



notitie

FORUM STANDAARDISATIE 10 juni 2015 Agendapunt 3: Adoptie open standaarden Stuknummer 3: Oplegnotitie adoptie

Van:	Stuurgroep adoptie open standaarden
Bijlagen:	3A TNO-rapport "Overheidsbrede beleidskaders voor IPv6-nummerplannen" 3B Concept-verslag Nationaal Beraad d.d. 18 mei 3C Verantwoording ministeries over open standaarden in jaarverslagen 2014

Ter bespreking

U wordt gevraagd:

1. de conclusies en aanbevelingen van het TNO-rapport "Overheidsbrede beleidskaders voor IPv6-nummerplannen" te bespreken en te komen tot een stellingname hierover (N.B. besluitvorming verloopt via Regieraad Interconnectiviteit);

Ter informatie

U wordt gevraagd om kennis te nemen van:

2. Terugkoppeling Nationaal Beraad d.d. 18 mei jl.;
3. Verantwoording ministeries over open standaarden in jaarverslagen 2014;
4. Voortgang Platform Internetstandaarden en Internet.nl;
5. Onderzoek samenhang en adoptie ICT-beveiligingsstandaarden (geen bijlage);
6. Adoptiesuccessen en bijeenkomsten (geen bijlage).

Ter bespreking

1. TNO-rapport "Overheidsbrede beleidskaders voor IPv6-nummerplannen" [Bijlage A]

Het Forum wordt gevraagd de conclusies en aanbevelingen van het rapport "Overheidsbrede beleidskaders voor IPv6-nummerplannen" te bespreken en te komen tot een stellingname hierover. Bestuurlijke besluitvorming verloopt via Regieraad Interconnectiviteit. BZK zal eventuele adviezen van het Forum Standaardisatie, waar mogelijk, in dit traject meenemen.

Aanleiding

De directie Burgerschap en Informatiebeleid van BZK heeft TNO i.s.m. PBLQ de opdracht gegeven om onderzoek te doen naar "gemeenschappelijke afspraken aangaande IPv6-nummerplannen tussen overheidsorganisaties". Dit heeft geresulteerd in het rapport "Overheidsbrede beleidskaders voor IPv6-nummerplannen".

Betrokkenen

De begeleidingscommissie van het onderzoek bestond uit vertegenwoordigers van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (DGBK en DGOBR), Logius, KING, IPO, UvW, de Manifestgroep en SURFnet. Daarnaast is gesproken met stakeholders en experts van Gemeente Alkmaar, Gemeente Heerlen, Hoogheemraadschap Hollands Noorderkwartier, Provincie Overijssel (SSC Zwolle), NCSC, British Telecom, Centric, KPN Lokale Overheid, Citkomm (Duitsland), FedICT (België), Ministerie van Binnenlandse Zaken (Duitsland), en Ministerie van Financiën (Spanje).

Bestuurlijke besluitvorming

Het in dit rapport voorgestelde IPv6-nummerplankader dient als startpunt voor een overheidsbreed IPv6-nummerplankader, dat nog definitief vastgesteld zal moeten worden. Verdere besluitvorming vindt (naar verwachting) plaats via de Regieraad Interconnectiviteit. BZK zal eventuele adviezen van het Forum Standaardisatie, waar mogelijk, in dit traject meenemen.

Overheidsbreed IPv6-beleidskader

Een overheidsbreed beleidskader voor IPv6-nummerplannen betreft gemeenschappelijke afspraken rondom de invoering van IPv6. Het gaat in essentie om de volgende afspraken:

1. de Nederlandse overheid registreert een eigen blok (of een beperkt aantal eigen blokken) met 'leveranciersafhankelijke' IPv6-adressen bij de Europese uitgifte-instantie RIPE NCC;
2. een centrale beheerder, zoals Logius, stelt volgens een afgesproken werkwijze en onder afgesproken voorwaarden op verzoek IPv6-adressen beschikbaar aan overheidsorganisaties;
3. iedere individuele overheidsorganisatie neemt de (op verzoek) ontvangen IPv6-adressen in gebruik conform een eigen, intern nummerplan dat voldoet aan de gestelde gemeenschappelijke voorwaarden.
4. Kortom: het beleidskader is faciliterend en stimulerend, maar bepaalt niet het tempo waarmee een individuele overheidsorganisatie IPv6 moet invoeren.

De Rijksoverheid hanteert reeds een dergelijk beleidskader, evenals een aantal buitenlandse overheden, zoals de Duitse en Spaanse. Het idee is om het huidige Rijks-beleidskader 'op te rekken' en voor de gehele overheid beschikbaar te

maken. Verschillende partijen (zoals gemeente Amsterdam) hebben hier ook al om gevraagd.

