC beargumenteert dat het domeinportfolio van overheidsorganisaties beperkt moet blijven, met zo min mogelijk domeinen. Toekomstig beleid moet daarom de focus leggen op bewustwording en inzicht. Daarnaast moet er meer druk uitgeoefend worden op organisaties om te voldoen aan de verplichte standaarden en kwaliteitseisen, stelt het NCSC. Volgens RVO stuurt huidig beleid niet voldoende aan op het voldoen aan de kwaliteit van internetdomeinen.

Decentrale overheden

SIDN stelt dat overheidsorganisaties nu niet over genoeg inzicht in hun domeinen beschikken. Decentrale overheden erkennen dat probleem. Volgens Parkstad IT hebben gemeenten niet inzichtelijk hoeveel en welke domeinen zij in hun bezit hebben. Weinig

gemeenten beschikken over overzicht en inzicht in hun internetdomeinen, en besteden weinig aandacht aan kwaliteitseisen. Achterliggende probleem is dat er geen centrale afspraken of beleid is om dat aan te sturen, stelt Parkstad IT. Ook Waterschappen hebben niet inzichtelijk hoeveel en welke domeinen zij in hun bezit hebben, dit is vaak niet concreet. Dit heeft mede te maken met het uitbesteden van verplichtingen rondom kwaliteitseisen aan externe leveranciers, benoemt de Unie van Waterschappen. Provincie Noord Holland erkent dit probleem en stelt dat er geen duidelijk beeld is van de mate waarin domeinen die uitbesteed zijn aan externe leveranciers voldoen aan kwaliteitseisen. Volgens de Unie van Waterschappen moet er meer prioriteit komen te liggen op het aansturen van kwaliteitsaspecten.

4.1.6. Gebrek aan praktijkaansturing van beheerprocessen zorgt voor onvoldoende beheersbaarheid van de levenscyclus van het internetdomeinportfolio.

Rijksoverheid

Momenteel wordt de praktijk onvoldoende aangestuurd, waardoor beheerprocessen uiteenlopen en de levenscyclus van het internetdomeinportfolio onvoldoende wordt beheerst. Volgens VWS en DPC is grip krijgen op de levenscyclus van internetdomeinen echter cruciaal om wildgroei tegen te gaan. Het NCSC stelt dat er momenteel geen duidelijke processen zijn omtrent het beheren van de levenscyclus van domeinen. Onduidelijke afspraken over het beheren van de levenscyclus van een domein brengen ook risico’s met zich mee, stelt RVO, zoals bij het vroegtijdig vrijgeven van een domein. Ook is de mate van verplichting is onvoldoende volgens BZK, waardoor processen in de praktijk anders lopen dan volgens beleid zou moeten. Richtlijnen bij registratie van nieuwe domeinen worden momenteel niet strikt nageleefd, waardoor er websites buiten deze richtlijnen worden opgericht, stelt BZK. Het NCSC en VWS sluiten zich hierbij aan, en stellen dat het van belang is dat benadrukt wordt dat er enkel bij de (centrale) registrar wordt geregistreerd, wat momenteel niet altijd volgens de afspraken gebeurt.

Volgens RVO is het goed om richtlijnen voor levenscyclusbeheer in te richten om internetdomeinbeheer beter aan te sturen. Ook DPC stelt dat criteria wenselijk zijn, maar meer in de vorm van sturende richtlijnen. AZ stelt dat criteria voor het registreren van een nieuw domein moet opgenomen worden in internetdomeinbeleid. Zo het kritisch kijken naar het doel van website vóór registratie, en doel vastleggen bij registratie onderdeel moeten zijn van het registratieproces, stellen RVO en DPC.

Volgens het NCSC zou verplichting relevant zijn voor het uitfaseren van domeinen, en herkenbaarheid zou een meer verplicht karakter moeten krijgen, zodat overheidsorganisaties verplicht zijn om duidelijk te maken dat het een overheidswebsite is, aldus het NCSC. Ook DPC stelt dat het belangrijk is dat een domein offline wordt gehaald bij end-of-life. Tevens stelt UWV dat het offline halen op basis van criteria (wanneer een website niet voldoet aan de eisen) een deel van de wildgroei oplost.

BZK beargumenteert dat de visie voor toekomstig beleid is dat het naar een hoger volwassenheidsniveau moet worden gebracht door praktijkprocessen aan te sturen,

richtlijnen, kaders of randvoorwaarden op te stellen voor de uitvoering, en beheer duurzaam in te richten.

Decentrale overheden

Parkstad IT stelt dat het relevant is om criteria voor het beheren van de levenscyclus van een internetdomein op te nemen. Momenteel zijn er geen afspraken, en dus ook niets om op te handhaven, omdat naleving de eigen verantwoordelijkheid is. Volgens Parkstad IT zijn er momenteel echter niet voldoende handvatten om in de praktijk naar te handelen. Daarom is het belangrijk om randvoorwaarden of criteria op te nemen om beheer beter te reguleren.

Gemeente Tilburg hanteert een eigen beleid 'webtoepassingen' waarin afspraken omtrent levenscyclusbeheer zijn opgenomen. Gemeente Tilburg zou deze afspraken ook graag terugzien in overheidsbreed internetdomeinbeleid. Een voorbeeld hiervan is het offline halen van een domein wanneer deze niet voldoende voldoet aan veiligheidseisen. Waar gemeente Tilburg eveneens tegenaan loopt is dat er geen afspraken zijn omtrent naamgeving van een domeinnaam. Vaak worden generieke domeinnamen geregistreerd, die geen specifieke herkenbaarheid vertonen. Dit heeft een negatief effect op de herkenbaarheid.

Provincie Noord Holland stelt dat er geen centrale afspraken of richtlijnen zijn omtrent het beheren van de levenscyclus van internetdomeinen. Hierdoor worden uit het gezichtsveld te makkelijk domeinnamen geregistreerd, is er geen eenduidigheid in naamgeving, en blijven domeinnamen na langdurige inactiviteit nog voortbestaan.

Praktijkuitvoering is niet eenduidig, stelt de Unie van Waterschappen. Dit is individueel geregeld, en er is geen duidelijke lijn in het gebruik van internetdomeinen. Volgens de Unie van Waterschappen is verplichting nodig om er in de praktijk naar te gaan handelen. Pas als er sprake is van wetgeving ontstaat er urgentie en wordt erin geïnvesteerd.

Volgens SIDN mist beleid criteria voor het offline halen van een domein. Wat betreft registraties zou er ook een lichte vorm van een registratieproces opgenomen moeten worden als instapproces, stelt SIDN. Ook zijn criteria voor herkenbaarheid belangrijk.

4.1.7. Toezicht, monitoring en handhaving ontbreekt

Rijksoverheid

Verplichte richtlijnen worden niet voldoende nageleefd, en uitvoering en handhaving is momenteel onvoldoende, stelt DPC. Ook op huidig domeinnaambeleid[14] is geen toezicht en handhaving, en consequenties ontbreken bij het niet naleven ervan. Dat is een gebrek volgens DPC. Bij het niet voldoen aan kwaliteitseisen, zijn sancties belangrijk. Vaak wordt het pas op orde gebracht wanneer er een consequentie aan vastzit. Als er iets in wetgeving wordt opgenomen, wordt het een stuk beter nageleefd

[14] Domeinnaambeleid, Rijksoverheid (2011). Geraadpleegd via www.domeinnaambeleid.nl.

omdat er consequenties meespelen. Beter handhaven is mogelijk door het gebruik van positieve en/of negatieve stimuleringen en/of consequenties.

Door mogelijkheden om af te wijken van richtlijnen worden beleidsrichtlijnen dus niet altijd nageleefd in de uitvoering. Er wordt niet vanzelfsprekend aan verplichtingen voldaan, stelt BZK. Daarvoor is controle en handhaving op naleving noodzakelijk. Enige vorm van handhaving ontbreekt in huidig beleid, er zijn geen consequenties wanneer afspraken niet worden nageleefd. Toezicht op veiligheid is iets wat men zou terugverwachten in het beleid, stelt BZK.

