notitie

FORUM STANDAARDISATIE 9 oktober 2019
Agendapunt 4B – Forumadvies RPKI

Nummer:	FS-191009.4B
Aan:	Forum Standaardisatie
Van:	Stuurgroep Open Standaarden
Datum:	9 oktober
Versie:	1.0
Bijlagen:	Expertadvies RPKI Commentaar op de openbare consultatie RPKI

1. Aanleiding en achtergrond
RPKI (Resource Public Key Infrastructure) is een techniek met als doel om zogenaamde route hijacks te voorkomen. Bij een route hijack wordt internetverkeer omgeleid naar de systemen van een niet geautoriseerd netwerk. Een hijack kan het gevolg zijn van een simpele typefout van een netwerkbeheerder die daarmee onbedoeld internetverkeer omleidt, of het gevolg zijn van een doelgerichte aanval op de infrastructuur van het internet om bijvoorbeeld websites onbereikbaar te maken of om gegevens van internetgebruikers afhandig te maken. Een relevante voorbeeld hiervan betreft een incident waarbij een set IP-adressen van het ministerie van Buitenlandse Zaken in 2014 tijdelijk gekaapt is door Bulgaarse bendes[1] [2].

2. Betrokkenen en proces
RPKI is aangemeld voor opname op de 'pas toe of leg uit'-lijst door Alex Band van NLnet Labs.

Voor het opstellen van het Forumadvies is de volgende procedure doorlopen:

1. De procesbegeleiders en de vertegenwoordiger van het Bureau Forum Standaardisatie hebben op 10 april 2019 een intakegesprek gevoerd met de indiener. Tijdens de intake is de standaard getoetst op de criteria voor in behandel name en is een eerste inschatting gemaakt van de kans rijkheid van de procedure.
2. Op basis van de intake heeft het Forum Standaardisatie op 12 juni 2019 besloten de aanmelding in procedure te nemen. Hierop volgend is een expertgroep samengesteld en een voorzitter aangesteld.
3. De leden van de expertgroep hebben een voorbereidingsdossier gekregen dat is opgesteld met informatie uit de aanmelding en het intake onderzoek. Voorafgaand aan de expertbijeenkomst heeft de expertgroep dit voorbereidingsdossier doorgenomen en aandachtspunten geïdentificeerd.
4. De expertgroep is op 24 juni 2019 bijeengekomen om de bevindingen in het algemeen en de geïdentificeerde aandachtspunten in het bijzonder te bespreken. Tijdens deze bijeenkomst zijn

[1] https://zoek.officielebekendmakingen.nl/ah-tk-20142015-3181.html
[2] https://www.volkskrant.nl/wetenschap/ip-adressen-ministerie-gekaapt-door-bulgaren~b75ad982/

ook het toepassings- en werkingsgebied vastgesteld. Zes experts hebben schriftelijk hun reactie gegeven voorafgaand aan de expertbijeenkomst.

De volgende experts waren daarbij aanwezig:
- Melchior Aelmans (Juniper Networks)
- Alex Band (NLnet Labs, indiener)
- Iljitsch van Beijnum (Muada)
- Tim Bruijnzeels (NLnet Labs)
- Marco Davids (SIDN)
- Robert Heuvel (Atom86)
- Joris Joosten (Logius)
- Hugo Leisink (NCSC)
- Twan van der Meer (IBD, VNG Realisatie)
- Damiën Meijer (Dictu)
- Edward Paijmans (Belastingdienst)
- Job Snijders (NTT, OpenBSD)
- Nathalie Trenaman (RIPE NCC)
- Christian Veenman (NCSC)
- Simone Verwer (Betaalvereniging)
- Teun Vink (BIT BV)
- Jeroen van de Weerd (Inlichtingenbureau)

Schriftelijk hebben een reactie gegeven:

- Jascha Gregorowitsch (Enable-U)
- Jac Kloots (SURFnet)
- Oscar Koeroo (KPN)
- Glenn Lutke Schipholt (Logius)
- Niels Raijer (Fusix)
- Martijn Keizer (Enable-U)

Als onafhankelijk voorzitter is opgetreden Bas van Luxemburg, hoofd Research en Development bij Lost Lemon. Jasper Muskiet (consultant) en Arjen Brienen (senior consultant) bij Lost Lemon, hebben de procedure in opdracht van het Bureau Forum Standaardisatie begeleid. Redouan Ahaloui van het Bureau Forum Standaardisatie was als toehoorder bij de expertbijeenkomst aanwezig.

De openbare consultatie heeft gelopen van 5 augustus 2019 tot en met 2 september 2019.

3. Consequenties en vervolgstappen

Tijdens de openbare consultatie is één reactie binnen gekomen. Een vertegenwoordiger van de Kamer van Koophandel geeft aan het eens te zijn met het expertadvies en de opname te ondersteunen. Zodra RPKI op de 'pas toe of leg uit'-lijst is geplaatst, stemt de KvK af met haar provider wanneer de standaard ondersteund wordt.

