PREUREDITEV JAVNEGA STORITVENEGA NASLOVNEGA PROSTORA OMREŽJA DRŽAVNIH ORGANOV

Avtorji:

mag. Aleksander Boh, Ministrstvo za notranje zadeve aleksander.boh@gov.si

Rok Hlavaty, Ministrstvo za notranje zadeve rok.hlavaty@gov.si

mag. Matevž Mesojednik, Astec d.o.o. matevz.mesojednik@astec.si

Polona Antončič, NIL d.o.o. pantoncic@nil.si

Povzetek

Direktorat za informatiko in e-storitve pod okriljem Ministrstva za notranje zadeve je v prvi polovici koledarskega leta 2013 uspešno zaključil zahtevno in vsebinsko obsežno nalogo preureditve IPv4 naslovnega prostora prostranega omrežja državnih organov. Urejeni novo pridobljeni neodvisni naslovni predstavlja temelj vsem na zunaj dostopnim aplikativnim, podpornim in transportnim javnim storitvam ter bodočim storitvam oblaka javne uprave, ki jih omrežje HKOM ponuja svojim uporabnikom, državnim organom in državljanom Republike Slovenije. Zaradi ključnih komponent, kot sta varnost in neprekinjena dosegljivost storitev omrežja HKOM, je bila izrednega pomena skrbna in tehnično utemeljena razdelitev novega naslovnega prostora.

V prispevku, razdeljenem v dva dela, so predstavljeni sinergijski učinki konsolidacije MNZ javnega storitvenega prostora omrežja državnih organov. Strnjena so strokovna priporočila in izkušnje pri načrtovanju zahtevnih posegov na uspešnem primeru HKOM. V prvem delu je predstavljena osnovna struktura in zahteve robnih storitvenih segmentov omrežja HKOM, naročnikov pogled na optimizacijo in preureditev javnega naslovnega prostora ter vplivi na njegove uporabnike. V drugem delu so s strani ekspertnega zunanjega konzorcija izvajalcev predstavljeni tehnični izzivi in obsežnost z naročnikom usklajenega poteka aktivnosti projekta. V prispevku so povzeti inovativni tehnični pristopi in uporabljene metode preštevilčenja storitvenega omrežja HKOM.

Namen

Srednjeročna obveza Ministrstva pristojnemu internetnemu registru je bila sprostitev starega javnega IPv4 naslovnega prostora in zamenjava z novim, po velikostnem razredu enakim IPv4 naslovnim ekvivalentom. Pri tem je preštevilčenje javnih storitev Ministrstva in državnih organov predstavljajo le postranski cilj sicer širše zasnovane projektne naloge preureditve naslovnega prostora. Prvenstveni dosežki Direktorata za informatiko in e-storitve so bili konsolidacija ponekod manj učinkovito razdeljenega IPv4 naslovnega prostora, vzpostavitev priporočenih postopkov nadaljnje delitve mrežnih rezervacij in pomenska naslovna razporeditev obstoječih podpornih in aplikativnih servisov. Ključna pridobitev po zaključku IPv4 preštevilčenja je avtonomno ter posledično zanesljivejše storitveno okolje, ki

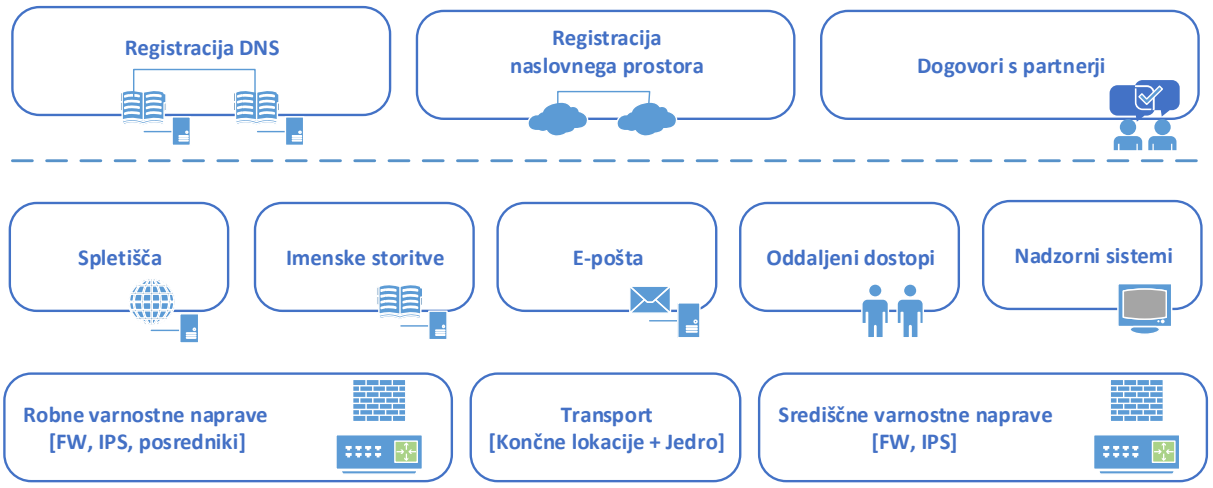
je osnovano na od ponudnika ISP neodvisnem naslovnem prostoru (angl. Provider Independent).