Er is nu weinig toezicht, stelt RVO. Als in grote lijnen rollen en bijbehorende taken vastgelegd zijn in beleid, helpt dat met het toezicht houden en handhaven wanneer er niet voldoende wordt nageleefd. Een verbeterde toezicht en handhaving is noodzakelijk. Momenteel zijn er geen consequenties als je niet voldoet. Winst kan behaald worden door een (Rijks)overheidsrol in te richten die naleving controleert en aanstuurt op betere (interne) handhaving. Vooral naleving en handhaving verdienen aandacht, aangezien er weinig instanties zijn die volledig voldoen aan de verplichte eisen.

Het huidige domeinnaambeleid[15] wordt niet vaak nageleefd, volgens het NCSC. Het voelt niet verplicht aan omdat er geen consequenties aan verbonden zijn wanneer er niet wordt nageleefd. In de praktijk is er dan ook weinig naleving van en handhaving op het beleid. Volgens het NCSC moet er op hoger managementniveau meer aandacht zijn voor toezicht en handhaving op internetdomeinbeheer.

Niet elke verplichting wordt momenteel nageleefd, stelt VWS. Er zouden strengere eisen moeten zijn aan het registreren bij een externe leverancier, mede omdat leveranciers niet altijd met moderne technieken meegaan waardoor niet alles wordt nageleefd. Ook moet er een mandaat zijn om websites uit de lucht te halen om veiligheid te waarborgen.

Ook AZ bevestigt dat er geen sprake is van toezicht en handhaving op het gebied van internetdomeinbeheer. Eveneens wordt er minimaal toegezien op de kwaliteit van internetdomeinen. Grenzen stellen, duidelijkheid bieden en daarop controleren is daarom cruciaal.

Decentrale overheden

Gemeente Tilburg stelt dat het beleid een minder adviserend, en méér verplichtend karakter mag hebben. Dit betekent dat er consequenties zijn bij het niet voldoen aan de eisen, zodat er beter gehandhaafd kan worden en de naleving ervan verbetert. Momenteel ontbreekt handhaving en worden afspraken niet voldoende nageleefd.

De Unie van Waterschappen zegt dat het in de praktijk vaak anders loopt dan op papier zou moeten staan. Doordat er geen concreet beleid is, is er geen toezicht op naleving van regels. Lang niet alle domeinen worden actief gemonitord, eveneens is dat zo op toepassing van verplichte richtlijnen. Internetdomeinbeheer zou ingebed

[15] Domeinnaambeleid, Rijksoverheid (2011). Geraadpleegd via www.domeinnaambeleid.nl.

moeten zijn zoals de BIO, door overheidsorganisaties het individueel te laten implementeren door verplichting, en dan centraal erop te monitoren.

Ook provincie Noord Holland stelt dat er niet wordt toegezien of gehandhaafd op internetdomeinbeheer. Dit is een individuele verantwoordelijkheid per provincie. Richtlijnen en randvoorwaarden zijn nodig om uniformiteit te creëren en toezicht en handhaving te bewerkstelligen. Nu zit er te veel verschil in uitvoering, en wordt er niet toegezien op naleving.

Parkstad IT beargumenteert ook dat er momenteel geen afspraken zijn, en dus ook niets om op te handhaven omdat naleving eveneens de eigen verantwoordelijkheid is van gemeenten.

4.2. Draagvlak voor adviezen

Overheidsorganisaties erkennen de behoefte voor de beschreven oplossingen. Dit blijkt uit de tweede fase van het onderzoek. In de tweede fase van het onderzoek zijn oplossingen verkend en vastgesteld. De vastgestelde oplossingen sluiten aan op geïdentificeerde knelpunten in de beleidsvoering en uitvoering van internetdomeinbeheer, die geconstateerd zijn in de eerste fase. In gesprekken met Rijksoverheidsorganisaties en decentrale overheden is onderzocht of deze opties een mogelijke uitkomst bieden voor de huidige knelpunten. De organisaties die onderdeel zijn van deze gesprekken zijn het CIP, CIO-Rijk (BZK), NCSC, DPC, Logius, het Waterschapshuis, Gemeente Tilburg, en Provincie Overijssel. De gesprekken zijn gevoerd met experts die betrokken zijn bij internetdomeinbeheer in de hierboven genoemde organisaties. Uitgaande van de standpunten en ervaringen van deze personen valt dit niet te generaliseren naar het perspectief van de gehele organisatie, maar is het oordeel gebaseerd op de geraadpleegde expertise.

Dit onderdeel beschrijft de perspectieven van de hierboven genoemde organisaties op (de prioritering van) de oplossingen en geeft per oplossing een korte samenvatting weer.

Algehele oordeel en prioriteiten

Ondanks dat niet iedere organisatie voor iedere oplossing een standpunt gedeeld heeft, beschouwen alle betrokken organisaties de hierboven opgestelde oplossingen als relevant en was er bij geen een organisatie de voorkeur om bepaalde oplossingen niet op te nemen in het advies. Om meer selectief in te zijn is er in de gesprekken gevraagd naar de prioritering van de oplossingen. In de prioritering komt duidelijk naar voren dat register internetdomeinnamen overheid (RIO) (2), een generieke overheidsextensie (3) en het aanstellen van een centrale overheidsregistrar (4) het meest de voorkeur krijgt. Volgens de meeste organisaties maken we een grote slag als we deze oplossingen realiseren. De andere oplossingen worden ongeveer op gelijke voet gezet wat betreft prioritering. Al met al zijn alle oplossingen relevant, maar zit er een verschil in noodzakelijkheid en dekkingskracht met betrekking tot de geconstateerde knelpunten. Het implementeren van RIO, een generieke overheidsextensie, en een centrale overheidsregistrar lijken een oplossing te bieden voor meerdere problemen,

waardoor andere opties bij het doorvoeren hiervan overbodig kunnen zijn. Deze oplossingen bieden daarom een hogere dekkingskracht en voor de geconstateerde knelpunten. Desondanks is benadrukt dat alle oplossingen relevant zijn om door te voeren, en het combineren ervan leidt tot een sterke vooruitgang in internetdomeinbeheer en bijbehorende kwaliteitsaspecten.

4.2.1. Register Internetdomeinnamen Overheid (RIO).

Rijksoverheid

Volgens Rijksorgansaties draagt inventariseren van domeinnamen bij aan de herkenbaarheid van de overheid. CIO-Rijk stelt dat RIO een stap in de goede richting is om overzicht en inzicht te verkrijgen in overheidsdomeinen, en daarmee het vergroten van de herkenbaarheid. Logius deelt dit standpunt, maar stelt dat het maken van duidelijke afspraken hiervoor cruciaal is. Zo stelt Logius dat het een vereiste moet zijn dat websites alleen als overheidswebsites geclassificeerd worden wanneer de in het register internetdomeinnamen overheid (RIO) opgenomen zijn. Ondanks de mogelijkheid tot verifiëren van overheidswebsites, spreekt het NCSC de twijfel uit dat burgers mogelijk niet snel een domeinnaam controleren in een register. Desondanks kan het register volgens het NCSC een belangrijke bijdrage leveren aan de transparantie van de overheid en aan onderzoeksdoeleinden en kwaliteitscontroles. Daarnaast beschouwt het CIP het hebben van een overheidsregister als een belangrijke optie, omdat van geïnventariseerde domeinnamen een .gov.nl/.overheid.nl variant vastgelegd kan worden. Zo vergemakkelijkt het de transitie naar een generieke overheidsextensie omdat overheidswebsites al geïnventariseerd zijn. Met andere woorden is nuttig om deze oplossing in combinatie met een generieke overheidsextensie (3) in te richten.

