21. marec 2012

Hotel Kompas, Kranjska Gora
Borovška cesta 100, Kranjska Gora,
Slovenija

Konferenca Arnes 2012

20 LET INTERNETA LJUDI

Zbornik člankov

Kazalo

Konferenca Arnes 2012 – 20 let interneta ljudi

Konferenca Arnes povezuje uporabnike s področja izobraževanja, raziskovanja ter kulture in je namenjena širokemu krogu obiskovalcev, saj pokriva tako uporabniške kot tudi sistemske vidike uporabe novih tehnologij.

V letu 2012 Arnes praznuje 20 let svojega delovanja. V teh 20 letih smo bili priča izjemnemu napredku internetne infrastrukture in storitev, prihodnost pa nam napoveduje »internet stvari«. Vendar smo ljudje tisti, ki nam ta tehnologija omogoča vedno lažje sodelovanje, in prav naše sodelovanje rodi razvoj vedno boljše tehnologije. Zato bi vas ob tej obletnici radi spomnili, da teh dvajset let gradimo omrežje ljudi, ne le žic. Na tokratni konferenci si bomo ogledali, kako smo internet uporabljali v njegovih začetkih in kaj nas čaka v prihodnosti, poseben poudarek pa bomo dali storitvam, ki nam pri naših aktivnostih lahko pomagajo že danes.

Skupno druženje na plenarnih predavanjih bomo začeli s predstavitvijo slovenskega izobraževalnega in raziskovalnega omreževanja ter takoj nato pogledali, kaj lahko na tem področju pričakujemo danes ali v prihodnosti.

Če smo pred 15 leti za medsebojno komunikacijo na spletu uporabljali IRC, se danes vse pogosteje srečujemo na družbenih omrežjih, pri tem pa pozabljamo, da so ta omrežja večinoma v lasti velikih korporacij, ki služijo z našimi podatki. Tako si bomo v nadaljevanju najprej osvežili spomin ter ogledali, kako se družbena omrežja dejansko uporabljajo pri nas. Pri tem bomo odprli tudi vprašanje zasebnosti, na katerega pri uporabi tovrstnih omrežij praviloma vse prepogosto pozabljamo. Na področju družbenih omrežij smo vedno bolj aktivni tudi na Arnesu, kjer bomo predstavili novi video portal, pri katerem boste natančno vedeli, kje so shranjeni vaši podatki.

Kar nekaj uporabnikov naših storitev že s pridom uporablja spletno identiteto AAI, od leta 2012 naprej pa bo ta uporaba še lažja in enostavnejša. Prav tako pa boste lahko izvedeli, kako svoje omrežje zaščititi pred nepridipravi in kako lahko uspešno ozaveščate o varnosti na svoji organizaciji tudi sami.

Sistemski administratorji boste tokrat na strokovno usmerjenih predavanjih lahko spoznali nove možnosti povezovanja ter podrobneje spoznali načine, kako v času recesije iz obstoječe povezave iztisniti kar največ, kar se le da. Spoznali boste tudi različna orodja, s katerimi si lahko pomagate pri upravljanju omrežij ali kako svoje omrežje še pred tednom IPv6 pripravite na novi protokol. Uporabniki storitev in vodstveni delavci boste v tem času lahko izvedeli več o možnostih povezovanja v omrežje ARNES in spoznali, kako si boste lahko nov elektronski naslov odprli kar sami. Sklop in s tem konferenco bomo zaključili s pregledom novosti na že obstoječih in predstavitvijo novih Arnesovih storitev.

Upamo, da tudi tokratna konferenca ne bo zgolj popotovanje čez zgodovino, sedanjost in prihodnost interneta, temveč prav tako odlična priložnost za izmenjavo izkušenj s področja IKT in prijetno druženje s stanovskimi kolegi. Predvsem pa si želimo, da vaša uporaba interneta in njegovih storitev zaradi nenehnih sprememb in novosti ne bo stresna, temveč prijetna in koristna.

ARNES 2012 conference – 20 years of the internet of people

The ARNES conference brings together users in the fields of education, research and culture, and is aimed at a wide range of visitors, covering both user and systems aspects of the use of new technologies.

In 2012, ARNES celebrates its 20th anniversary. In that time, we have witnessed exceptional progress in internet infrastructure and services, with the future promising an “internet of things”. But it is people who cooperate more easily thanks to this technology, and it is precisely such cooperation that gives rise to ever improving technologies. We would therefore like to use this anniversary to recall that for twenty years we have been building a network of people, not just wires. At this year's conference, we will look back at how we used the network in the early days and look forward to future developments, with particular emphasis on services that even today can help us in our activities.

Plenary talks will start with a presentation of Slovenian education and research networking, followed immediately by a review of what we can expect in this field today and in the future.

Whereas 15 years ago we used IRC to communicate over the web, today people increasingly meet on social networks, forgetting that social networks are mostly owned by large corporations which exploit our data. We will continue by refreshing our memories and reviewing how social networks are actually used in Slovenia. In doing so, we will also raise the issue of privacy, which we all too often neglect when using social networks. Here at ARNES we are also increasingly active in the area of social networks, and will launch a new video portal, which will explain exactly where your data are stored.

Quite a number of our service users are already benefiting from the use of AAI web identities, and from 2012 it will be easier and simpler to do so. You can also learn how to protect your network against miscreants and how you can successfully provide information on security in your organisation.

In the professional talks, systems administrators can learn about new connection options and detailed information on ways to make the most of existing connections at a time of recession. You will also learn about various tools you can use to help manage networks or ahead of IPv6 week to prepare them for the new protocol. Service users and management staff will also be able to learn more about the options for connecting to the ARNES network and how they can set up new electronic addresses themselves. This section, and the conference as a whole, will close with a review of innovations in existing ARNES services, as well as a presentation of new services.

We hope that once against this conference will be more than just a trip through the past, present and future of the internet, instead providing a decisive opportunity to exchange experience in ICT, as well as a chance to socialise with professional colleagues. We particularly want to ensure that your use of the

internet and internet services is pleasant and beneficial, and not stressful because of continual changes and innovations.

Avgust Jauk,
Arnes

Mejniki v slovenskem izobraževalnem in raziskovalnem omreževanju
Milestones in Slovenian education and research networking

Povzetek

Se še spomnite, kakšno je bilo prvo omrežje v Sloveniji in kako se je imenovalo? Katere storitve so bile takrat na voljo? Kako nam je uspelo prehoditi dolgo pot od nekaj kilobitnih povezav do današnjih optičnih zvez, ki omogočajo več 10 gigabitov ter kakšne težave smo pri tem premagovali? Katere zahtevnejše storitve so s tem postale mogoče? Kje smo danes, kam gremo in kje so trenutno glavne ovire? Vse to in še kaj bo tema tega prispevka.

Ključne besede: Arnes, internet, Decnet, hibridno omrežje, virtualizacija, storitve v oblaku

Abstract

Do you remember what the first network in Slovenia was like, and what it was called? What services were available? How did we get from connections of a few kilobits to today's optical connections with speeds of tens of gigabits, and what difficulties did we overcome? What more demanding services became possible as a result? Where are we today, where are we headed, and what are the main obstacles? This presentation covers all this and more.

Key words: ARNES, Internet, Decnet, hybrid network, virtualization, cloud services

Uvod

Računalniška omrežja imajo v Sloveniji dolgo tradicijo. Niso se začela z uvedbo interneta, ampak že slabo desetletje prej – leta 1984, ko so sistemski inženirji vzpostavili prvi povezavi med glavnimi računalniki Instituta Jožef Stefan in NBS ter Univerze v Ljubljani in Univerze v Mariboru. Počasi je začelo rasti omrežje, ki je povezovalo obe univerzi, večino institutov in drugih javnih institucij ter tudi nekatera podjetja (Jauk, 2011). Zaradi uporabljene tehnologije proizvajalca Digital je bilo poimenovano kar Decnet. V tistem času je bilo to omrežje nekaj posebnega. Po svetu so sicer obstajala akademska omrežja ter omrežja posameznih korporacij, ni pa znan primer omrežja, ki bi sredi osemdesetih let povezovalo tako akademsko kot tudi poslovno okolje.

Omrežje Decnet je močno vplivalo na nadaljnji razvoj. Pridobivalo in širilo se je znanje o omrežnih tehnologijah, uporaba omrežnih storitev med raziskovalci in študenti ter kultura sodelovanja med posamezniki in institucijami. Le-to je kasneje omogočilo ustanovitev Arnesa in vpeljavo najmodernejših tehnologij in storitev v naše okolje.

V nadaljevanju članka je podrobneje opisan celoten proces razvoja omrežij in storitev v izobraževalno-raziskovalnem okolju, od Decneta pa vse do zmogljivega omrežja z bogatim naborom storitev, ki so nam na voljo danes.

Mejniki v razvoju omrežja

Povezave v našem prvem omrežju **Decnet** so bile za današnje razmere zelo šibke: od 1,200 kb/s do 19,2 kb/s. Toda za tiste čase to ni bila resna slabost, za tekstovne komunikacije je prepustnost namreč zadoščala. Glavni problem je bila geografska omejenost omrežja na področje Slovenije oz. Jugoslavije.

V osemdesetih letih prejšnjega stoletja ni bilo globalnega omrežja, kot ga poznamo danes, ampak je obstajala množica omrežij, zgrajenih na različnih tehnologijah. Če smo hoteli komunicirati npr. z raziskovalci v ZDA, smo morali poskrbeti za dvoje: za mednarodno povezavo ter za posebne omrežne elemente, imenovane prehodi (angl. Gateways), ki so omogočali komunikacijo z omrežji, zasnovanimi na drugih tehnologijah.