Uporabljene metode in izhodišča

Aktivnosti preureditve javnega naslovnega prostora so bile v sestavi projektne skupine DIES in konzorcija zunanjih izvajalcev razdeljene v več vsebinsko povezanih projektnih faz. V nadaljevanju povzemamo tehnične in organizacijske korake preštevilčenja javnih podpornih in storitvenih gradnikov omrežja HKOM, ki so kot taki lahko vodilo ter praktična usmeritev bralcu in tehničnim skrbnikom, po obsegu sorodnih informacijskih sistemov.

V prvem delu preureditve naslovnega prostora je bil revidiran celovit popis HKOM javnih storitev, posameznih skrbništev in medsebojnih odvisnosti. S tem je bilo mogoče kakovostno pripraviti razdelitev novega naslovnega prostora, ki je bila prirejena kratko- in srednjeročni viziji razvoja storitev omrežja HKOM. Postopek je kot prvo vseboval analizo obstoječega stanja in potreb po dejanski zasedenosti obstoječega naslovnega prostora ter predloge in dogovore o možni širitvi in rezervaciji možnih dodatnih širitev zahtev po javnih naslovih. Pomembno vlogo pri vodenju ažurne evidence optimalneje razpršenega naslovnega prostora je imela vzpostavitev referenčne translacijske tabele. V ta namen je bila implementirana avtomatizirana programska rešitev, ki je vsebovala na eni strani dogovor o prevajanju starih mrežnih naslovov v novi naslovni prostor, na drugi strani pa tudi interakcijski mehanizem potrjevanja ustreznosti posameznih preslikav s strani naročnika ali skrbnikov dotičnih storitev. Namen in uporaba translacijske tabele sta bila v zaključku prve faze projektne naloge predstavljena nosilcem posameznih storitvenih podsklopov omrežja HKOM in zunanjim izvajalcem, ki so bili neposredno ali posredno vključeni v nadaljnje aktivnosti preurejanja HKOM naslovnega prostora.

Uskladitvi enoumno in učinkoviteje razporejenih HKOM storitvenih segmentov je sledila projektna faza nizkonivojskega načrtovanja. Vodilo pri pripravi načrtov, ki so bili strnjeni po posameznih storitvenih sklopih (npr. središčno in transportno omrežje, robni varnostni gradniki, končne lokacije …), je bilo minimiziranje morebitnih motenj v prehodnem obdobju selitve domovanja storitev.



Slika 1: Storitveni in izvedbeni podsklopi preureditve naslovnega prostora HKOM

Ključno vlogo pri načrtovanju sprememb in teh vplivov na storitveno razpoložljivost je imelo skrbno snovanje sosledja aktivnosti in vnaprejšnje komunikacije s pristojnimi tehničnimi skrbniki. Nizkonivojski načrti so med drugim vsebovali:

- potrebne izpolnjene predpogoje za domovanje storitev na novem naslovnem prostoru,
- priporočeno časovno zaporedje izvedbe posameznih tehničnih ali operativnih aktivnosti,
- koračne scenarije potrditve delovanja storitev s strani nosilnega izvajalca (zunanji izvajalec, naročnik ali skrbnik) dotične storitve in tudi
- komunikacijska priporočila s primeri obvestil skrbnikom končnih subjektov (organi, Ministrstva, skrbniške skupine)
- komunikacija in obveščanje zunanjih organov in organizacij (zunanji izvajalci, pogodbeni partnerji) z informacijami in nameni sprememb dostopnih točk.

Načrtovanje in izvedba

Načrtovalne in izvedbene aktivnosti preureditve HKOM javnega naslovnega prostora so vključevale tesno sodelovanje projektne skupine z zunanjimi inštitucijami. V nadaljevanju navajamo opravljene zunanje postopke in izvedbene aktivnosti projektne skupine.