Decentrale overheden

Provincie Overijssel stelt dat RIO een ideale optie is om de herkenbaarheid van de overheid te verbeteren. Ook delen zij het standpunt van CIO-Rijk dat het voor overzicht en inzicht in overheidsdomeinen zal zorgen, en dat dat cruciaal is voor de herkenbaarheid van de overheid. Ook het Waterschapshuis stelt dat een overheidsregister een goede oplossing biedt, omdat het de mogelijkheid geeft om te controleren welke websites van de overheid zijn.

4.2.2. Generieke overheidsextensie (.gov.nl/.overheid.nl)

Rijksoverheid

Het CIP, NCSC, DPC, en CIO-Rijk beschouwen een generieke overheidsextensie als een belangrijke oplossing. Volgens het CIP is een generieke overheidsextensie de ideale oplossing, ondanks dat hier veel werk aan vast zit. Het CIP, CIO-Rijk, en het NCSC beargumenteren allen dat een generieke overheidsextensie cruciaal is voor het bestrijden van het herkenbaarheidsprobleem, wat zij als een centraal probleem beschouwen. Echter draagt het pas écht bij als het voor de gehele overheid geldt, geeft het CIP aan. Wat dus belangrijk is, is dat iedereen hierin meegaat. Zolang het vrijblijvend blijft of voor een deel geïmplementeerd wordt, heeft het niet veel zeggingskracht. Als het gaat om de herkenbaarheid, is het belangrijk het als een big-bang te implementeren. Wanneer er klein gestart wordt, heeft de burger er niet veel

aan voor de algehele herkenbaarheid van de overheid, beargumenteert het CIP. Dan blijven er teveel domeinnamen over die niet meegaan, maar wel van de overheid zijn. Om die reden is het volgens het CIP en Logius van belang dat er gedefinieerd is wat onder een overheidsorganisatie valt. Volgens het CIP moeten hier ook agentschappen en ZBO's onder vallen. Echter is het de vraag of bijvoorbeeld campagnewebsites daar ook onder moeten vallen. Het is dus belangrijk dit duidelijk te definiëren.

Meerdere organisaties zien in dat het een lange adem betreft. Echter, door met doorverwijzingen te werken, kun je een transitieproces in werking zetten en de transitie over een behoorlijke tijd uitstrekken, stelt het CIP. Alle organisaties hebben dan een eenduidige extensie waar de bezoeker naartoe kan, die doorverwijst naar de websites die de organisatie in bezit heeft. De extensie biedt dan een transitieperiode waarin de organisatie op eigen tempo de overgang kan maken. Volgens het CIP is het hierbij mogelijk om rekening te houden met de wil en het tempo van verschillende overheidsorganisaties.

DPC ziet de generieke overheidsextensie als een mooi streven, maar trekt in twijfel of alle decentrale overheidsorganisaties hierin meegaan. Dan zou een verplichting nodig zijn.

Decentrale overheden

Provincie Overijssel en het Waterschapshuis stellen dat het implementeren van een generieke overheidsextensie een belangrijke oplossing is. Volgens het Waterschapshuis en provincie Overijssel is een generieke overheidsextensie cruciaal voor de herkenbaarheid van de overheid. Zo stelt provincie Overijssel dat het bezoekers van overheidswebsites veel zal helpen, omdat duidelijk is dat ze met een overheidsorganisatie te maken hebben. Het Waterschapshuis is van mening dat een transitieproces de overgang zal vergemakkelijken. Dit geeft organisaties de ruimte om over te stappen. Deze transitieperiode is volgens het Waterschapshuis erg belangrijk.

Gemeente Tilburg ziet een generieke overheidsextensie als een goede oplossing, maar betwijfelt of decentrale overheidsorganisaties hier zonder verplichting in meegaan. Dan is verplichting vanuit de Rijksoverheid nodig. Zij stellen dat gemeenten vanuit communicatief oogpunt vaak zelfstandig herkenbaar willen blijven, al zou het wel als een redirect ingesteld kunnen worden. Anderzijds stelt het Waterschapshuis dat, ondanks dat zij voor de generieke overheidsextensie pleiten en het idee van het transitieproces met doorverwijzingen opperen, het verleiden juist wél beter zal werken dan verplichten wanneer het Rijk hierin het voorbeeld toont. Ook provincie Overijssel geeft aan dat organisaties wel mee moeten als het samen gedaan moet worden, omdat het dan urgentie kweekt.

4.2.3. Centrale overheidsregistrar

Rijksoverheid

Het CIP, NCSC en Logius zien een centrale overheidsregistrar als een erg relevante oplossing. Het NCSC stelt dat het inrichten van een centrale overheidsregistrar gestimuleerd moet worden, zodat registraties op één plek gebeuren en er minder 'verweesde' domeinnamen ontstaan. Ook Logius is voorstander om dit soort

dienstverlening te centraliseren. Tevens biedt het meer overzicht en inzicht in de domeinnamen binnen de overheid. Volgens het NCSC is het één van de meest essentiële oplossingen om het probleem van wildgroei aan te pakken.

Toezicht moet ingeregeld worden en onder het takenpakket vallen van de centrale overheidsregistrar. Op dit moment zijn toezichthoudende taken nergens formeel vastgelegd. Dat zou gemandateerd moeten worden. Een centrale overheidsregistrar bevordert door het hebben van overzicht ook het zelfstandig uitvoeren van (intern) toezicht, omdat dat overzicht gebruikt kan worden om (periodieke) controles uit te voeren. Punt 8 (verplicht periodieke controlechecks) en punt 9 (toezicht en handhaving) kunnen dus bij het inrichten van een centrale overheidsregistrar ingeregeld worden. Ook punt 7 (leverancierseisen) is deels inherent aan een centrale overheidsregistrar, volgens CIO-Rijk (BZK).
Verschillende organisaties zoals het NCSC en Logius zijn het er over eens dat hier capaciteit hiervoor beschikbaar stellen noodzakelijk is. CIO-Rijk stelt dat het aanwijzen van een centrale overheidsregistrar pas écht een oplossing vormt als het niet meer mogelijk is om buiten de centrale overheidsregistrar te registreren.

DPC is iets terughoudender in het inzetten van een centrale overheidsregistrar. Zo geven zij aan dat het voor decentrale overheden geen belemmeringen moet opwerpen. Het moet decentrale overheden ontzorgen. Daarnaast beargumenteert DPC dat het in de huidige situatie al niet vlekkeloos gaat – met name door het aantal registraties dat buiten DPC geregistreerd wordt. Ondanks dat sluit DPC zich aan bij het NCSC in het argument dat wellicht de wildgroei stopt als de meerwaarde van een centrale overheidsregistrar wordt ervaren.

Decentrale overheden

Het Waterschapshuis en Gemeente Tilburg beschouwen het inzetten van een centrale overheidsregistrar als erg relevant. Zo stelt gemeente Tilburg dat het een aantal problemen in de periferie oplost, en het wildgroei beperkt.

4.2.4. Centrale afspraken omtrent levenscyclusbeheer

Rijksoverheid

Logius geeft aan dat het cruciaal is dat een CIO of CISO het krijgt om een domein offline te halen wanneer deze niet voldoet aan beveiligingsstandaarden. Daarnaast stelt het CIP dat het van belang is een domeinnaam direct offline te halen wanneer het zijn doel niet meer dient, zoals bij het stoppen van een campagne. Ook moet er voorkomen worden dat een domeinnaam (té snel) vrijgegeven wordt, omdat het directe overname door een andere partij mogelijk maakt. Dit gaat ten koste van het vertrouwen van de burger in de overheid, omdat de burger mogelijk nog denkt te maken te hebben met de overheid. Het eigenaarschap moet dan bij de overheid blijven liggen. Een centrale organisatie-eenheid houdt de domeinnaam in bezit, als een soort ‘domeinnamendepot’. Dit kan de centrale overheidsregistrar zijn. Volgens het NCSC moeten er echter afspraken gemaakt worden over dit termijn, zodat er niet te veel losse domeinen geregistreerd blijven, die weinig kans op misbruik hebben en niet gebruikt worden. DPC stelt dat wanneer er e-mailcommunicatie op het domein plaatsvond, het hoe dan ook onwenselijk is om een domeinnaam vrij te geven. Voorkomen dat er vanuit een

‘ogenschijnlijk overheidsdomein’ gemaild wordt naar de burger, is belangrijk voor de herkenbaarheid van de overheid en het vertrouwen van de burger in de overheid.