Mednarodno povezljivost v evropsko raziskovalno omrežje **IXI** smo leta 1989 dobili v okviru projekta Eureka8/Cosine, ki se mu je kot edina takrat »vzhodnoevropska« država pridružila tudi Jugoslavija. Omrežje IXI je bilo zgrajeno na osnovi protokola X.25. Prepustnost naše povezave je bila sprva 48 kb/s, kasneje pa smo jo nadgradili na 64 kb/s. Prehode do drugih omrežij so nam velikodušno omogočala druga akademska omrežja (do BITNET-a in interneta nemško omrežje – DFN, do UUCP pa švicarsko – SWITCH).

Novembra 1991 je bila, takrat še v imenu YUNAC-a – jugoslovanskega akademskega omrežja, v okviru Laboratorija za odprte sisteme na IJS s pomočjo nizozemskega fizikalnega inštituta Nikhef preko omrežja IXI vzpostavljena prva **povezava v internet**. S tem je bil izpolnjen predpogoj za začetek širitve interneta pri nas.

Z **ustanovitvijo Arnesa** 15. maja. 1992 je bil podan organizacijski okvir za vzpostavitev enotnega raziskovalno-izobraževalnega omrežja. Tehnične zahteve za hrbtenično omrežje so bile usklajene med Arnesom, IZUM-om, IJS in obema univerzama junija 1992. Določeno je bilo, da mora biti hrbtenica omrežja enotna, pokrivati mora tako potrebe knjižničnega informacijskega sistema KIS/SZTI, ki ga je gradil IZUM, kot tudi vse ostale storitve, potrebne v akademskem okolju. Podana je bila zahteva po hkratni podpori več protokolov: DECnet (faza IV in faza V oz. CLNS), X.25 in IP (Jauk, A., Baš, I., Bibič, S., Šoštarič, D., Vidmar, R., Wedam, M., 1992). V skladu s programom dela Arnesa za 1992 (Arnes, 1992) smo začeli z izgradnjo omrežja in širitvijo interneta po Sloveniji. Pri tem smo dosegli kar nekaj uspehov:

- še v okviru projekta KIS/SZTI, ki ga je vodil IZUM, je bilo doseženo bistveno povečanje prepustnosti povezav: med Ljubljano in Mariborom ter med glavnimi vozlišči v Ljubljani na 2 Mb/s, do Kranja ter do večine članic pa na 64 kb/s;
- junija 1992 smo (kot drugi v Evropi) od RIPE n.c.c. pridobili blok IP-naslovov in ga začeli dodeljevati članicam;
- julija 1992 smo vzpostavili vrhnji DNS za domeno .SI in začeli z registracijo slovenskih domen;

- novembra 1992 smo med prvimi v Evropi uvedli usmerjevalni protokol nove generacije BGP-4, ki je omogočal optimizacijo velikosti usmerjevalnih tabel v internetu in s tem njegovo nadaljnjo rast.

Sledilo je obdobje širjenja omrežja v večje slovenske kraje, povezovanja novih članic, na začetku iz raziskovalne in univerzitetne sfere ter knjižnic, kasneje pa vedno več iz srednjega in osnovnega šolstva. Hkrati z rastjo števila priključenih članic ter uvajanjem novih storitev so se večale tudi potrebe po zmogljivosti omrežja. Kmalu je bilo 2 Mb/s premalo. Potrebovali smo zmogljive in cenovno sprejemljive povezave. Slednje je bilo zaradi kroničnega pomanjkanja denarja še posebej pomembno. Podobno kot znotraj Slovenije, so se večale tudi potrebe po zmogljivejših mednarodnih povezavah. Na obeh področjih smo se začasno morali zadovoljiti z drago in kompleksno tehnologijo ATM, s katero smo dosegali prepustnosti do 155 Mb/s. Toda kmalu je bilo tudi to premalo. Edina rešitev je bila zakup optičnih vlaken, ki na enostaven način in relativno poceni omogočajo doseganje tako rekoč poljubne prepustnosti.

Zaradi zapoznele liberalizacije telekomunikacij v Sloveniji smo prve **optične povezave** v hrbtenici omrežja ARNES dočakali šele leta 2000, ko nam je pri Telemachu uspelo zakupiti optiko med vozlišči v Ljubljani. Še večji uspeh smo dosegli leta 2003, ko smo pri Stelkomu zakupili optična vlakna med vozlišči po Sloveniji. S postopno izgradnjo lokalnih privodov smo vse zakupljene povezave nadomestiti z optiko, preko katere smo s tehnologijo ethernet dosegli prepustnost 1 Gb/s.

Zaradi hitre rasti prometa je bila prepustnost 1 Gb/s na povezavi med Mariborom in Ljubljano kmalu premalo. Začasno smo s pomočjo cenene tehnologije CWDM vzpostavili tri vzporedne gigabitne povezave, v letu 2007 pa smo bili prisiljeni preiti na 10 Gb/s. To smo dosegli s pomočjo tehnologije **DWDM**, ki nam omogoča tako rekoč poljubne prepustnosti: med vozlišči omrežja lahko vzpostavimo več vzporednih povezav prepustnosti 10 Gb/s, po potrebi pa bomo lahko prešli tudi na večje prepustnosti – 40 Gb/s oz. celo 100 Gb/s.

Ker nam tehnologija DWDM omogoča vzpostavitev več vzporednih povezav, smo dobili **hibridno omrežje**, ki omogoča dve vrsti storitev:

- s pomočjo usmerjevalnikov prometa zagotavljamo IP-povezljivost z upoštevanjem prioritete posameznih vrst promet (QoS); od leta 2003 poleg IPv4 podpiramo tudi IPv6;
- za zahtevnejše uporabnike zagotavljamo namenske povezave točka–točka prepustnosti 1 Gb/s oz. 10 Gb/s.

Od leta 2007 je tudi naša mednarodna povezava vzpostavljena na osnovi zakupljenih optičnih vlaken ter tehnologije DWDM. V Ljubljani je vozlišče evropskega izobraževalno-raziskovalnega omrežja GÉANT, ki je z več povezavami prepustnosti 10 Gb/s povezano na Dunaj in preko Zagreba na Budimpešto. S tem smo po mnogih letih odpravili ozko grlo, ki ga je predstavljala skoraj ves čas polna mednarodna povezava. Ker je tudi omrežje GÉANT hibridno, lahko namenske povezave točka–točka zagotavljamo tako rekoč med poljubnimi izobraževalno-raziskovalnimi institucijami v Evropi in preko povezav do drugih kontinentov tudi širše.

Organizacije so se na vozlišča omrežja ARNES sprva povezovale zgolj z zakupljenimi vodi. Tehnologija je omogočala prepustnosti do 2 Mb/s. Ko je Telekom Slovenije uvedel ISDN in kasneje še DSL, smo za priklop oddaljenih članic uporabili tudi ti dve tehnologiji. Ponekod smo uporabili tudi dostop preko KTV-omrežij. Toda vse te tehnologije omogočajo zgolj zelo omejene prepustnosti. Le optična vlakna lahko ponudijo potrebne prepustnosti, žal pa marsikje niso na voljo, če pa so že, je njihova cena nerazumno visoka. Zato si je precej organizacij zgradilo **lastne optične povezave**.

Za razvoj interneta v Sloveniji je bila zelo pomembna tudi storitev klicnega dostopa za posameznike, ki ga je Arnes sprva omogočal preko analognih telefonskih linij, kasneje pa tudi preko ISDN. Danes je ta storitev v uporabi zgolj v komunikacijsko najbolj nerazvitih delih Slovenije, kjer nimajo nobene druge možnosti.

Pozabiti ne smemo na **SIX**, Slovenian Internet Exchange, ki je omogočil medsebojno povezovanje vseh slovenskih ponudnikov interneta. Ko smo ga vzpostavili februarja 1994, je bil eno prvih tovrstnih vozlišč v Evropi.

Mejniki v razvoju storitev

V omrežju Decnet smo uporabniki imeli na voljo presenetljivo širok nabor storitev, ki so, čeprav v nekoliko drugačni obliki, aktualne še danes: elektronska pošta, prenos datotek, diskusijske oz. novičarske skupine, oddaljen dostop do strežnikov in pošiljanje kratkih sporočil. Dokler nismo leta 1989 vzpostavili povezave v mednarodno akademsko omrežje IXI, smo bili pri tem omejeni na območje Jugoslavije. Potem pa se nam je odprla kopica novih možnosti. Prehodi, ki so nam jih nudila druga nacionalna akademska omrežja, so nam omogočali komunikacijo z uporabniki omrežij, zgrajenih na drugih tehnologijah: internetom, BITNET-om in omrežjem UUCP. S pomočjo elektronske pošte in posebnih prehodov smo lahko brskali po repozitorijih datotek na internetu in BITNET-u ter prenašali datoteke. Pomembno vlogo so odigrali tudi e-poštni sistemi za distribucijske liste. Najbolj znana med njimi sta bila RokPress in Pisma-bralcev.