Hoofdconclusies

In het onderzoek komt naar voren dat een dergelijke beleidskader, niet allen voor de Rijksoverheid maar overheidsbreed, de onderstaande voordelen biedt.

- Leveranciersafhankelijkheid: Door gebruik te maken van overheidseigen (in plaats van leveranciersspecifieke) IPv6-adressen kunnen omnummerkosten bij een leverancierswissel worden voorkomen en wordt het mogelijk om overheden redundant via verschillende internetproviders aan te sluiten.
- Informatieveiligheid: Het gebruik van één of beperkt aantal adresblokken maakt IPv6-adressen herkenbaarder en eenvoudiger te registreren wat kan helpen bij detectie van misbruik en het maken van onderscheid tussen overheidsverkeer en niet-overheidsverkeer.
- Financieel voordeel: Het gebruik van overheidseigen IPv6-adressen (in plaats van leveranciersspecifieke) brengt kostenvoordelen met zich mee als daardoor een significant aantal omnummeractiviteiten wordt voorkomen. Door een centraal overheidsnummerblok te registreren hoeven individuele overheden niet allemaal zelf (betaald) lid te worden van Europese uitgifte-instantie RIPE NCC om eigen IPv6-adressen te ontvangen.
- Overige baten: Mede door IPv6 zal het aantal netwerkconnecties de komende jaren exponentieel toenemen. Enige structuur aanbrengen helpt om een goed beheersbare en toekomstvast IPv6-infrastructuur in te richten.

Aanbevelingen: Elementen IPv6-beleidskader

1. Streef ernaar dat overheidsorganisaties gebruik maken van IPv6-adressen die eigendom zijn van de overheid.
2. Beperk het aantal overheidseigen IPv6-adresblokken en maak Logius de centrale uitgifte-instantie (LIR), waarbij decentrale overheden terechtkunnen.
3. Gebruik bij het overheids-IPv6-uitgiftebeleid de conventies van RIPE-beleid. [...] Houd ruimte over bij het uitdelen van IPv6-adresblokken aan overheidsorganisaties, zodat bij uitbreiding in de toekomst het adresblok kan worden vergroot.
4. Adviseer organisaties om structuur aan te brengen in hun IPv6-nummerplan.
5. Iedere overheidsorganisatie dient te beschikken over een goed leesbaar IPv6-nummerplan, waarbij best practices (zoals weergegeven in bijvoorbeeld dit rapport en in het Rijksnummerplan) in beschouwing zijn genomen.

Aanbevelingen: Besturing, uitvoering en financiering van IPv6-beleidskader

1. Maak het kader onderdeel van de Generieke Digitale Infrastructuur van de overheid (GDI) en daarmee de besluitvorming over de wenselijkheid en inhoud van het kader onderhavig aan de daarvoor geldende governance-structuur.
2. Geef sectoren en regionale samenwerkingsverbanden de vrijheid om onderling verdergaande afspraken te maken ter verdere invulling van het overheidsbrede kader. Zorg er via de centrale uitgifte-instantie (LIR) voor dat deze afspraken binnen het overheidsbrede kader passen.
3. Zorg ervoor dat het nummerplankader wordt gebruikt door de bestaande voorzieningen, referentiearchitecturen en als aanbeveling op de pas-toe-of-leg-uit lijst. Laat het waar mogelijk aansluiten bij andere discussies aangaande overheidscommunicatie, bijvoorbeeld over besloten netwerken en overheidscloud-initiatieven. Dit hoort thuis in de governancestructuur van de GDI.

4. Beleg de uitvoering en het onderhoud van het nummerplankader bij één landelijk centrale partij. Laat deze partij afspraken maken met overige partijen over de disseminatie van het nummerplan.
5. Overweeg of het wenselijk is om ook overige taken ter ondersteuning van overheden bij de invoering van IPv6 bij de centrale beheerder te beleggen.
6. Regel de financiering van het beheer van het nummerplankader structureel door deze mee te nemen in de financiering van de GDI.

Ter informatie

2. Terugkoppeling Nationaal Beraad d.d. 18 mei jl. [Bijlage B]

Het Forum Standaardisatie heeft het Nationaal Beraad gevraagd in te stemmen met:

1. voorgestelde resultaatsafspraken adoptie informatieveiligheid-standaarden (tegen vervalsingen van overheidswebsites en -email); en
2. herbevestiging en verlenging van de bestaande overheidsbrede 'pas toe of leg uit' -afpraak tot eind 2017; en
3. opname van standaarden op het gebied van informatiebeveiliging (ISO27001/2, DMARC,SPF) en begrippenuitwisseling (SKOS) op de 'pas toe of leg uit' lijst (conform bijlage).