4. Gevraagd besluit

Het Forum Standaardisatie wordt gevraagd om in te stemmen met onderstaand advies.

Het Forum Standaardisatie adviseert het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO) om:

1. *RPKI op te nemen op de 'pas toe of leg uit'-lijst.*
2. *Het functioneel toepassingsgebied voor RPKI als volgt vast te stellen: "RPKI moet worden toegepast door netwerkaanbieders en houders van blokken IP-adressen bij het aanbieden van netwerkconnectiviteit, ter beveiliging van het BGP (Border Gateway Protocol). Dit geldt zowel voor het publiceren van ROA's (Route Origin Authorisations) als voor het valideren en het 'droppen' van invalide routes."*
3. *Ten aanzien van de adoptie van RPKI de oproepen te doen die beschreven staan in paragraaf 5.5 hieronder.*

5. Toelichting

5.1 Over de standaard

Resource Public Key Infrastructure (RPKI) is een techniek met als doel om zogenaamde route hijacks te voorkomen. Bij een route hijack wordt internetverkeer omgeleid naar de systemen van een niet-geautoriseerd netwerk. Een hijack kan het gevolg zijn van een simpele typefout van een netwerkbeheerder die daarmee onbedoeld internetverkeer omleidt, of het gevolg zijn van een doelgerichte aanval op de infrastructuur van het internet om bijvoorbeeld websites onbereikbaar te maken of om gegevens van internetgebruikers afhandig te maken. [3] Een relevant voorbeeld hiervan betreft een incident waarbij een set IP-adressen van het ministerie van Buitenlandse Zaken in 2014 tijdelijk gekaapt is door Bulgaarse bendes[4] [5].

Met RPKI kan de rechtmatige houder van een blok IP-adressen een autoritatieve, digitaal getekende verklaring publiceren met betrekking tot de intenties van de routering vanaf haar netwerk. Deze verklaringen, genaamd Route Origin Authorisations (ROA's),kunnen andere netwerkbeheerders cryptografisch valideren en vervolgens gebruiken om filters in te stellen. Hiermee filteren routers routes uit die in strijd zijn met de voor de betreffende IP-adressen gepubliceerde ROA's (invalid = reject).

RPKI vraagt dus om actie vanuit twee partijen. Ten eerste moet de houder van de IP-adressen ROA's publiceren. Ten tweede moet de partij die via Border Gateway Protocol (BGP) routes ontvangt van andere netwerken filteren op basis van alle wereldwijd gepubliceerde ROA's, waarbij invalide routes nooit geaccepteerd of geadverteerd mogen worden. Partijen die namens overheden IP-adressen publiceren moeten dus conform voorgaande ROA's publiceren. Verder moeten partijen die aan overheden netwerkdiensten aanbieden genoemde filtering toepassen. Overheden die deze diensten zelf uitvoeren en beheren moeten deze acties uiteraard zelf uitvoeren. Hierbij wordt aangemerkt dat hier tijdens de initiële uitrol en evaluatiefase van kan worden afgeweken ten behoeve van monitoren en testen van de effecten. BGP Routering valt terug op bestaande (onbeveiligde) routering als RPKI wegvalt. Er is geen onderbreking van de routering te verwachten wanneer RPKI data niet beschikbaar is.

RPKI Route Origin Validation dient te worden toegepast conform RFC 6811[6], waarbij gebruik gemaakt kan worden van de operationele ervaring zoals beschreven in sectie 5 van RFC 7115[7], en in het hoofdstuk "validating routes" van "https://rpki.readthedocs.io", een RPKI-documentatie project geschreven door leden van de Internet-gemeenschap.[8]

5.2 Hoe is het proces verlopen?

Het proces is goed verlopen. NLnet Labs heeft begin februari 2019 aangemeld voor plaatsing op de 'pas toe of leg uit'-lijst. De procesbegeleider (Lost Lemon) heeft op 10 april 2019 een intakegesprek gevoerd met de indiener. Op basis van de intake heeft het Forum Standaardisatie op 12 juni 2019 besloten RPKI in procedure te nemen. Zie hoofdstuk 2 voor een nadere toelichting op het verloop van het proces.

5.3 Hoe scoort de standaard op de toetsingscriteria?

Open standaardisatieproces

RPKI specificatie wordt beheerd door de IETF. De ontwikkeling en het beheer van RPKI is op een open, onafhankelijke, toegankelijke, inzichtelijke, zorgvuldige en duurzame wijze ingericht.