Z uvedbo interneta sprva nismo dobili kopice dodatnih storitev (izjema je bil Usenet News), ker jih takrat na internetu še ni bilo. Res pa je, da za oddaljen dostop do strežnikov v internetu, prenos datotek in elektronsko pošto nismo več potrebovali nerodnih prehodov; seveda zgolj s sistemov, na katere smo naložili ustrezno programsko opremo. V začetku devetdesetih let so bili operacijski sistemi večinoma še brez podpore za internet. Za nekatere je bila na voljo brezplačna programska oprema, za večje sisteme pa jo je bilo treba kupiti. Ob uvedbi interneta smo poskrbeli tudi za lastne prehode med Decnetom in internetom.

Internet, kot ga nekateri razumejo danes in ga pomotoma celo enačijo s **spletom**, se je v Sloveniji začel s prvim spletnim strežnikom, ki so ga postavili na računalniškem centru Instituta Jožef Stefan (Oblak-Črnič, 2008). Spletna tehnologija se je zelo hitro razširila, z njo je bilo na voljo vedno več storitev, tudi takšne, kot smo jih poznali že od prej: novičarske skupine in forumi ter e-pošta. Zaradi rastočega zanimanja za to tehnologijo smo tudi gostujočim uporabnikom

na Arnesovem centralnem strežniku Stenar omogočili postavitev lastnih spletnih strani.

Večanje prepustnosti povezav v omrežju ARNES ter razvoj strojne in programske opreme je postopoma omogočil **multimedijske storitve**. Po prvih, zaradi nezrelih implementacij relativno nerodnih korakih v začetku tisočletja smo v letu 2003 ponudili podporo za večtočkovne videokonference po standardu H.323 in H.320 (videokonference preko protokola IP ter preko ISDN), kasneje pa tudi po standardu SIP. Članice so se začele opremljati s sobnimi videokonferenčnimi sistemi, ki so zagotavljali relativno kakovostno sliko in zvok. Kasneje smo dodali še sistem za snemanje H.323-videokonferenc ter podporo za videokonference visoke ločljivosti, najprej 720p, nato pa še 1080p. Leta 2010 smo dodali storitev spletnih konferenc – VOX, ki je zaradi enostavnosti uporabe multimedijsko komunikacijo približala širokemu naboru uporabnikov. V 2011 smo razvili in začeli s pilotnim delovanjem video portala – storitve videa na zahtevo, ki uporabnikom omogoča nalaganje lastnih video vsebin, ter portala za upravljanje centralnega sistema za večtočkovne videokonference H.323/SIP.

Zaradi vse večje **mobilnosti** raziskovalcev in kasneje tudi študentov je bilo treba poskrbeti za dostopnost do storitev od koder koli, in sicer na varen način in z minimalno količino administriranja. Le-to smo dosegli z vzpostavitvijo dveh storitev: storitvijo gostovanja pri dostopu do brezžičnega omrežja (**Eduroam)** leta 2004 ter storitvijo enotne prijave v spletne aplikacije (federacija **ArnesAAI**), ki je nadgradnja storitve eduroam, leta 2010. Storitvi omogočata uporabo istega uporabniškega imena tako za prijavo v omrežje kot v spletne aplikacije.

Razvoj mehanizmov za **virtualizacijo** ter večanje prepustnosti omrežnih povezav sta omogočila, da smo leta 2007 članicam ponudili možnost **gostovanja navideznih strežnikov** – GVS. Storitev smo postopoma dopolnjevali, tako da je sedaj na voljo v vseh treh oblikah **storitev v oblaku**: infrastruktura kot storitev (IaaS), platforma kot storitev (PaaS) in programska oprema kot storitev (SaaS). V slednji različici vsebuje v izobraževalnem okolju popularna CMS (Joomla) ter LMS (Moodle). V letu 2011 smo ponudili še eno storitev vrste IaaS – Arnes storage, ki članicam omogoča dostop do prostora na diskovnem sistemu, na katerega lahko shranjujejo svoje podatke. Ta storitev je zaradi velikih zahtev do omrežja na voljo zgolj članicam, ki imajo ustrezno zmogljivo povezavo v omrežje ARNES.

V letu 2010 smo vzpostavili testno gručo strežnikov na osnovi tehnologije **GRID**, ki slovenskim znanstvenikom omogoča spoznavanje s to tehnologijo za porazdeljeno izvajanje kompleksnih izračunov.

V 2011 in 2012 smo razširili nabor storitev v oblaku s poudarkom na **podpori skupinskemu delu** ter uporabi **enotne prijave**: ponudili smo storitev »blog«, ki omogoča enostavno postavitev dinamičnih spletnih strani tudi za posameznike, »planer« za usklajevanje terminov sestankov ter »filesender«, ki poenostavlja izmenjavo do 100 GB velikih datotek. Posameznikom, ki so na svoji domači organizaciji pridobili netID (uporabniško ime, ki je veljavno v federaciji ArnesAAI), smo ponudili spletni portal, na katerem si lahko ustvarijo uporabniško ime, gostujoče na Arnesu (guest.arnes.si), mu podaljšujejo veljavnost ter upravljajo nastavitve. S tem se izognejo zamudnim postopkom s papirnatimi prijavnicami in formularji za podaljševanje.

Zaključek

Z Decnetom se je začel relativno hiter in uspešen razvoj omrežja in storitev. Večali smo prepustnosti povezav, širili omrežje ter uvajali nove, zahtevnejše storitve. Včasih so storitve morale čakati na razvoj omrežja, drugič pa je omrežje čakalo na storitve, ki ga bodo zapolnile. Nenehno nas je spremljalo pomanjkanje finančnih sredstev in kadra. Ključno za uspeh pa je bilo sodelovanje med vsemi akterji.

Kaj nas čaka v prihodnosti? Vsekakor nadaljnji razvoj. Prihajajo še zahtevnejše storitve, povečan bo poudarek na orodjih za podporo skupinskemu delu, multimedijskih storitvah, zagotavljanju mobilnosti, storitvah v oblaku ter zmogljivejših in bolj prilagodljivih omrežnih povezavah. Pri snovanju rešitev ne smemo pozabiti na varovanje osebnih podatkov. Pomembno vlogo pri tem bo igral federativni pristop pri zagotavljanju storitev. Organizacije bodo storitve ponujale tudi uporabnikom iz drugih organizacij. Pri razvoju storitev bodo med seboj sodelovale. Pogoj za uspešen razvoj bo tudi v prihodnje dostop do optičnih vlaken ter spoštovanje principa odprtosti omrežja. Vsaj za izobraževalno-raziskovalno sfero je to zaradi potrebe po razvoju novih storitev ključnega pomena.

Eden od izzivov, ki ga moramo rešiti, je, kako storitve približati uporabnikom, kako jih pritegniti k sodelovanju pri njihovem razvoju ter kako zagotoviti ustrezen nivo podpore, med drugim s pomočjo izobraževanja IT-strokovnjakov v posameznih organizacijah. Pa smo spet pri sodelovanju, ki je za razvoj in zagotavljanje modernih naprednih storitev ključnega pomena.

Viri

1. Arnes, (1992): Program dela za leto 1992. Gradivo za 1. sejo Upravnega odbora Arnes,. 21. 9. 1992.
2. Prispevek v zborniku: Jauk, A. (2011): Medmrežje v Sloveniji – od začetkov do eksplozije interneta. V: Informacijska družba – IS 2011, Ljubljana.
3. Jauk, A., Baš, I., Bibič, S., Šoštarič, D., Vidmar, R., Wedam, M. (1992): Zahteve za bodočo slovensko akademsko mrežo, 24. 6. 1992.
4. Oblak-Črnič, T. (2008): O začetkih Interneta na Slovenskem, Javnost – The Public, št. 15, str. 151–174, Ljubljana.

Cees de Laat, University of Amsterdam

Internetne inovacije v podporo znanosti in izobraževanju
Internet Innovation to support Science & Education

Povzetek

Cees de Laat bo v svojem plenarnem govoru govoril o uporabi najsodobnejših omrežij pri podpori e-znanosti in mnogih prednostih omrežij ter e-infrastrukture za raziskovalce v številnih strokah. Na podlagi bogatih izkušenj iz projektov s področja fizike osnovnih delcev, radijske astronomije, projektiranja nasipov, medicinskih in drugih raziskav nam bo Cees de Laat predstavil, kako so se z inovacijami na področju omrežij razvile nove oblike in nove možnosti sodelovalnega raziskovanja.

Abstract

In his plenary address, Cees de Laat will talk about the use of state-of-the-art networking in support of e-Science and the great benefit of networking and e-Infrastructure to researchers in many disciplines. With experience from projects in high-energy physics, radio-astronomy, dike engineering, medical research, and more, Cees de Laat will show us how networking innovations enable research collaborations on a new scale with novel capabilities.

Jessica Willis, DANTE

Odprta pot za raziskovanje na evropski in svetovni ravni: prednosti sodelovanja Arnesa v omrežju GÉANT

Enabling European and global research: the benefits of ARNES participation in GÉANT

Povzetek

Na predavanju boste spoznali, kako uspešno delovanje Arnesa v omrežju GÉANT uporabnikom omogoča sodelovanje na mednarodni in svetovni ravni. Izvedeli boste, katere so prednosti za posamezne uporabnike Arnesa v Sloveniji in tudi za slovensko ter evropsko konkurenčnost v celoti, saj je projekt ključni del vizije EU o brezmejni coni za raziskave. Jessica bo predstavila primere uporabnikov, ki uporabljajo storitve omrežja GÉANT, in povedala, kako lahko uporabniki v Sloveniji v največji meri izkoristite dostop do omrežja GÉANT.