In de bijlage treft u het concept-verslag van het Nationaal Beraad aan. Het Nationaal Beraad heeft niet ingestemd met punt 1. Met punt 2 en 3 is wel ingestemd. Door het Bureau is verzocht om de positieve besluitvorming t.a.v. de punten 2 en 3 explicieter te maken in het definitieve verslag (het staat er nu impliciet als "om de voorgestelde standaarden en afspraken vast te stellen").

3. Verantwoording ministeries over open standaarden in jaarverslagen 2014 [Bijlage C]

In het kader van 'pas toe of leg uit' zijn overheden verplicht om zich te verantwoorden over afwijkingen van open standaard in het jaarverslag. Het Bureau heeft de recent gepubliceerde departementale jaarverslagen doorgenomen en de relevante passages m.b.t. verantwoording over open standaarden op een rij gezet. In de bijlage treft u het resultaat aan.

4. Voortgang Platform Internetstandaarden en Internet.nl

De website Internet.nl werd na de lancering tijdens de Cybertop gelijk al veel gebruikt. In vier weken tijd zijn meer dan 27.000 tests uitgevoerd. Op de website kunnen bezoekers eenvoudig testen of hun website, e-mail en internetverbinding gebruik maakt van moderne internetstandaarden.

Voor veel partijen blijkt dat er het een en ander te verbeteren valt. Maar er zijn ook verschillende organisaties die het prima voor elkaar hebben en laten zien dat een 100%-score goed mogelijk is, zoals ibdgemeenten.nl, tilburguniversity.edu, pleio.nl, surf.nl en defensie.nl .

Ook hebben we gezien dat verschillende partijen hun score inmiddels hebben verbeterd door over de resultaten in contact te treden met hun webhoster, mailhoster of ISP.

De huidige website is een eerste versie. Platform Internetstandaarden zal de website verder ontwikkelen. Je kan de ontwikkelingen ook volgen via Twitter (https://twitter.com/internet_nl). Eventuele feedback of vragen zijn welkom via vraag@internet.nl.

5. Onderzoek samenhang en adoptie ICT-beveiligingsstandaarden

Binnenkort start VKA in opdracht van het Bureau met de uitvoering van een onderzoek naar de samenhang en adoptie van ICT-beveiligingsstandaarden. Daarin staan de volgende vragen centraal.

1. Lijst en blinde vlekken: Welke IB-standaarden staan nu op de lijst? Ontbreken er IB-standaarden op de lijst? Zijn er belangrijke nieuwe ontwikkelingen?
(N.B. ook kaders/richtlijnen meenemen, zoals "Grip op secure software development (SSD)", "ICT-beveiligingsrichtlijnen voor webapplicaties, "Framework Secure Software")
2. Samenhang: Hoe verhouden de geïdentificeerde IB-standaarden zich tot elkaar? Hoe zou de samenhang kunnen worden versterkt?
3. Adoptie: Hoe verloopt de adoptie van deze standaarden en hoe kan deze worden versneld? (ook evt. via harmonisatie om audit-/implementatiedruk te verlichten)

Eind vorig jaar heeft het Forum besloten om een stuurgroep informatiebeveiliging op te richten. Deze stuurgroep zal het onderzoek begeleiden. Het voorstel is om de stuurgroep te laten bestaan uit de volgende Forum-leden: Guus Bronkhorst, Erwin Bleumink en Nico Romijn.

6. Adoptiesuccessen en bijeenkomsten

- Webrichtlijnen.nl doet IP6 en DNSSEC.
- SSC-ICT doet sinds kort DMARC-checks en verstuurt DMARC-rapportages voor inkomende e-mail. Ze ondersteunden al SPF- en DKIM-validatie. (anti-phishing/-spoofing).
- Sessie over DANE (extra beveiliging certificaten o.b.v. DNSSEC) bij DPC/AZ op 20 mei. Presentaties op aanvraag beschikbaar.
- Eén centraal platform voor open bouwstandaarden: Het BIM Loket brengt 12 open BIM (Bouw Informatie Model) standaarden bijeen. Het Loket zal zich ontwikkelen tot een centraal informatie- en beheerpunt voor deze standaarden in de bouw. De feestelijke start was tijdens de goed bezochte BIM Praktijkdag op 30 april in de Jaarbeurs.
- In navolging van de Engelse overheid organiseert het Bureau i.s.m. de Internet Society op 17 september in Den Haag een ODF Plugfest. In ieder geval zal een vertegenwoordiger van de UK Cabinet Office aanwezig zijn. We verwachten daarnaast ook Google, Microsoft en andere belanghebbende leveranciers aan tafel.