Het NCSC benadrukt dat het afspraken moeten zijn met een meer verplichtend dan vrijblijvend karakter, om te voorkomen dat ze niet nageleefd worden. Wanneer een partij structureel niet voldoet mogen er consequenties aanzitten. Volgens het NCSC blijft de vraag wie er toeziet gaat houden op naleving van afspraken echter lastig te beantwoorden.

Decentrale overheden

Provincie Overijssel geeft aan het prettig te vinden als er centrale afspraken zijn omtrent levenscyclusbeheer. Zij stellen dat veel overheidsorganisaties wel beter beheer willen inrichten, maar niet altijd weten hoe zij dat moeten aanpakken. Het maken van centrale afspraken helpt daarbij. Ook heb je dan een manier om het beleid af te dwingen. Afspraken over naamgevingsconventie zijn gewenst, stelt provincie Overijssel. Dit komt de herkenbaarheid ten goede.

Het Waterschapshuis stelt dat het proces rondom levenscyclusbeheer van een domeinnaam vastgelegd moet zijn binnen een organisatie, zodat erop geaudit kan worden. Een organisatie moet kunnen aantonen dat de procedures rondom levenscyclusbeheer (registratieproces, verhuizen, uitfaseren/offline halen en vrijgeven) goed ingericht zijn. De manier waarop daar richting aan wordt gegeven hoeft niet vastgelegd te zijn, beargumenteert het Waterschapshuis, maar het moet wel ingeregeld zijn. Vervolgens kun je hierop toezien door controlepunten in te bouwen. Tevens stelt het Waterschapshuis dat het ook goed zou zijn om bepaalde (technische) basiseisen te stellen voor het verkrijgen van een domein.

4.2.5. Beleggen van rollen en verantwoordelijkheden

Rijksoverheid

Aansluitend bij de conclusies uit de eerste fase benadrukken Logius en het NCSC dat er een gebrek is aan het beleggen van verantwoordelijkheden en rolverdeling. Volgens Logius zou het helpen om een rol te beschrijven met bijbehorende verantwoordelijkheden, en deze rol toekennen aan een functie binnen een organisatie. Dat moet vervolgens vastgelegd en gecommuniceerd worden. CIO-Rijk sluit zich hierbij aan en stelt dat een organisatie dit intern moet inrichten op basis van gestelde richtlijnen binnen een stelsel of rijkskader van de Rijksoverheid. Vanuit daar moet geadviseerd worden over rolverdeling, waarbij verantwoordelijkheden moeten zijn belegd en rollen open blijven ter invulling van de organisatie. Ook het NCSC is van mening dat het van belang is internetdomeinbeheer en de bijbehorende verantwoordelijkheden te beleggen binnen een organisatie. Belangrijk volgens het NCSC is dat er passende rollen worden toebedeeld, met bijbehorende verantwoordelijkheden. Een van de belangrijkste verantwoordelijkheden is dat er daadwerkelijk geregistreerd wordt bij DPC, of de centrale overheidsregistrar. Wel moeten deze verantwoordelijkheden goed uitgeschreven worden, zonder deze te koppelen aan standaard rollen. Daarover kan geadviseerd worden, maar moet niet verplichtend zijn. Zolang ze maar verdeeld worden binnen de organisatie. Het NCSC

stelt dat het hierbij belangrijk is oog te houden voor het bundelen van verantwoordelijkheden, om te voorkomen dat het nog verder versnippert.

Daarnaast is eigenaarschap belangrijk. Niet alleen internetdomeinen, maar ook het internetdomeinbeleid zelf moet een duidelijke eigenaar hebben, benadrukt Logius. Momenteel doen organisaties individueel hun best om er zelf richting aan te geven, maar daardoor ontstaat er geen één digitale overheid. Een eigenaar van het internetdomeinbeleid kan aansturen op eenduidigheid. Daarnaast moeten er kaders gesteld worden, en binnen de kaders moet hulp aangeboden worden om beheer zelfstandig in te richten, stelt Logius.

Decentrale overheden

Gemeente Tilburg en provincie Overijssel stellen, net als Rijksoverheidsorganisaties, dat rollen en verantwoordelijkheden niet duidelijk belegd zijn. Het is onduidelijk wie er aanspreekpunten zijn op het gebied van internetdomeinbeheer. Provincie Overijssel stelt dat het enorm zou helpen als verantwoordelijkheden duidelijk belegd zijn en geeft hier de prioriteit aan. Ook delen zij de behoefte dat er kaders gesteld worden vanuit de Rijksoverheid, waarin de Rijksoverheid binnen die kaders decentrale overheidsorganisaties kan ondersteunen in het zelfstandig inrichtingen van beheer. Zij stellen dat procesmatige richtlijnen, randvoorwaarden en kaders nodig zijn voor de processen in de praktijk.

4.2.6. Leverancierseisen bij het uitbesteden van registratie/beheer bij een externe leverancier

Rijksoverheid

CIO-Rijk benoemt het belang van basiseisen voor externe leveranciers en noemt dit een belangrijk punt. Externe leveranciers moeten aan de eisen voldoen die de Rijksoverheid stelt. Het NCSC benadrukt dat het wederom bij alle verplichtingen belangrijk is om toe te zien op naleving.

Decentrale overheden

Het Waterschapshuis beargumenteert dat het probleem is dat contracten met leveranciers voor een langere periode worden vastgelegd, terwijl sommige standaardeisen in het contract na verloop van tijd achterhaald zijn. Provincie Overijssel deelt deze mening, en stelt dat het zelfs vaak de vraag is of je een contract van een langere periode geleden kunt terugvinden, omdat het intern zo versnipperd is. Tevens kiest men vaak voor een partij die al bekend is bij de overheid, zonder bij aanbesteding de standaardeisen te controleren, stelt het Waterschapshuis. Provincie Overijssel beargumenteert dat ze wel eisen voor leveranciers stellen, maar dat ze dan wel zeker weten dat Overijssel met die leverancier in zee gaat. Desondanks is het bij voorbaat afstellen van leverancierseisen goed. Het zou goed zijn om op deze manier het aantal leveranciers terug te dringen om ook daar versnippering tegen te gaan en wildgroei te beperken.

Gemeente Tilburg legt eveneens uit dat het belangrijk is om basiseisen te stellen, zodat bij contractuele afstemming de leverancier aan vastgestelde eisen voldoet. Volgens Gemeente Tilburg moeten er minimale eisen gesteld worden aan diensten van

dienstverleners, zodat er toezicht ontstaat op de kwaliteit van generieke diensten. Ze beargumenteren dat het van belang is dat leveranciers die diensten aan veel gemeenten leveren ook moeten voldoen aan de eisen die de Rijksoverheid stelt. Het Waterschapshuis sluit zich bij gemeente Tilburg en provincie Overijssel aan en stelt eveneens dat leverancierseisen wenselijk zijn. Volgens het Waterschapshuis moeten leveranciers voldoen aan een bepaald basisniveau. Er zijn veel websites bij kleinere leveranciers. De volwassenheid ervan groeit met het instellen van basiseisen. Echter is het afdwingen hiervan lastig als er geen handhaving op is.