Abstract

Jessica will explain how ARNES successful participation in GÉANT enables its users to collaborate on a European and global scale. She will explain the benefits not only to individual ARNES users in Slovenia but as a key part of the EU's vision for a border-free zone for research and to Slovenian and European competitiveness as a whole. Jessica will give examples of users taking advantage of the GÉANT services and will explain how users in Slovenia can maximise the benefit they get from access to GÉANT.

Đulijana Juričič,
OŠ Trnovo

Kako smo vodili projekte s pomočjo IRC-a
IRC in on-line projects

Povzetek

Šole v Sloveniji so sodelovale z drugimi na državni in mednarodni ravni že pred obstojem sodobne informacijsko-komunikacijske tehnologije. Uvajanje in razvoj IKT sta intenzivno vplivala tudi na to področje delovanja šol. Navdušenost nad preprosto izmenjavo elektronskih sporočil je zamenjala potreba po kompleksnejših komunikacijskih storitvah, ki naj bi med drugimi omogočale ne le on-line komunikacijo, ampak tudi objavo različnih prispevkov in sporočil, ki bi bili dostopni vsem sodelujočim, izmenjavo le-teh, iskanje partnerjev itd. Ali ni to bistvo socialnih omrežij?

Abstract

Slovenian schools collaborated with other schools, both nationally and internationally, even before the existence of modern information and communication technology. The introduction and development of ICT have had a major impact on this aspect of schools' activities. Enthusiasm for the simple exchange of e-mail massages has been replaced by need of more complex communication tools which could enable not just online communication, but also publication and exchange of various material and messages accessible to all participants, finding partners tools etc. Is that not the essence of social networks?

Domen Savič, 5do9

Družabni splet in mi – medijski #TEHNODETERMINIZEM
The social web and us – Media #technodeterminism

Povzetek

Tehnologija se v medijskem poročanju vedno bolj prepleta z družbenim delovanjem posameznika. Vedno bolj je prisoten medijski tehnodeterminističen pogled, ki predpostavlja, da je tehnologija glavni generator družbenih sprememb oziroma da se spremembe v družbi dogajajo izključno in samo zaradi uporabe tehnoloških rešitev.

Ključne besede: Družabni splet, mediji, Twitter, Facebook, družba.

Abstract

Media reports suggest that technology is increasingly involved in society's social activities. Media reports reflect a strongly technodeterministic viewpoint, where social changes stem directly from the use of particular technologies.

Key words: Social web, media, twitter, facebook, society

Tehnologija je lastnost svojega uporabnika

Da je družbeno omrežje oziroma z angleškim izrazom social web vedno bolj prisotno v naši medijsko-politični sferi, ni ravno novica. Medijski prostor pravkar pretečenega leta 2011 je bil poln novic in zgodb o vse večji prisotnosti omrežij Facebook in Twitter, o nujnosti uporabe in o drastičnih posledicah abstinence.

Tehnodeterminističen vidik, ki ga je posvojila večina teh zgodb, nam ni tuj – tehnološka determiniranost komunikacijskih kanalov in orodij je prisotna že vsaj od srednjega veka naprej, ko so politični vladarji pravico do razmnoževanja intelektualnih vsebin neposredno povezovali z lastništvom orodij za razmnoževanje vsebin in ko se je rodil danes vsem znani »copyright«.

Zmožnost komuniciranja je torej danes v spletni sferi v veliki večini primerov neposredno povezana z znanjem uporabe orodji za komuniciranje in stroka orodjarjev skuša kot dominantno uveljaviti prepričanje, da je ravno znanje uporabe orodij tisto, ki šteje pri komuniciranju. Če torej ne znate uporabljati telefona, potem svojim sorodnikom RES nimate kaj povedati.

Prodaja tehnologij, brez katerih ni mogoče ustvarjati vsebin oziroma brez katerih ni mogoče komunicirati, je šla tako daleč, da se uporabnike orodij v medijih predstavlja kot člane iste interesne skupine, da se jih razume kot homogeno skupino z enakimi lastnostmi oziroma da se jim pripisuje enake družbene lastnosti. Le-to naj bi postali, ko so začeli uporabljati skupno tehnologijo, čeprav se sporočila, ideje o uporabi in dejanska raba po navadi od posameznega uporabnika do posameznega uporabnika zelo razlikujejo ali si celo nasprotujejo.

Vsa zgoraj našteta dojemanja spletnih komunikacijskih tehnologij vodijo v nevaren trend – relativizacijo človeške aktivnosti in poudarjanje tehnološkega elementa kot gonilnika družbenega napredka. V nadaljevanju bomo pregledali tri odmevne

zgodbe, ki so medijsko občinstvo še dodatno utrdile v prepričanju, da tehnologija definira uporabnike in da se brez nje družbeno pomembni dogodki ne bi mogli zgoditi.

#arabska_pomlad – neznosna lahkost tvitanja

Protivladne demonstracije, ki so v Alžiriji in Egiptu sprožile propad aktualnega političnega režima, se ne bi mogle zgoditi brez digitalnega smodnika in krogel v obliki omrežja Facebook in Twitter. Tako poenostavljene trditve smo lahko spremljali lansko leto spomladi, ko so se Egipčani in Alžirci podali na ulice in s fizično prisotnostjo strmoglavili svoje predsednike.

Redukcija kompleksne družbeno-politične revolucije, ki se je dogajala v državah z zelo nizko penetracijo spletnega dostopa (Egipt dobrih 20 %, Alžirija slabih 5 %) (Internet World Stats, 2012), novinarskim interpretom in analitikom ni preprečila, da ne bi zmage nad režimom z vso težo medijske resnice pripisali uporabi tehnologije.

V pregledu leta na najbolj branem medijskem portalu v državi lahko v članku beremo naslednje: »Zgodovino minulega leta so pisala gibanja, kot so Arabska pomlad, Gibanje 99 % in Occupy Wall Street – spontane revolucije, ki so se manifestirale na podlagi skupnih interesov, ki so jih skanalizirala prav družbena omrežja« (Rejc, 2011).

Čeprav so določeni mediji od organizatorjev protestov samih pridobili izjave, da tehnologija ni igrala osrednje vloge in da je bila samo neobvezni pripomoček, se prevladujoče mnenje v javnosti ni spremenilo – mediji so bili polni člankov o Twitter revoluciji in Facebook protestnikih, članki pa so bili podloženi s fotomontažami protestnikov in logotipov obeh storitev.

Tako so mediji skoraj v celoti ignorirali že prej omenjene nizke penetracije spletnega dostopa, relativne neizobraženosti demonstrantov oziroma dejstva, da so se demonstracije dogajale tudi takrat, ko so samodržci tehnologijo izločili iz enačbe oziroma ugasnili dostop do spleta (Egipt, januarja prejšnje leto) (Kvas, 2011).

#trenirke – še dobro, da imamo tehnologijo!

Da se lahko tudi Slovenci pohvalimo z lastno spletno revolucijo, je bilo očitno lanskega decembra, ko je neimenovana politična stranka na spletu objavila kolumno, na katero so prvi odreagirali ravno spletni uporabniki. Kolumna se je nanašala na rezultate aktualnih parlamentarnih volitev, zaradi enostavne uporabe in hitre narave tehnologije pa so se nanjo prvi odzvali nekateri spletni uporabniki. Ključna beseda v zadnjem stavku je NEKATERI.

Medijev to ni motilo in tako je npr. Dnevnik poročal, da so »med koncem tedna o trenirkah množično začeli pisati slovenski uporabniki družbenega omrežja Twitter. Poleg šaljivih, ciničnih in kritičnih komentarjev na račun Majerjevega zapisa so tviteraši sklenili, da se bodo v ponedeljek zvečer na Prešernovem trgu v Ljubljani dobili na pravcatem "trenirkameetu". Predpisano oblačilo – trenirka.«

Navidezna kohezivnost uporabnikov storitve Twitter (in ne ljudi, ki so protestirali neodvisno od uporabe tehnologije za izražanje tega protesta) je tako v javnosti

pustila vtis, da je Twitter skupnost ostro profilirana, družbeno zelo aktivna in levičarsko usmerjena, čeprav se jih je na dejanskem shodu zbralo bore malo.

Mediji o uporabnikih, ki so se udeležili spletnega oziroma fizičnega shoda, niso izbrskali nobene druge podrobnosti, čeprav so se na Prešernovem trgu zbrali tudi pripadniki organizacij (Legebitra, Liberalna akademija, Mirovni inštitut ...), ki niso bili udeleženi v slovensko Twitter sfero oziroma so prišli protest na Prešernovem trgu podpreti zato, ker so se identificirali s sporočilom protesta – ne pa tehnologijo, s pomočjo katere je bil protest uvodoma skomuniciran. Njih ni nihče nič vprašal.

Nekateri mediji so šli še dlje – poudarjali so, da se v primeru odsotnosti tehnologije Twitter protesti sploh ne bi zgodili; da je bila tehnologija potrebna ne samo kot organizacijsko, temveč tudi kot motivacijsko orodje, kar naj bi medijsko občinstvo prepričalo v vero o samozadostni tehnologiji, ki človeka sploh ne potrebuje več.