Nosilec novega naslovnega prostora je moral za uspešno vključitev opraviti ustrezne zunanje postopke, ki se tičejo:

- registracije in ureditev naslovnega prostora ter vzdrževalnih objektov pri evropski organizaciji za upravljanje z javnim naslovnim prostorom (RIPE)
- usmerjanja naslovnega prostora na strani ponudnikov internetnega dostopa

- registracije povratnih (PTR) DNS zapisov za ta naslovni prostor
- registracije sprememb vseh DNS strežnikov, ki so objavljeni v tem naslovnem prostoru

Za skrbnike HKOM javnih spletišč so bila že v fazi načrtovanja oblikovana skrbniška navodila s podrobnim opisom priporočenih korakov prehoda podpornih strežnikov in na njih gostujočih spletišč v preurejen naslovni prostor. Potreben izpolnjen pogoj pred spremembo omrežnih in sistemskih nastavitev spletišč so bile predhodno podvojene konfiguracije na nosilnih transportnih, varnostnih in imenskih gradnikih središčnega in robnega dela omrežja HKOM. Pri tem velja poudariti, da je tovrstna predpriprava lahko učinkovita le do mere, ki tehnološko in izvedbeno takšno dvodomnost dopušča.

Med spremembe, pri katerih so lahko bile konfiguracije pripravljene že vnaprej, smo v prvem delu izvedbene faze uvrstili podvojitev vseh imenskih zapisov v zunanjih DNS strežnikih (A zapisi), podvojitev objektov in pravil varnostne politike na središčnih in robnih požarnih pregradah, podvojitev dostopovnih varnostnih pravil oddaljenih VPN dostopov ter podvojitev restriktivnih konfiguracij in izjem na sistemih za preprečevanje vdorov.

Manevrski prostor vnaprejšnjih sprememb je bil ožji v storitvenih in transportnih segmentih omrežja, ki celovite dvodomnosti že z naslova uporabljenih tehnologij ali narave protokolov ne omogočajo. V nadaljevanju navajamo le nekaj takšnih primerov:

- konfiguracije privzetih prehodov na mrežnih, varnostnih in strežniških napravah;
- prevajalna pravila realnih ciljev ali prevedenih virov mrežnih preslikav (npr. NAT);
- izvorni naslov zastopniških (proksiranih) storitev;
- prilagoditev naprav in storitev, ki ne omogočajo dvojnega oštevilčenja storitve ali omrežnega vmesnika.

Posebej obravnavan tako tehnični kot tudi koordinacijski izziv v izvedbeni fazi HKOM preštevilčenja so predstavljale obstoječe konfiguracije informacijskih ter komunikacijskih virov, ki niso v neposredni domeni upravljanja tehničnih skrbnikov MNZ ali v administrativnem dosegu izvajalca. Konkretni primeri so specifične konfiguracije storitev ter sistemov, ki se v svojem drobovju sklicujejo neposredno na mrežne naslove, restriktivne politike zunanjih subjektov (organi, končni uporabniki, zunanji partnerji), ki v smeri odhodnih komunikacij dovoljujejo le poznane cilje (npr. na stare IPv4 naslove). S proaktivnim obveščanjem končnih uporabnikov s strani tehničnih skrbnikov naročnika ter izvajalca in z uporabo diagnostičnih orodij na nivoju robnih požarnih pregrad so bili tovrstni dostopi enoumno identificirani, dotični subjekti pa tudi ustrezno obveščeni. Pomemben rezultat celovite preureditve naslovnega prostora v omrežju MNZ gostujočih storitev je bilo prav revidiranje nosilcev tovrstnih konfiguracij in osveščanje zunanjih tehničnih skrbnikov, ki so takšne konfiguracije prilagodili v skladu s priporočeno prakso.

Zaključek

Uporabljeni pristopi preureditve javnega naslovnega prostora ter storitveno in komunikacijsko obsežnega omrežja javnih organov ponujajo preizkušeno metodologijo in priporočila organizacijam, ki se soočajo s tovrstnim izzivom. Ekspertiza in pridobljene izkušnje projektne skupine v sestavi Ministrstva in konzorcija zunanjih izvajalcev so lahko koristno vodilo načrtovalcem IT velikih kot tudi srednje velikih informacijsko-komunikacijskih sistemov.

Posredni učinek preureditve MNZ naslovnega prostora, ki v prispevku ni eksplicitno omenjen, pa mu pripisujemo pomembno vrednost, je sinergijski. Aktivno sodelovanje skrbniških skupin izvajalca, tehničnih skrbnikov HKOM omrežja in zunanjih partnerjev je razširilo vzajemno bazo znanja med strokovnjaki različnih področij. Ta je lahko odlično izhodišče nadaljnjega uresničevanja vizije omrežja javnih organov v smeri zagotavljanja neprekinjene zanesljivosti omrežja in storitev, zagotovitve sobivanja na novi verziji internetnega protokola (IPv6) in ponudbe storitvenega oblaka javne uprave.