4.2.7. Intern verplicht periodieke kwaliteitscontroles

Rijksoverheid

CIO-Rijk constateert dat controle op toepassing van open standaarden en andere verplichte richtlijnen nu onvoldoende is. Volgens CIO-Rijk moet dit intern bij organisaties een plek krijgen. Echter moet het dan wel helder zijn waar dat belegd is en moet de verantwoordelijkheid die het departement zelf heeft om dat intern in te richten duidelijk zijn. Daarnaast moet duidelijk zijn waar toezicht op het uitvoeren van controlechecks belegd is.

Decentrale overheden

Volgens gemeente Tilburg is het instellen van verplichte periodieke controlechecks een belangrijk punt. Zij stellen dat dit zowel intern als extern ingericht kan worden. Echter ligt de voorkeur van gemeente Tilburg bij het inzetten van één overheidsorganisatie die periodieke controlechecks uitvoert en daarmee overheidsorganisaties op de hoogte houdt met de stand van zaken. Provincie Overijssel geeft eveneens de voorkeur aan het centraal inregelen van periodieke controlechecks. Zij stellen er veel baat bij te hebben wanneer er vanuit het Rijk wat is opgelegd, omdat er dan het meeste waarde aan wordt gehecht.

4.2.8. Vormgeving van toezicht, monitoring en handhaving

Rijksoverheid

Volgens het NCSC moet je toezicht beleggen bij één organisatie. Idealiter is dit DPC, of een organisatie die dit in samenwerking met DPC uitvoert. Het NCSC stelt dat toezicht hoogstwaarschijnlijk niet voldoende prioriteit krijgt als het belegd is bij een organisatie zelf, met als resultaat dat je eindigt met de huidige situatie. Als het op die manier ingericht wordt, is het beleid er wel maar de capaciteit vaak niet. Een externe organisatie die bevindingen teruglegt kan meer druk uitoefenen om verbetering te realiseren. Tevens kost het veel meer capaciteit om alle overheidsorganisaties controle zelf te laten uitvoeren, dan wanneer dit belegd is bij één organisatie.

Het CIP sluit zich erbij aan, en geeft aan dat je explicieter moet maken dat je toezicht en handhaving wil organiseren op kwaliteitseisen voor online middelen. Ook pleit het CIP voor het centraliseren hiervan en stelt dat als je een centrale overheidsregistrar aanwijst, je daar ook toezicht kan beleggen.

DPC stelt dat in algehele zin een toezichthouder ontbreekt. Er is onvoldoende grip op de uitvoering, en er zijn veel organisaties binnen het Rijk die (on)bewust het huidige

domeinnaambeleid ondermijnen. DPC is sterk van mening dat de toezichtshouderrol niet bij DPC zelf belegd moet worden. Toezicht en sancties in dit opzicht zijn wenselijk, maar DPC zou dit meer beleggen bij CIO-Rijk of Directie Digitale Samenleving.

CIO-Rijk benadrukt dat het erg belangrijk is nader uit te schrijven wat er onder toezicht valt.

Decentrale overheden

Provincie Overijssel ziet dit idealiter centraal belegd. Dit creëert meer urgentie. Inrichten als een soort audit, zodat organisaties moeten laten zien dat ze het op orde hebben. En als de orde er niet is, dan handhaven. Echter moet het dan wel duidelijk belegd zijn hoe handhaving geregeld wordt. Op het moment dat er geen sancties zijn, wordt het vaak niet serieus genomen. Het is volgens provincie Overijssel dus wel wenselijk om sancties eraan te binden wanneer er structureel niet voldaan wordt aan gestelde eisen. De Waterschappen suggereren dat gemeenschappelijke afspraken op dit gebied vastgelegd kunnen worden in bijvoorbeeld de BIO, of in een wet.

Volgens gemeente Tilburg zou er op dit gebied een verplichte functionaris moeten zijn. Vanuit wet -en regelgeving is er op bepaalde onderdelen een verplichte functionaris, en andere onderdelen niet. Zonder toezicht heeft beleid niet het gewenste effect. Als je daar verplichte toetsen in opneemt is er een grotere kans dat het beleid wordt nageleefd.

4.2.9. Interbestuurlijke werkgroep waarbij iedere overheidslaag gerepresenteerd is.

Rijksoverheid

Het CIP stelt dat een overheidsbreed Interbestuurlijke werkgroep wenselijk is, en is van mening dat een vergelijkbare structuur als de werkgroep BIO kan werken rondom internetdomeinbeleid. Een centrale organisatie die gericht is op internetdomeinbeheer zou een klankbordgroep of gebruikersgroep kunnen inrichten om dit vorm te geven. Het CIP ziet dit als een basisnormenkader waarin je risicogestuurd aanvullende maatregelen treft, naast een aantal verplichte basismaatregelen. Het is dan aan individuele organisaties zelf hoe ze deze maatregelen toepassen en de risico’s taxeren. Als je binnen de conventieafspraken beheer decentraliseert, dan praat je meer samen over het nakomen van de conventies en distribueer je meer.

CIO-Rijk ziet het als wenselijk om het als een klankbordgroep in te richten, om praktijkinformatie en ‘best practices’ uit te wisselen over de uitvoering van internetdomeinbeheer.
Ook het NCSC ziet dit als een relevante optie. Volgens het NCSC kan je met dat Interbestuurlijke werkgroep signalen afgeven richting het bestuurlijk niveau.

Decentrale overheden

De Waterschappen missen een Interbestuurlijke werkgroep waarbij overheidspartijen samenkomen en nadenken over dit soort beleid en afspraken. Zij refereren naar de werkgroep BIO. Volgens de Waterschappen is Interbestuurlijke werkgroep waarin

iedere overheidslaag vertegenwoordigd is, zodat ze het kunnen gieten in eigen organisatiestructuur, wenselijk. Ook provincie Overijssel ziet het als een erg nuttige optie, omdat organisaties veel van elkaar kunnen leren in het uitwisselen van (praktijk)informatie.

4.2.10. Intern interdisciplinair expertiseteam

Rijksoverheid

CIO-Rijk stelt dat een interdisciplinair expertiseteam een goede oplossing is, maar dat organisaties dit zelf intern moeten inregelen. Volgens het NCSC is dit een relevante optie voor grote(re) organisaties. Kleinere organisaties hebben niet altijd voldoende expertise in huis, waardoor een interdisciplinair expertiseteam niet relevant is. Als kleine organisaties zelf niet over de expertise beschikken, kunnen ze ook een beroep doen op een externe groep experts. Het NCSC stelt dat deze optie meer als advies opgenomen moet worden dan als verplichtend in beleid.

Decentrale overheden

Provincie Overijssel geeft aan goed is om intern in te richten, maar het vaak een capaciteitsprobleem is. Om die reden moet het meer een advies zijn dan een verplichting. Ongetwijfeld zijn er meerdere disciplines nodig, dus er is geen ontkomen aan om het interdisciplinair in te richten. Capaciteit blijft echter een doorn in het oog.

Gemeente Tilburg duidt op het expertiseteam dat zij zelf intern hanteren op het gebied van internetdomeinbeheer. Het expertiseteam helpt niet bij extern gehoste websites die niet in lijn zijn met het gevoerde beleid gericht op internetdomeinbeheer (beleid webtoepassingen). Volgens hun is dit een stok achter de deur. Echter zijn zij wel van mening dat een interdisciplinair expertiseteam niet overal noodzakelijk is omdat daar de capaciteit niet altijd voor is en advies ook extern gevraagd kan worden.

Aanvullingen

Rijksoverheid

Het NCSC suggereert om een banner ter herkenning te plaatsen op webpagina’s, om te controleren of een website valide is. Echter is deze optie niet meer nodig wanneer er wordt gekozen voor een generieke overheidsextensie. Mogelijk is het nuttig bij het centrale overheidsregister (RIO), maar het is fraudegevoelig en er kan een nepregister achter geplaatst worden. Al met al blijft een generieke overheidsextensie de voorkeur hebben volgens het NCSC.