#virant – psevdodogodek, ki so ga pri življenju držali mediji

Če so bili odzivi na članek o volilni bazi zmagovalca volitev vsaj relativno povezani z družbeno aktivnostjo in so imeli jasen cilj izražanja nestrinjanja s politično držo stranke v državi, se je januarja 2012 na omrežju Twitter odvila t. i. akcija #virant, ki je dokazala obupano povezavo medijev z »novimi« tehnologijami in pokazala, da bodo tudi letos zelo verjetno mediji veliko bolj navdušeni nad tehnologijo sporočanja kot pa nad sporočilom samim.

#virant se je začel z enim uporabnikom. Za razliko od organizacije protesta v primeru #trenirke pri #virant ni šlo za politični protest oziroma usmerjeno komunikacijo proti določeni interesni skupini. Bila je preprosta šala, ki nikoli ni bila izoblikovana za tisto, kar je sledilo po njej.

V prvem koraku so jo pograbili različni slovenski uporabniki Twitterja. Po meritvah ekipe Sitweet, ki se ukvarja z analitiko družabnega spleta, je bilo v enem dnevu objavljenih blizu 2000 objav, ki so se navezovale na besedne igre #virant.

V drugem koraku so te uporabnike opazili mediji in jih, pričakovano, predstavili kot interesno skupino, čeprav smo lahko iz vsebine posameznih sporočil razbrali, da obstajajo vsaj tri skupine uporabnikov, ki so sodelovali.

V prvi skupini so bili tisti, ki so v #virant videli politični humor in zadeve niso jemali kot resen protest proti trenutnim družbeno-političnim razmeram. V drugi skupini so bili tisti, ki so namensko protestirali proti Gregorju Virantu kot politični figuri in niso imeli nobene povezave s prvo skupino. V tretji skupini so bili tisti, ki so akciji nasprotovali, a vseeno sodelovali v njej z glasnim nasprotovanjem.

Mediji so celotno komunikacijo predstavili kot politično motivirano in ignorirali drugi dve skupini. Šli so še korak dlje. Čeprav sem kot prvi uporabnik, s katerim se je #virant začel razvijati, od začetka pojasnjeval pravi razlog oziroma odsotnost razloga, je večina medijev moje izjave prilagodila tako, da pojasnila niso prišla do odjemalcev množičnih medijev.

#virant je tako iz popolnoma brezpredmetne komunikacije mutiral v komunikacijo z dvemi kritičnimi sporočili – mediji se ne zavedajo svojih vlog, vsebino pa

prilagajajo obliki sporočila. Hkrati je #virant izpostavil zelo efektivno distribucijo sporočil prek spleta, ki se dogaja brez komunikacijskega središča oziroma brez neposredne koristi za komunikatorje sporočila.

Kdo poganja koga?

Sodeč po medijskem portretiranju uporabnikov spletnih tehnologij lahko v prihodnosti pričakujemo konstantno medijsko izenačevanje družbenih skupin in uporabnikov tehnologije, ki bo v medijih s stereotipizacijo posameznega tipa uporabnika služila za poenostavljeno predstavljanje družbenih sprememb.

Hkrati se bo z vsako novo tehnologijo, ki se bo pojavila na trgu, hitro našel stereotip uporabnikov te tehnologije, toliko prej, če bodo tehnologijo uporabljale znane osebnosti oziroma medijsko zanimive interesne skupine. Stremeti je treba k medijski kontekstualizaciji socialnih sprememb, ki so se zgodile tudi s pomočjo tehnologij, ne pa izključno zaradi njih.

Viri in literatura:

1. Internet World Stats. (13.1.2012). Internet World Stats. Pridobljeno 13. 1. 2012 iz http://www.internetworldstats.com/stats1.htm.
2. Rejc, M. (2012). Pestro leto 2011 na Twitterju. Pridobljeno 13. 1. 2012 iz http://24ur.com/ekskluziv/zanimivosti/2011-na-twitterju.html.
3. Kvas, B. (2011). Egiptovsko sodišče je oglobilo Mubaraka zaradi izklopa dostopa do spleta. Pridobljeno 13. 1. 2012 s http://www.e-demokracija.si/2011/05/30/egiptovsko-sodisce-je-oglobilo-mubaraka-zaradi-izklopa-dostopa-do-spleta/.
4. Anderšek, A. (2011). Gibanje trenirk s spleta do vrha države. Pridobljeno 13. 1. 2012 z http://www.dnevnik.si/novice/slovenija/1042494937.

Mag. Andrej Tomšič, Informacijski pooblaščenec RS

Varstvo zasebnosti na internetu na poti od netransparentnih poslovnih praks do regulacije
Privacy protection on the internet on the road from non-transparent business practice to regulation

Povzetek

Spletni velikani, spletna oglaševalska industrija in nekatera inovativna start-up podjetja se na podlagi pritiskov varuhov zasebnosti počasi premikajo iz sistema naknadnega preklica (opt-out) v sistem vnaprejšnje privolitve v obdelavo osebnih podatkov (opt-in). Ali je opt-in sistem tisto ključno orodje, s katerim lahko posamezniku vrnemo pravico do odločanja o svojih osebnih podatkih, in ali se lahko nanj v popolnosti zanesemo?

Ključne besede: zasebnost, osebni podatki, spletna družbena omrežja, DPI, privolitev, opt-in, opt-out.

Abstract

Major web companies, the web advertising industry and some innovative start-ups, facing recurrent pressures from privacy advocates, are slowly shifting from opt-out to opt-in regimes for processing personal data. Is opt-in the key tool that can restore users' power of control of our personal data, and can we fully rely on this concept?

Key words: privacy, personal data, social networks, Deep Packet Inspection, consent, opt-in, opt-out.

»Najprej ocenijo, ali lahko uporabniki in regulatorji ugotovijo, kaj v resnici počnejo s podatki. Nato presodijo, ali se bodo ljudje začeli množično odjavljati z njihove storitve, in ocenijo, kakšne so možnosti tožbe. Če so tveganja zanemarljiva, bodo zakone pač prekršili.« Tako je modus operandi večjih internetnih podjetij, kot sta Google in Facebook, v intervjuju Lenartu J. Kučiću pojasnil avstrijski študent prava Max Schrems, ki ga je omenjeno stanje dovolj vznemirilo, da se je spustil v boj z mlini na veter. In uspel. Na podlagi zahteve za seznanitev z lastnimi osebnimi podatki – ene temeljnih pravic posameznika po evropski zakonodaji o varstvu osebnih podatkov – je dobil za dobrih 1200 strani svojih osebnih podatkov in irskemu informacijskemu pooblaščencu (Facebook ima v Dublinu svojo podružnico) podal 22 prijav kršitev irskega zakona o varstvu osebnih podatkov. Schrems je zaključil, da kot onesnaževanja ni več mogoče zagovarjati z argumentom, da so okoljski standardi nepraktični, dragi in da znižujejo konkurenčnost onesnaževalcev, tudi ni več razloga, zakaj ne bi smeli od internetnih podjetij zahtevati, naj spoštujejo zakone, poslujejo transparentno in upoštevajo pravice uporabnikov, ne pa da jih obravnavajo zgolj kot surovine, na katerih temeljijo njihovi poslovni modeli.

Schremsove ugotovitve lahko povsem enostavno potrdimo sami. Se spomnite storitve Facebook Beacon? Beacon je bil del Facebookovega oglaševalskega sistema, pri čemer so se podatki o uporabi 44 drugih spletnih mest posameznikov (npr. nakupi na eBayu) prikazovali na njihovem zidu. Posamezniki se pred tem

seveda niso kaj dosti strinjali, saj jim je bila dana zgolj možnost naknadnega odstopa od uporabe (t. i. opt-out). Po obsežnem nasprotovanju v javnosti je bila storitev umaknjena septembra 2009, Facebookov ustanovitelj Mark Zuckerberg pa je nato izjavil, da je bil Beacon napaka. Opisani primer lepo kaže ustaljeno prakso poskusov, v smislu »ali bo šlo čez«. V tej luči je tudi opazen počasen prehod iz sistema poznejšega odstopa (opt-out) v sistem vnaprejšnje privolitve (opt-in). Sistem opt-out so tako posamezniki kot varuhi zasebnosti že dalj časa zamerili Facebooku, ki se je nanj zanašal pri marsikateri svoji funkcionalnosti, npr. pri dodajanju prijateljev v skupine brez njihove vnaprejšnje privolitve ali pri označevanju (t. i. tagging). Z vidika varstva osebnih podatkov je treba poudariti, da je razlika med omenjenima sistemoma ogromna in da vsaj evropska zakonodaja omogoča obdelavo osebnih podatkov praviloma na podlagi zakona ali osebne privolitve (torej opt-in), sistem opt-out pa je kvečjemu izjema in ga je moč zaslediti le na tistih področjih, kjer bi bilo vztrajanje pri sistemu opt-in nesmiselno, nesorazmerno ali celo neizvedljivo, npr. pri neposrednem trženju po navadni pošti in telefonu ali pri izvajanju videonadzora. V letih so z nekakšno prikrito legalizacijo opt-outa s pomočjo piškotkov uspešno poslovali tudi oglaševalci na internetu, saj nas nihče predhodno ni vprašal, ali dovolimo namestitev piškotkov na svoj računalnik in jih lahko le blokiramo in pozneje brišemo.