Toegevoegde waarde

Aangetoond is dat RPKI voldoende toegevoegde waarde heeft als standaard. RPKI is bedoeld ter beveiliging van de routing informatie op het internet. Er is geen directe relatie met andere standaarden die gaan over het beveiligen van het netwerkverkeer zelf (HTTPS en DNSSEC bijvoorbeeld). RPKI werkt complementair op reeds opgenomen standaarden.

---

[3] https://www.computable.nl/artikel/opinie/infrastructuur/6526971/1509029/de-on-veiligheid-van-de-routetabel.html, https://tweakers.net/nieuws/131133/phishingcampagne-gericht-op-myetherwallet-heeft-13000-euro-opgeleverd.html, https://rpki.readthedocs.io/en/latest/rpki/resources.html#examples-of-bgp-hijacks

[4] https://zoek.officielebekendmakingen.nl/ah-tk-20142015-3181.html

[5] https://www.volkskrant.nl/wetenschap/ip-adressen-ministerie-gekaapt-door-bulgaren~b75ad982/

[6] RFC 6811 https://tools.ietf.org/html/rfc6811 | BGP Prefix Origin Validation

[7] RFC 7115, sectie 5: https://tools.ietf.org/html/rfc7115#section-5

[8] Validating Routes: https://rpki.readthedocs.io/en/latest/rpki/using-rpki-data.html#validating-routes

Bij de implementatie van RPKI kunnen er risico's op het gebied van beschikbaarheid ontstaan. De experts roepen NCSC op om in samenhang met het implementatieadvies van NLnet Labs waar nodig aanvullend te adviseren over de beveiligingsrisico's. De NCSC verwijst als reactie hierop naar het nog door NLnet Labs te schrijven implementatieadvies.

Draagvlak

RPKI kan rekenen op voldoende draagvlak bij de overheid en marktpartijen. RPKI is ontworpen voor het beveiligen van externe routing-systeem. Interne netwerken (bv. Diginetwerk) kunnen op een andere manier beveiligd worden, maar er zijn wel mogelijkheden om RPKI toe te passen voor interne routing-systeem.[9] Ook de Kamer van Koophandel heeft in de consultatieronde aangegeven de opname te ondersteunen.

Opname bevordert de adoptie

Door de experts is aangegeven dat opname op de lijst nodig is om de adoptie te vergroten. er is op dit moment genoeg tractie voor de standaard voor breed gedragen adoptie. Het publiceren van ROA's gebeurt al op veel plekken. Het valideren wordt nog in mindere mate toegepast. Met plaatsing op deze lijst wordt verder gebruik gestimuleerd voor zowel publiceren als valideren.

5.4 Wat is de conclusie van de expertgroep en de consultatie?

Conclusie van het expertonderzoek

De experts adviseren om de standaard RPKI op te nemen op de 'pas toe of leg uit'-lijst.

Analyse van reacties uit de openbare consultatie

Uit de consultatie is één reactie naar voren gekomen vanuit de Kamer van Koophandel. Deze reactie was positief over de opname van RPKI.

5.5 Welke additionele adviezen zijn er ten aanzien van de adoptie van de standaard?

De expertgroep adviseert het Forum Standaardisatie en OBDO om bij de opname op de 'pas toe of leg uit'-lijst de volgende oproepen ten aanzien van de adoptie van RPKI te doen:

- Aan NLnet Labs om advies en documentatie over het gebruik van RPKI te communiceren. Dit geldt voor zowel het faciliteren van online documentatie als het adviseren van het gebruik van RPKI[10].

- Aan experts van de standaard RPKI om het Forum Standaardisatie actief te informeren over beschikbare vervolgstappen op het gebied van Route Origin Validation. De experts monitoren het speelveld van RPKI en zullen het Forum Standaardisatie actief informeren bij nieuwe ontwikkelingen.

- Aan Rijkswaterstaat om in de verlenging van de Rijksbrede internetdiensten (het ON2013 raamcontract: https://on2013.nl/) toepassing van RPKI van leveranciers te vereisen.

- Aan het Forum Standaardisatie om te monitoren op de juiste toepassing van de standaard, met name op het publiceren van ROA's en het valideren met het principe "invalid = reject".

    - Het Platform Internetstandaarden wordt opgeroepen om monitoring van RPKI publicaties te faciliteren via het platform internet.nl

- Aan RIPE NCC om in gesprek te gaan met partijen over de invulling en intensiveren van cursussen over RPKI met partijen die hierin geïnteresseerd zijn.

[9] https://vincent.bernat.ch/en/blog/2019-bgp-host-rpki
[10] https://rpki.readthedocs.io

6. Referenties

[1] Expertadvies RPKI:
https://www.forumstandaardisatie.nl/sites/bfs/files/Expertadvies-RPKI.pdf

[2] Reacties uit de consultatieronde RPKI:
https://www.forumstandaardisatie.nl/sites/bfs/files/Commentaar-uit-de-openbare-consultatie-RPKI.pdf