Daarnaast suggereert het NCSC om bij verantwoordelijkheden op te nemen dat iedere organisatie iemand heeft die verstand heeft van internetstandaarden en kwaliteitseisen. De desbetreffende persoon is dan verantwoordelijk voor het zorgdragen van (nieuwe) standaarden of kwaliteiteisen, deze integreren in de organisatie, het controleren ervan, en op de hoogte blijven van nieuwe verplichtingen.

Capaciteit is volgens zowel Logius als het NCSC noodzakelijk om deze opties in te richten.

Naming & shaming werkt effectief volgens Logius. Kan mogelijk bijdragen aan toezicht en handhaving.

Decentrale overheden

Capaciteit is volgens provincie Overijssel noodzakelijk om de bovenstaande opties in te richten.

Naming & shaming werkt effectief volgens gemeente Tilburg. Kan mogelijk bijdragen aan toezicht en handhaving.

5. Achtergrondinformatie onderzoek

5.1. Aanleiding

De overheid worstelt al enige jaren met een wildgroei aan internetdomeinen, en huidige afspraken omtrent domeinnaambeleid lijken dit niet effectief genoeg tegen te gaan. Overheidsorganisaties hebben vaak geen overzicht van hun domeinen en hebben daardoor weinig grip op kwaliteitsaspecten (zoals veiligheid, herkenbaarheid, toegankelijkheid, rechtmatigheid en effectiviteit) van de domeinnamen, en de online middelen die daar achter zitten.

Beleidsmakers zijn zich er steeds meer van bewust dat onvoldoende beheersing van het domeinportfolio significante risico's met zich meebrengt. Om de risico's te beperken is het van belang dat de overheid meer regie voert op het gebruik van internetdomeinen. De nota Herkenbare Digitale Overheid benoemt overheidsinzet voor eenduidig internetdomeinbeleid om de grip op internetdomeinen van de overheid te verhogen, en het Kamerstuk Informatieveiligheid agendeert overheidsbreed internetdomeinbeleid en stelt het belang van verankering van afspraken op dit gebied vast. Staatssecretaris Knops schreef op 18 maart 2021 aan de Kamer: *"Overheidsbreed wordt de komende jaren gewerkt aan verankering van afspraken op het gebied van domeinnaambeleid via bijvoorbeeld de BIO en het Forum Standaardisatie*[16]*."*

5.2. Doel onderzoek

In voorbereiding op deze toezegging aan de Tweede Kamer voert Bureau Forum Standaardisatie in opdracht van directie Digitale Samenleving van het ministerie van BZK een onderzoek uit naar de regie op internetdomeinen binnen de overheid. Dit onderzoek richt zich op de vraag, *'Hoe zou toekomstig overheidsbreed internetdomeinbeleid er idealiter uitzien?'* en leidt tot een adviesrapport dat kan fungeren als basis voor overheidsbreed internetdomeinbeleid. Met effectief beleid voor het gebruik van internetdomeinen kan de overheid beter sturen op de kwaliteit en het beheer van internetdomeinen en achterliggende online middelen.

Het onderzoek richt zich op:

1) Het inzichtelijk krijgen van de stand van zaken van internetdomeinbeheer binnen de overheid, en de behoeften en belangen van overheden evalueren

2) Het evalueren hoe overheden beter aangestuurd kunnen worden om overzicht en inzicht te verkrijgen in hun internetdomeinen en verantwoordelijkheid te nemen voor goed internetdomeinbeheer

[16] Kamerbrief Informatie- en communicatietechnologie (ICT); Brief regering; Voortgang informatieveiligheid bij de overheid, R.W. Knops (2021). Geraadpleegd via Informatie over Kamerstuk 26643, nr. 749 | Overheid.nl > Officiële bekendmakingen (officielebekendmakingen.nl)

3) Het adviseren over het opstellen van richtlijnen, randvoorwaarden en/of kaders voor toepassing van internetdomeinbeleid in de praktijk

4) Analyseren hoe de adoptiegraad van de pas-toe-of-leg-uit-lijst van het Forum Standaardisatie[17] en andere verplichte richtlijnen[18] verhoogd kan worden

5) Het adviseren over opties en oplossingsrichtingen om wildgroei te beperken en kwaliteitsaspecten als veiligheid en herkenbaarheid te verbeteren

De scope van het onderzoek omvat zowel internetdomeinen als domeinnamen, met achterliggende online middelen en verplichte richtlijnen van dien. Bij de start van het onderzoek spraken we van domeinnaambeleid, wat al snel veel onduidelijkheid opriep over wat het onderzoek inhoudelijk dekt. De naam domeinnaambeleid insinueerde dat het enkel gericht zou zijn op de naamgeving van internetdomeinen. Sindsdien spreken we van internetdomeinbeleid, om de scope wat breder te trekken.

Concluderend leidt deze fasering tot een adviesrapport met als doel om het beheer van internetdomeinen en de achterliggende kwaliteit overheidsbreed beter aan te sturen.

5.3. Methode en fasering

Fase een

Het onderzoek is opgedeeld in twee consultatiefases met stakeholders en andere relevante betrokkenen. In de eerste fase zijn knelpunten in beleidsvoering en in de uitvoering van internetdomeinbeheer bij zowel Rijksorganisaties als decentrale overheden geïdentificeerd door middel van gespreksvoering. In deze eerste gespreksfase is vanuit het Rijk gesproken met DPC, RVO, UWV, VWS, BZK, NCSC, en AZ, en vanuit decentrale overheden met Provincie Noord-Holland, de Unie van Waterschappen, Gemeente Tilburg, en Parkstad IT (registrar voor een aantal gemeenten). Daarnaast is ervoor gekozen om ook met SIDN in gesprek te gaan, als overheidsleverancier en .nl-domein houder. In de gesprekken zijn vragen gesteld op basis van relevante onderwerpen met betrekking tot internetdomeinbeheer.

Aan de hand van deze gesprekken is een rapport[19] opgesteld en de bevindingen die hieruit voortgekomen zijn hebben de basis gelegd voor de tweede fase. Onder hoofdstuk 4.1 zijn de hoofdbevindingen van deze fase toegelicht.

Fase twee

In de tweede fase zijn oplossingsrichtingen verkend op basis van de geconstateerde knelpunten uit de eerste fase. Na het vaststellen van een aantal oplossingsrichtingen zijn deze voorgelegd bij Rijksorganisaties en decentrale overheden. De oplossingsrichtingen zijn gedurende dit proces aan de hand van gesprekken bijgesteld.

[17] Lijst open standaarden, Forum Standaardisatie. Geraadpleegd via Lijst open standaarden | Forum Standaardisatie

[18] Inhoudelijke informatie met betrekking tot de verplichte richtlijnen online middelen zijn te vinden op de pagina 'Handreiking Verplichte richtlijnen websites en andere online middelen', UBR (2019).

[19] Rapportage eerste fase onderzoek overheidsbreed internetdomeinbeleid, Forum Standaardisatie (2021). Niet online te raadplegen, wordt op verzoek intern gedeeld.

Eveneens is gevraagd naar de prioritering van deze oplossingsrichtingen. Er hebben gesprekken plaatsgevonden met het NCSC, DPC, Logius, en CIO-Rijk van de Rijksoverheid, en met de Provincie Overijssel, het Waterschapshuis, en gemeente Tilburg van decentrale overheden. Daarnaast is er een gesprek met het CIP aangegaan over de opgestelde oplossingen.

De resultaten hiervan zijn eveneens in een rapport[20] vastgelegd en vormen de basis voor het uiteindelijke advies. In hoofdlijnen zijn de uitkomsten van het rapport beschreven in 4.2 van dit rapport. Uiteindelijk is fase twee afgesloten met tien oplossingen, die in het advies opgenomen zijn (zie hoofdstuk 3).