In kakšna je razlika med opt-in in opt-out? Da gre pri opt-out in opt-in za dva izrazito različna sistema lepo opozarja primer iz čisto drugega sveta – doniranje organov. Študija, ki sta jo izvedla Johnson in Goldstein, je namreč ugotovila, da se v večini držav stopnja doniranja organov ustali bodisi okrog 20 odstotkov bodisi okrog 80 odstotkov populacije. Sprva je kazalo, da so krive kulturne razlike, kar pa ni pojasnilo ogromne razlike med Švedsko (85,9 %) in Dansko (4,25 %). Ugotovili so, da ima že samo način, kako je postavljeno vprašanje, izrazit vpliv na rezultate in tako so imeli v državah z nizkimi odstotki donacij organov sistem opt-in, kjer je morala oseba sama izraziti to željo, tiste z visokimi deleži pa so uporabljale opt-out – če nisi reagiral nasprotno, si se uvrstil med donatorje. Da, eno samo potrditveno okence lahko pomeni bistveno razliko.

Nadvse zgovoren primer, ki nakazuje na razliko med opt-out in opt-in, prihaja iz ZDA, kjer se je ponudnik internetnega dostopa Embarq odločil, da se bo povezal s podjetjem NebuAd, in sicer bo NebuAd izvajal vedenjsko trženje na podlagi dostopa do podatkov o spletnih aktivnostih uporabnikov internetnega dostopa Embarq.[1] Testiranje delovanja sta pogodbena partnerja zavila v politiko zasebnosti, ki je bila dolga 5000 besed, uporabnikov pa posebej niso obvestili o tem, da bodo z določenim dnem podvrženi testiranju NebuAd-ove tehnologije. Uporabnikom je bila dana možnost, da pozneje zavrnejo takšno spremljanje spletne aktivnosti, in sicer prek povezave, ki je bila bolj ali manj skrita v prej omenjeni politiki zasebnost. Rezultat je bil zelo zgovoren – možnost zavrnitve spremljanja spletne aktivnosti, torej opt-out, je izkoristilo le 15 od 26.000 naročnikov Embarqa, ki so bili vključeni v testiranje. Torej je le 0,06 % uporabnikov izkoristilo možnost opt-out, zato lahko trdimo, da je med načelom opt-in, ki temelji na predhodni privolitvi, in načelom opt-out, ki omogoča le

[1] arstechnica.com/old/content/2008/07/06-opt-out-nebuad-hides-link-in-5000-word-privacy-policy.ars> (21. 7. 2009)

poznejšo zavrnitev, ogromna razlika. Pri varstvu osebnih podatkov je zato lahko načelo opt-out le pogojno uporabljeno, in sicer na mestih, kjer naj posegi v zasebnost posameznika ne bi bili tolikšni, da bi zahtevali vnaprejšnjo privolitev posameznika in bi se lahko s poznejšo zavrnitvijo obdelave osebnih podatkov lahko ustrezno zagotovilo varstvo pravic posameznika.

Kako gre nekaterim panogam sistem opt-out v nos, kaže tudi srdit boj spletne oglaševalske industrije proti novemu režimu oglaševanja na podlagi spletnih piškotkov, ki ga prinaša Direktiva 2009/136. Slednja bi (že) morala biti prenesena v zakonodaje članic EU maja lani, uveljavlja pa sistem opt-in na področju piškotkov. Oglaševalska industrija, ki je dolga leta kovala dobičke s profiliranjem posameznikov in ciljnim oglaševanjem, ne da bi se spletni uporabniki sploh zavedali, kako to poteka, kdo vse zbira njihove podatke in v kakšnih sociodemografskih kategorijah so sploh uvrščeni, seveda ne izbira sredstev v boju proti takšni ureditvi.

Ne gre seveda pozabiti tudi na primer Phorm, ki je na skrivaj izvajal poskuse z uporabo t. i. »Deep Packet Inspection« tehnologije tako, da bi v sodelovanju s ponudniki dostopa do interneta in s poseganjem v samo vsebino komunikacije lahko uspešneje izvajal ciljno oglaševanje. Po javnem napadu je podjetje izginilo iz novic, s sorodnimi ponudniki, kot je Kindsight, pa se počasi vrača s pretkanim prehodom na sistem opt-in in mamljivimi ponudbami za uporabnike: »Prav. Glasno in jasno vam povemo – brali bomo vsebino vaše spletne komunikacije in temu prilagajali oglase. Gmail to že počne. V zameno vam damo cenejši – kaj cenejši, BREZPLAČNI dostop do interneta.« Uporabniki bodo podpisovali anekse kot nori. In to ni vse – Kindsigth ponuja brezplačen varnostni paket in varovanje pred krajo identitete in kot navaja njihov promocijski material, je 60 % uporabnikov pripravljenih uporabiti njihove brezplačne varnostne storitve v zameno za prejemanje ciljnih oglasov. Kakšna ironija, opozarja Ryan Kim – posamezniki so pripravljeni ponuditi svoje osebne podatke o uporabi spleta v korist dobička oglaševalcev in operaterjev v zameno za varstvo pred »zlonamernimi tretjimi osebami«, ki bi želeli vdreti v njihove osebne podatke in jim ukrasti identiteto za lastno finančno korist.

Vrnimo se k spletnim družbenim omrežjem, kjer ne moremo mimo Facebooka in Googla s storitvijo Google+. Oba sta pred kratkim najavila uvedbo metod za samodejno prepoznavo (obrazov) oseb na fotografijah. Google+ bo na fotografijah, ki jih bodo uporabniki naložili, samodejno identificiral njihove prijatelje, Facebook pa uvaja podobno funkcionalnost (»Tag Suggestions«), ki uporabniku s pomočjo prepoznave obrazov poda namige, kdo naj bi bil udeležen na fotografijah in kako mu enostavno pripeti ime in priimek. Če je Facebook to možnost vključil kot privzeto in dal uporabnikom le možnost opt-out, je Google ubral bolj prefinjeno pot in je uporabo tega orodja označil kot izbirno. Glede na dogovor z irskim pooblaščencem bo, kot vse kaže, tudi Facebook moral veliko svojih praks spremeniti v sistem opt-in. Spletni velikani so že sprevideli, da jo precej bolje odnesejo, če nas prepričajo, da si nekaj res želimo, kot pa da nas prisilijo v deljenje podatkov s sistemom opt-out.

Je torej opt-in rešitev in srebrna krogla za težave z netransparentnimi poslovnimi praksami in zavajanjem posameznikov? Se bojim, da ne (povsod).

Kot navaja Morozov, se spletni velikani ne sprašujejo, ali ima uporaba njihovih orodij, kot je samodejna prepoznava obrazov, tudi katere širše, celo negativne družbene posledice, temveč na orodja gledajo le kot na sredstvo za doseganje cilje, ki naj ne bi imelo drugih implikacij. Morozov to ponazarja z uporabo avtomobila kot orodja za premik iz točke A v točko B, pri čemer pa uporaba avtomobila za sabo pušča obsežen vpliv na ljudi, prostor, okolje, stopnjo smrtnosti in podobno, pri tem pa vprašanje, ali je uporabnik tehnologijo začel uporabljati po sistemu opt-in ali opt-out, ni tako bistveno. Podobno ima tudi samodejna prepoznava obrazov svoje implikacije, tega pa različni Phormi, NebuAdi in Facebooki ne želijo obravnavati, podobno kot prodajalce sistemov za nadzor dostopa na prstne odtise ne zanimajo nikakršni negativni vidiki uporabe le-teh. V njihovih propagandnih materialih ne boste dobili odgovorov na vprašanje, kje bomo ob zlorabi dobili nov prstni odtis ali obraz, če ga bomo nekega dne uporabljali kot vsakdanje sredstvo identifikacije pri vstopu v pisarno, računalnik, na mestni avtobus ali nogometni stadion. Preden se ljudska masa zave negativnih implikacij, je običajno že prepozno, saj je tehnologija že preveč vgrajena v naše življenje. Neoluditi na pohodu, bodo na to rekli kritiki – kako pa naj predvidimo vse mogoče uporabe tehnologije, ne da bi pri tem zavirali tehnološkega razvoja? Odgovor je težko najti, gotovo pa zanašanje na privolitev uporabnikov ne more biti vedno dovolj.

Nekatera področja našega življenja se namreč dotikajo tako pomembnih vrednot, da mehanizmov varstva enostavno ne smemo prepustiti posamezniku. Država nas nič ne vpraša, ali se strinjamo z obvezno uporabo varnostnega pasu v avtomobilu, čeprav bi marsikateri voznik raje podpisal sto soglasij in izjav, da se zaveda nevarnosti, samo da se mu ne bi bilo treba privezati pred vožnjo. Takšnih področij, kjer je država ocenila meje, kjer soglasje posameznika ne zadošča, je seveda veliko. Če bi namreč pristali na splošno poseganje v zasebnost komunikacije na podlagi privolitve posameznika v zameno za brezplačni internet, kot to želijo Phorm in njemu podobni, potem smo podpisali smrtno obsodbo zasebnosti na internetu. Čeprav v zameno za brezplačni internet je to cena, ki si je ne moremo in ne smemo privoščiti. Negativne eksternalije izgubljene zasebnosti so namreč preveč dolgoročno porazdeljene, da bi jih posameznik zmogel ustrezno oceniti. Mnenje Mednarodne delovne skupine za varstvo osebnih podatkov v telekomunikacijah (IWGDPT) tako trdno zagovarja stališče, da bi se operaterji morali vzdržati kakršnekoli uporabe DPI-tehnologij v namene oglaševanja. Če želimo ohraniti svojo komunikacijsko in informacijsko zasebnost na internetu, morajo biti države na področjih, kjer so vprašljive temeljne človekove pravice, toliko pokroviteljske, da bodo šle tudi čez zavestne odločitve posameznika in bodo od spletnih velikanov zahtevale več etičnosti in presoje vplivov na zasebnost oziroma bodo posegle po orodjih regulacije. Spremembe ePrivacy direktive v Evropi in ukrepi ameriškega nadzornika za trg (Federal Trade Commission) le-to potrjujejo.