Voor alle gesprekken geldt dat deze gevoerd zijn met kennisexperts en deskundigen die betrokken zijn bij internetdomeinbeheer in de hierboven genoemde organisaties. Uitgaande van de standpunten, perspectieven en ervaringen van deze personen valt dit niet te generaliseren naar het perspectief van de gehele organisatie, of de gehele overheid.

[20] Rapportage tweede fase onderzoek overheidsbreed internetdomeinbeleid, Forum Standaardisatie (2022). Niet online te raadplegen, wordt op verzoek intern gedeeld.

6. Bijlagen

6.1. Bijlage 1: Aanbevelingen voor levenscyclusbeheer

In onderstaande procesbeschrijving zijn suggesties gedaan voor het invullen van een beheerproces. Het proces dient nader verfijnd te worden en fungeert als een voorzet voor verdere inrichting van processen omtrent levenscyclusbeheer. De afspraken die benoemd zijn in de oplossingen dienen als leidraad in de procesopzet. Ook het rijksbreed afwegingskader online middelen[21] en de handreiking verplichte richtlijnen websites en andere online middelen[22] dienen als een voorbeeld-format voor het vastleggen van beleidsregels en richtlijnen.

Afspraken omtrent levenscyclusbeheer

Registratieprocedure:

Een overheidsorganisatie dient bij een nieuwe communicatiebehoefte, vóór het registreren van een nieuw domein, een aantal stappen na te gaan:

1) Het vaststellen van het (communicatie)doel en doelgroep van de domeinnaam;

2) Te controleren of het (communicatie)doel niet aansluit bij een voorgaand communicatiedoel, en of de gecommuniceerde informatie niet al eerder gecommuniceerd is op het hoofddomein of een subdomein (informatie dient niet gedupliceerd te worden);

3) Als deze informatie niet eerder gecommuniceerd is, maar wel aansluit bij een al eerder (communicatie)doel kan deze informatie ondergebracht worden onder een bestaand hoofd- of subdomein (bijvoorbeeld door een extra webpagina op een hoofd- of subdomein of een pagina op andere domeinnaam in beheer van de desbetreffende organisatie) (versnippering van informatie en daarmee slechte vindbaarheid voorkomen);

4) Als het om nieuwe informatie gaat met een nieuw (communicatie)doel, controleren of deze informatie ondergebracht kan worden onder een herkenbaar basisdomein (.gov.nl of .organisatie.nl, bestaande subsite). Het uitgangspunt als basis is dat alle informatie op het basis domein, of subdomein ervan, wordt ondergebracht;

5) Als dit niet geregistreerd kan worden onder een bestaand basisdomein (pas-toe-of-leg-uit), dan de nieuwe domeinnaam registreren volgens naamgeving richtlijnen

[21] Rijksbreed afwegingskader online middelen, Rijksvoorlichtingsdienst (2020). Geraadpleegd via Rijksbreed afwegingskader online middelen | Publicatie | CommunicatieRijk

[22] Handreiking verplichte richtlijnen websites en andere online middelen, Rijksoverheid (2019). Geraadpleegd via Handreiking Verplichte richtlijnen websites en andere online middelen | Brochure | UBRijk

(zie punt 2 over naamgeving) en volgens richtlijnen herkenbare overheidsextensie (punt 3);

6) Registreren via communicatietechnisch en IT-tactisch advies (centrale overheidsregistrar en interne adviseurs);

7) Vastleggen wie eigenaar en beheerder van de domeinnaam is (zie bijlage 2 over rollen en verantwoordelijkheden);

8) Registratieproces in werking zetten bij centrale overheidsregistrar (zie punt 4 over registrar).

Naamgevingsrichtlijnen

Bij registratie dient de naamgeving niet herkenbare, maar organisatie-specifiek te zijn om de herkenbaarheid van de overheidsorganisatie ten goede te komen. De naam dient herleidbaar te zijn naar de organisatie, zodat het voor de burger duidelijk is met welke overheidsorganisatie hij of zij interacteert.

Herkenbare overheidsextensie

Bij het doorvoeren van een herkenbare overheidsextensie dienen afspraken gemaakt te worden wanneer een (nieuw) domein in aanmerking komt voor deze extensie. Dit kan geïdentificeerd worden op basis van RIO. Alleen de centrale overheidsregistrar mag domeinen met de herkenbare overheidsextensie registreren. DNS-beheer kan zowel bij de centrale overheidsregistrar of uitbesteed worden aan een externe leverancier. Daarvoor gelden leverancierseisen volgens de verplichte richtlijnen van de Rijksoverheid.

Centrale overheidsregistrar:

1) Registratie gebeurt ten alle tijden via de domeinnaam liaison, of bij het ontbreken van een domeinnaam-liaison via de CIO/CISO;

2) Registratie gebeurt ten alle tijden bij de centrale overheidsregistrar;

Na het registreren van een nieuwe domeinnaam dienen de vastgelegde rollen en verantwoordelijkheden openlijk gecommuniceerd te worden naar de centrale overheidsregistrar en RIO, en schriftelijk te worden vastgelegd binnen de eigen organisatie zodat duidelijk is voor (Rijks)overheidsorganisaties hoe de verantwoordelijkheden van o.a. eigenaarschap en beheer belegd zijn binnen een organisatie (zie bijlage 2 over rolverdeling en verantwoordelijkheid).

Procedure voor uitfasering en het offline halen van een domeinnaam

Een overheidsorganisatie dient een website uit te laten faseren wanneer:

1) Het vooraf gestelde (communicatie)doel van de domeinnaam al behaald of verstreken is (bijvoorbeeld na afloop van een campagne);

2) Bij langdurige inactiviteit (langer dan periode X);

3) Wanneer de (communicatie)doelstelling al is ondergebracht onder een andere domeinnaam of webpagina;

4) Website dient dan volgens de verplichte richtlijnen[23] gearchiveerd te worden bij uitfasering.

De domeinnaam dient direct offline te worden gehaald wanneer:

1) De domeinnaam niet aan score X (90-100%) van toepassing van de veiligheidseisen voldoet (signalering n.a.v. centrale monitoring/periodieke controlechecks van RIO), en na periode X hier nog niet aan heeft voldaan, of;

2) Wanneer er niet conform dit beleid geregistreerd en/of beheerd is;

3) De CISO/CIO heeft dan het mandaat om de website offline te halen na een waarschuwing met een bepaald termijn om aanpassing te voeren.

Procedure voor het vrijgeven van een domeinnaam

Een domein(naam) dient niet vrijgegeven te worden wanneer:

1) Er e-mail gedraaid heeft op het domein, dan dient deze definitief behouden te worden;

2) Als er gevoelige en/of belangrijke overheidsinformatie op heeft gestaan, dient deze definitief behouden te worden;

3) Als gewenst wordt deze niet te behouden, dan dient er een verklaring van vernietiging ingediend te worden bij de centrale overheidsregistrar, vóór verwerking in RIO.

   Een domein(naam) dient na een afgesproken termijn vrijgegeven te worden wanneer:

   1) Overname door een andere partij kan leiden tot onherkenbaarheid bij de burger. Het eigenaarschap dient dan bij de overheid blijven liggen, bijvoorbeeld bij een 'domeinnamendepot' van de centrale overheidsregistrar. Het domein wordt dan pas vrijgegeven wanneer er een bepaald termijn is verstreken (dat vooraf is afgesproken op basis van kans op misbruik van het domein), en in dit termijn naar de burger is gecommuniceerd dat het domein niet meer onder de overheid valt;

   2) Als een domein op de herkenbare overheidsextensie heeft gedraaid, dient er een termijnafspraak gemaakt te worden over het vrijgeven van een domein. Deze

[23] Inhoudelijke informatie met betrekking tot de verplichte richtlijnen online middelen zijn te vinden op de pagina 'Handreiking Verplichte richtlijnen websites en andere online middelen', UBR (2019).

dient niet direct vrijgegeven te worden. De termijn is afhankelijk van de inhoud van het domein.

6.2. Bijlage 2: Aanbevelingen voor verantwoordelijkheden en rollen

Onderstaande opzet is een voorzet voor verdere beleidsinvulling. De oplossing is om dit verder te specificeren voor vastlegging in het internetdomeinbeleid. Zie ook de handreiking beheer internetdomeinen rijksoverheid[24] voor verdere specificatie van verantwoordelijkheden. Daarnaast dienen ook het rijksbreed afwegingskader online middelen[25] en de handreiking verplichte richtlijnen websites en andere online middelen[26] als een format voor het vastleggen van beleidsregels en richtlijnen.

Rollen en verantwoordelijkheden

Het advies is om verantwoordelijkheden vast te leggen, en de rolverdeling aan de hand van organisatiestructuur te laten inrichten door de organisatie zelf. Met betrekking tot de invulling van deze rolverdeling zijn suggesties gedaan van relevante rollen met betrekking tot internetdomeinbeheer[27].

1) Een overheidsorganisatie dient de onderstaande verantwoordelijkheden te beleggen in de organisatie, en dient de formele vastlegging te rapporteren aan de centrale overheidsregistrar en RIO. De rolverdeling[8] dient de organisatie aan te passen aan eigen organisatiestructuur en capaciteit.

Onder deze verantwoordelijkheden vallen het koppelen van rollen aan internetdomeinen van de organisatie;

1. Het beleggen van eigenaarschap van een domein(naam);
2. Het beleggen van het beheer van een domein(naam), waaronder levenscyclusbeheer en procesvastlegging daarvan;
3. De nazorg van een domein bij het overdragen van een functie;
4. Etc.

[24] Handreiking Beheer Internetdomeinen Rijksoverheid, RDDI (2021). Geraadpleegd via Nu beschikbaar: Handreiking Beheer Internetdomeinen Rijksoverheid | Nieuwsbericht | Rijksprogramma voor Duurzaam Digitale Informatiehuishouding

[25] Rijksbreed afwegingskader online middelen, Rijksvoorlichtingsdienst (2020). Geraadpleegd via Rijksbreed afwegingskader online middelen | Publicatie | CommunicatieRijk

[26] Handreiking verplichte richtlijnen websites en andere online middelen, Rijksoverheid (2019). Geraadpleegd via Handreiking Verplichte richtlijnen websites en andere online middelen | Brochure | UBRijk

[27] Rollen die in veel gevallen deze verantwoordelijkheden dragen zijn (web)eigenaar, functioneel beheerder, portfoliobeheerder, liaison, communicatieadviseur of CISO.

Maar ook de interne *governance* omtrent internetdomeinbeheer binnen een organisatie:

1. Het beleggen van de liaisonrol naar de centrale overheidsregistrar en RIO;
2. Het aanstellen van een intern centraal aanspreekpunt met betrekking tot internetdomeinbeheer;
3. Het voldoen aan kwaliteitseisen als open standaarden en verplichte richtlijnen;
4. Het zijn van een aanspreekpunt naar externe leveranciers en het bewaken van leverancierseisen;
5. Etc.

2) Wanneer de rollen interdisciplinair op verschillende afdelingen belegd zijn (zoals zowel bij communicatie als bij de IT directie), dan dient eenvoudige samenwerking en communicatie tussen deze directies mogelijk te zijn. Tevens wordt geadviseerd een interdisciplinair expertiseteam op te stellen (zie punt 3.10)

3) Een overheidsorganisatie dient een centraal aanspreekpunt aan te stellen op het gebied van domeinnaambeheer, en deze te communiceren naar de centrale overheidsregistrar en RIO.

4) De CISO/CIO is eindverantwoordelijke om deze rollen te delegeren en te communiceren.

Voorbeeld voor beleggen verantwoordelijkheden internetdomeinen (intern)

Verantwoordelijkheid	**Domein(naam)**	**Rol**	**Contactpersoon**
Eigenaarschap		Webeigenaar	Jan Rijk
(Levenscyclus)beheer (zie bijlage 1)	www.rijksoverheid.gov.nl	Functioneel beheerder	Ben Gemeen
Wijzigingen doorvoeren in RIO	www.rijksoverheid.gov.nl	Functioneel beheerder	Ben Gemeen
Nazorg domein bij functie-overdracht	www.rijksoverheid.gov.nl	Webeigenaar	Jan Rijk
Etc.			

Voorbeeld voor beleggen verantwoordelijkheden internetdomeinbeheer (intern)

Verantwoordelijkheid	**Rol**	**Contactpersoon***
Schriftelijke vastlegging van verantwoordelijkheden en rolverdeling	CIO/CISO	Piet Pres
Centraal aanspreekpunt internetdomeinbeheer intern	Communicatieadviseur	Mark Min
Centraal aanspreekpunt naar centrale overheidsregistrar	Liaison	Dirk Wat
Centraal aanspreekpunt naar RIO	Liaison	Dirk Wat
Centraal aanspreekpunt naar externe leveranciers	Portfoliobeheerder	Henk Pro
Intern overzicht bewaken en actualiseren	Portfoliobeheerder	Henk Pro
Voldoen aan kwaliteitseisen	CISO	Piet Pres
Uitvoeren van periodieke kwaliteitscontrole	Portfoliobeheerder	Henk Pro
Etc.		

***Contactpersoon kan ook functionele mailbox zijn**

6.3. Referenties

Buitenlandonderzoek Domeinnaambeleid, PBLQ. (2019). Geraadpleegd via Buitenlandonderzoek domeinnaambeleid | Kennisbank Openbaar Bestuur (kennisopenbaarbestuur.nl).

Domeinnaambeleid, Rijksoverheid (2011). Geraadpleegd via www.domeinnaambeleid.nl.

Handreiking Beheer Internetdomeinen Rijksoverheid, RDDI (2021). Geraadpleegd via Nu beschikbaar: Handreiking Beheer Internetdomeinen Rijksoverheid | Nieuwsbericht | Rijksprogramma voor Duurzaam Digitale Informatiehuishouding

Handreiking verplichte richtlijnen websites en andere online middelen, UBR (2019). Geraadpleegd via Handreiking Verplichte richtlijnen websites en andere online middelen'

Handreiking verlopen domeinnamen, Z-CERT. (2021). Geraadpleegd via Z-CERT_Handreiking2021.pdf

Herkenbaarheid van en vertrouwen in websites en e-mails van de overheid, Kantar. (2019). Geraadpleegd via Herkenbaarheid van en vertrouwen in websites en s van de overheid - PDF Free Download (docplayer.nl).

Kamerbrief Informatie- en communicatietechnologie (ICT); Brief regering; Voortgang informatieveiligheid bij de overheid, R.W. Knops (2021). Geraadpleegd via Informatie over Kamerstuk 26643, nr. 749 | Overheid.nl > Officiële bekendmakingen (officielebekendmakingen.nl)

Lijst open standaarden, Forum Standaardisatie. Geraadpleegd via Lijst open standaarden | Forum Standaardisatie

Rapportage eerste fase onderzoek overheidsbreed internetdomeinbeleid, Forum Standaardisatie (2021). Niet online te raadplegen, wordt op verzoek intern gedeeld.

Rapportage tweede fase onderzoek overheidsbreed internetdomeinbeleid, Forum Standaardisatie (2022). Niet online te raadplegen, wordt op verzoek intern gedeeld.

Rapport technische impactanalyse eenduidige domeinnaam, ICTU. (2022). Niet online te raadplegen.

Rijksbreed afwegingskader online middelen, Rijksvoorlichtingsdienst (2020). Geraadpleegd via Rijksbreed afwegingskader online middelen | Publicatie | CommunicatieRijk

Testtool internet.nl. Geraadpleegd via www.internet.nl.