Države so bile primorane regulirati monopole na številnih področjih. Ali nas torej protimonopolna zakonodaja čaka tudi pri monopolistih na trgu zbiranja osebnih podatkov? Če država ne bo poskrbela za nas, si bomo pomagali sami? Če se uporabniki doslej še niso vprašali, pa je verjetno sedaj – ko nam je Google z združitvijo podatkov svojih storitev na enem mestu in enotno politiko »zasebnosti« bolj plastično predstavil, kaj dejansko vse ve o nas – pravi čas za ponovni

premislek, ali resnično lahko zaupamo toliko podatkov enemu samemu podjetju. Morda pa regulacija s strani države ni pravi pristop in se rešitev skriva v civilni nepokorščini, ekstremni ozaveščenosti in aktivizmu uporabnikov interneta. Gibanja 99 %, pravične trgovine in okoljske aktiviste že poznamo v realnem svetu. Lahko podobno pričakujemo na področju zasebnosti in svobode na internetu? Annonymous in piratske stranke kažejo v to smer. Bomo videli. Se dobimo čez deset let, ko se tega najbrž ne bomo več spraševali.

Viri:

- International Working Group on Data Protection in Telecommunications: Working Paper on the Use of Deep Packet Inspection for Marketing Purposes, 48th meeting, 6-7 September 2010, dostopno na: http://www.datenschutz-berlin.de/attachments/726/WP_DPI_07_09_2010_675_41_10__2_.pdf?1292413821.
- Johnson, E. in Goldstein, D. Medicine: Do Defaults Save Lives? Science Magazine, 302 (5649), 1338-1339, 21. 11. 2003.
- Kim, R.: Deep Packet Inspection Circles Back for a Second Look. 24. 11. 2011, dostopno na: http://gigaom.com/2010/11/24/deep-packet-inspection-circles-back-for-a-second-look/.
- Kučić, Lenart J: Prvi uspeh kampanje proti Facebooku. 24. 12. 2011, dostopno na: http://www.lenartkucic.net/2011/12/24/prvi-uspeh-kampanje-proti-facebooku/.
- Lyons, D.: The Truth About Facebook Privacy—if Zuckerberg Got Real, 30. 11. 2011, dostopno na: http://www.thedailybeast.com/articles/2011/11/30/the-truth-about-facebook-privacy-if-zuckerberg-got-real.html.
- Morozov E.: Saving Face. How Google, Facebook, and other tech companies hide behind “opt-in” policies, 19.12.2011, dostopno na: http://www.slate.com/articles/technology/future_tense/2011/12/google_s_and_facebook_s_facial_recognition_opt_in_policies_are_a_smokescreen_.html
- O'Dell J.: Facebook’s biggest change yet: Actions are here. 18.1.2012, dostopno na: http://venturebeat.com/2012/01/18/facebook-actions-rollout/
- Tomšič, Andrej in Burnik, Jelena: DPI - pandorina skrinjica interneta? Pravna praksa 2011/13, 7.4.2011.

Matjaž Batič Finžgar, Arnes

Arnesov spletni video portal
Arnes video web portal

Povzetek

Konec 2011 smo na Arnesu pripravili nov video portal za pretočni video v flashu. Namenjen je objavljanju video posnetkov, ki so jih uporabniki posneli s svojimi kamerami ali telefoni. V kratkem pa bo portal omogočal tudi prenose v živo.

Ključne besede: video portal, flash pretočni video, pretočni video v živo, H.323-videokonference, spletne konference VOX.

Abstract

In 2011 Arnes launched new web page for flash video streaming, that allows users to upoload video recordings and stream live video.

Key words: video portal, flash video streaming, live video streaming, H.323 videoconferences, VOX web conferences

Uvod

Na Arnesu se vsako leto trudimo uporabnikom ponuditi nove storitve s področja večpredstavnosti, pri tem pa smo zelo pozorni, da so storitve kakovostne, stabilne in preizkušene, saj lahko le tako uporabnikom zagotovimo varno in udobno uporabo svojih storitev.

Osrednji del

Video portal omogoča ogled video posnetkov v flash pretočnem videu in HTML5. Prijava v video portal je omogočena vsem članom federacije ArnesAAI, vsi profesorji pa preko AAI-atributov samodejno pridobijo pravico nalaganja in objavljanja posnetkov, ki so jih posneli s svojimi telefoni ali kamerami. Ob nalaganju posnetkov na portal se posnetki samodejno pretvorijo v obliko, primerno za pretočni video v flashu in HTML5 za pametne telefone, pripravi se slika s povzetkom videa, uporabnik pa lahko vnese opis videa v obliki, ki je prilagojena svetovnim iskalnikom gradiv.

Ker je video portal vključen v federacijo ArnesAAI, lahko profesorji dostop do svojih posnetkov omejijo na izbrane posameznike ali skupine. Vsaka organizacija, priključena v federacijo ArnesAAI, pa določi tudi skrbnika video portala, ki lahko spreminja diskovne kvote profesorjem svoje organizacije, obravnava neprimerne posnetke in komentarje profesorjev in študentov, z obrazcem pa lahko zaprosi tudi za povečanje diskovne kvote celotne organizacije.

Pri nalaganju posnetkov je obvezen vnos metapodatkov, ki so v prilagojeni slovenski izobraževalni sferi v Dublin core formatu. Portal s sistemom ključnih besed vseeno omogoča tako enostavno kategorizacijo znotraj posameznih predavanj kot kategorizacijo splošnih dogodkov. Vsak profesor lahko metapodatke pri svojih posnetkih dodatno ureja po končanem nalaganju posnetkov, lahko pa to pravico dodeli tudi poljubnemu članu federacije ArnesAAI.

Za profesorje, ki nalagajo posnetke na video portal, ni nujno, da so tudi avtorji posnetkov, v nasprotnem primeru pa morajo imeti dovoljenje za nekomercialno objavo brez predelav po Creative commons licenci.

Zaključek

Video portal združuje svet video prenosov v živo in videokonferenc s flash pretočnim videom, ki omogoča, da so video vsebine dostopne na osebnih računalnikih in pametnih telefonih. Video portal s svojim iskalnikom omogoča javnosti enostaven dostop do posnetkov videokonferenc in posnetkov, ki so jih uporabniki posneli s svojimi kamerami.

Tomi Dolenc,
Arnes

Z verodostojno e-identiteto do storitev
Your trusted e-identity – a key to services

Povzetek

Na voljo vam je vedno več storitev in tudi Arnes v zadnjem letu ponuja kar precej novega. Pogosto pa se niti ne zavedate, da geslo za uporabo teh novih storitev verjetno že imate. »Zvijača« je v tem, da tudi v Sloveniji vedno več institucij (vse univerze, kar nekaj šol ...) podeljuje svojim članom oz. uporabnikom e-identitete, ki jih »priznavajo« različne storitve na podlagi skupnega modela (t. i. AAI). Če sami takšne e-identitete še nimate, jo boste verjetno dobili jutri. Danes pa lahko za dostop do teh storitev preprosto uporabite Arnesovo uporabniško ime na nov način.

Ključne besede: E-identiteta, federacija, ArnesAAI, storitve, enotna prijava.

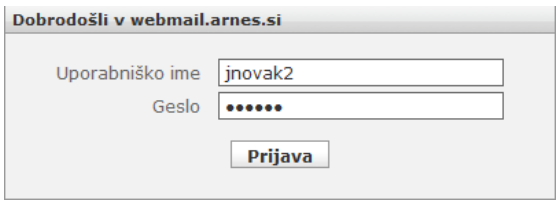
Abstract

More and more services are available, and in the last year ARNES too has had much new to offer. People often don't even realise that they already have a password to access these new services. The “point” is that institutions in Slovenia (all universities, quite a number of schools) increasingly allocate e-identities to their members and users that are “recognised” by various services on the basis of a shared model (i.e. AAI). If you still don't have such an e-identity, you'll probably get one tomorrow. Today you can simply use your ARNES user name in a new way to access these services.

Key words: E-identity, federation, ArnesAAI, services, single-sign-on.

Kako do (spletne) storitve, ki zahteva prijavo?

Odgovor na vprašanje v naslovu je videti banalen: seveda, nekam – najbrž v ustrezno okence (slika 1) – je treba vpisati uporabniško ime (ali nekaj podobnega) in geslo, pa je.



SLIKA 1: TIPIČNA PRIJAVA V SPLETNO APLIKACIJO.

Preden to storimo prvič, je treba najbrž opraviti registracijo, ob kateri ponudniku storitve posredujemo nekaj svojih podatkov, v zameno pa dobimo zgoraj omenjeni »ključ« za uporabo. Od vrste storitve in ponudnika je odvisno, kako zapleten in formalen je postopek registracije. In to je v grobem to.

Ali gre tudi drugače?

V prispevku bomo pojasnili simpatičen koncept, ki želi uporabnikom zmanjšati število potrebnih gesel za različne storitve, ponudnikom pa prihraniti breme registracije. Vse skupaj temelji na pojmu verodostojne e-identitete, ki jo pridobimo

oz. že imamo »doma«, torej nekje, kjer nas že poznajo in se nam torej ni treba ponovno registrirati.

Koncept ni nov in ga največkrat povezujemo s pojmi »federated services« in AAI (Authentication and Authorization Infrastructure). Tokrat se bomo pri njegovi obravnavi osredotočili na perspektivo uporabnika – odtod nekoliko vzgojni ton prispevka[2] – in pri tem skoraj v celoti obšli razlago tehnologije, ki je potrebna za delovanje takšnega sistema.

Pri branju se vam morda razkrije, da imate že danes v rokah ključ do nekaterih novejših storitev, ne da bi se tega zavedali. Preden pa postopek prijave praktično opišemo, bomo pojasnili zamisel sistema in pojme, ki nastopajo v njem.

E-identiteta

Pojem elektronske identitete je širše gledano nek nabor podatkov o posamezniku, ki se uporablja pri dostopanju do omrežnih virov oz. storitev. V tem prispevku bomo z izrazom »e-identiteta« največkrat označevali kar konkretno oznako (identifikator), s katero kot uporabniki v e-svetu izkazujemo svojo istovetnost. Leto je lahko uporabniško ime, ki smo ga pridobili od ponudnika, digitalni certifikat, vpisna številka študenta, profil v družbenem omrežju (npr. na Facebooku). Te identitete imajo različno stopnjo verodostojnosti in tudi uporabljamo jih za različne namene. Težava z njimi je med drugim ta, da jih je vedno več.

Seveda ni verjetno, najbrž pa tudi nesmiselno ali varno, da bi lahko kar eno samo od teh identitet uporabili za vse različne namene. Vendar bi vseeno radi to zmedo nekoliko zmanjšali. Ena očitna pot je, da uporabljamo več storitev istega ponudnika in upamo, da zanje zadošča ena e-identiteta, ki nam jo je ta ponudnik dodelil (pomislimo npr. na velike ponudnike, kot sta Google in Microsoft, ki ponujata celo paleto različnih storitev, ali Arnes v slovenski izobraževalno-raziskovalni skupnosti). Mnoge storitve so takšne, da jih bolj kot verodostojnost identitete uporabnika zanima, kako lahko identitete (in obnašanje) posameznika med seboj povežejo in poleg možnosti registracije dopuščajo ali celo spodbujajo prijavo z obstoječo e-identiteto (»Prijavi se s svojim Facebook profilom!«). Spletne banke npr. *niso* primer takšnih storitev, saj morata obe strani zanesljivo vedeti, s kom imata opravka; pri dostopu do takšnih storitev se zato uporabljajo identitete, overjene s certifikati.

Federacija in verodostojna e-identiteta

Omejimo se nekoliko na svoje delovno oz. učno okolje. Pri svojem delu dostopamo do različnih virov in uporabljamo vrsto storitev, ki so nam dodeljene na podlagi pripadnosti instituciji ali naše delovne vloge v njej (raziskovalec, profesor, študent). Primeri takih storitev so npr. vse, ki sestavljajo delovno okolje – morda prijava v računalnik ali lokalno brezžično omrežje, vstop v spletno učilnico, dostop

[2] Obstaja prepričanje, da se uporabniki – torej ljudje, ki uporabljajo (spletne) storitve – bojijo novosti in da jim je treba vsako stvar potrpežljivo razložiti. Ton razlage, ki so ga vajeni iz šole, naj bi jih zazibal v hipnotičen občutek varnosti, v katerem bodo pojasnilo, kot nekoč v šoli, zlahka sprejeli. Ta predpostavka je iz več razlogov napačna pa tudi če bi držala, je do uporabnikov podcenjujoča, zato je omenjeni ton moč uporabljati le kot stilsko figuro z ustreznim opravičilom ☺.

do člankov in oddaljenih baz podatkov, prijava na izpite, storitve Arnesa ... Vse takšne storitve zahtevajo določeno stopnjo verodostojnosti pri prijavi, saj so bodisi namenjene določeni uporabi (znotraj institucije ali pri sodelovanju s sorodnimi), vezane na pogoje pogodbe z našo matično institucijo (dostop do oddaljenih vsebin) ali ponujajo posebne pogoje glede na status (npr. popust oz. brezplačna uporaba za študente).

Ob tem pa praviloma takoj ob prihodu v to svoje okolje dobimo vsaj eno e-identiteto za uporabo storitev, ki so v bistvu naša delovna (e-)orodja – torej geslo za omrežje, za vstop v spletno učilnico, za izpite ... Ta identiteta je verodostojna znotraj institucije, saj le-ta ve, komu jo je podelila.

Izhodišče za razvoj koncepta »federacije« oz. povezovanja različnih storitev v enotnejšo uporabniško izkušnjo je sedaj preprosto: zakaj ne bi za vse ali vsaj čimveč teh storitev, ki sestavljajo naše delovno okolje, uporabili iste e-identitete (ki jo že imamo oz. jo moramo pridobiti takoj, ko želimo uporabljati e-storitve v svojem okolju)?

Da koncept deluje, je potreben *dogovor:* uporabnik je – na neki standardiziran način – registriran in dobi *e-identiteto* na enem mestu, naravno oz. praviloma je to njegovo delovno okolje oz. matična institucija (fakulteta, šola), ki njegovo identiteto pozna in je torej ni treba dodatno preverjati. Ta institucija nastopa kot *ponudnik (in tudi varuh) identitete* svojega člana – uporabnika storitev. Storitev (oz. ponudnik, ki za njo stoji) pa mora, namesto da bi zahtevala registracijo, sprejeti e-identiteto uporabnika in verjeti njeni verodostojnosti. Ker za verodostojnost jamči matična organizacija, le-ta kot *ponudnik identitete* sklene s *ponudnikom storitev* ustrezen dogovor in se tako z njim poveže v zvezo (federacijo).

Vse to dogovarjanje seveda uporabnika bolj malo zanima: zanj je pomembno le, da dobi »geslo«, ki je uporabno za čim več e-orodij, ki jih pri svojem delu potrebuje.

Vse lepo in prav, vendar ali tudi deluje?

Iz zgoraj povedanega je razvidno, da so za delovanje koncepta – poleg dogovora, ki v resnici pride na koncu – potrebne naslednje komponente: nekakšna infrastruktura, ki vse skupaj povezuje, ustrezno upravljanje identitet in seveda primerno število storitev, ki tak dogovor upoštevajo.

E-infrastruktura (middleware)

Za izobraževalno-raziskovalno okolje uvajajo evropska in svetovna nacionalna omrežja, kakršno je Arnes, enotno programsko infrastrukturo (AAI, aai.arnes.si), ki omogoča delovanje koncepta federacij. Slovenska izobraževalna federacija ArnesAAI je del te infrastrukture, sorodna je tudi federacija Eduroam (eduroam.arnes.si), ki povezuje brezžična omrežja predvsem univerz po Evropi in tudi izven nje, uporabnikom pa ponuja preprost dostop v omrežje z enotnim geslom na katerikoli od članic federacije. Arnes vzdržuje programsko infrastrukturo in upravlja obe federaciji ter pri tem ponuja pomoč pri vključevanju v federacijo in gostovanje ustreznih strežnikov.

Upravljanje identitet

Matična institucija oz. ponudnik identitete mora ustrezno upravljati identitete uporabnikov (skrbeti za ažurnost, za distribucijo e-identitet svojim članom), kar načeloma ne bi smelo biti pretežko, saj že zdaj upravlja vsaj eno (verjetno pa več) registrov svojih članov za najrazličnejše namene. Seveda pomaga, če imamo za to primerna orodja. V sodelovanju z Arnesom se v okviru projekta E-šolstvo razvija orodje, ki bo to upravljanje olajšalo vsaj slovenskim srednjim in osnovnim šolam, verjetno pa bo uporabno tudi širše (Podbrščček, 2012).

Storitve

Število storitev, ki so dostopne na ta način, se povečuje. Vsekakor so v slovenskem raziskovalnem in izobraževalnem okolju to vse novejše Arnesove spletne storitve – *Filesender* (filesender.arnes.si), *Arnes Blog* (blog.arnes.si), *spletne konference VOX* (vox.arnes.si) – ki zahtevajo identifikacijo uporabnika in mu morda na podlagi njegovega statusa (učitelj, dijak) tudi določijo različne pravice.

Danes na Arnesu vse spletne storitve razvijamo tako, da bi bile preko ArnesAAI takoj dostopne vsem upravičenim uporabnikom na univerzah, v šolah in drugih organizacijah brez zamudnih postopkov s prijavnicami in potrjevanjem statusa. Novost v letu 2012 je npr. spletna aplikacija, ki vsem imetnikom veljavne e-identitete v federaciji ArnesAAI omogoča, da si na Arnesovem strežniku pridobijo nekaj lastnega prostora in odprejo svoj poštni predal, kar je bilo doslej mogoče le s »papirno« registracijo (Vreča, 2012).

Ker gre pri AAI za standardne in razširjene protokole, se mnoge tipične spletne aplikacije, uporabne v izobraževalnem okolju (npr. spletne učilnice Moodle) preprosto prilagodijo temu načinu prijave.[3] Prilagojene so mu tudi storitve, ki nastajajo v okviru projekta E-šolstvo (www.sio.si). Možnost prijave preko AAI brez težav upoštevamo pri razvoju novih storitev in tako sledimo cilju, da bi za čim več vsakodnevnih opravil potrebovali le eno geslo. Če le gre, je smiselno prilagoditi tudi že obstoječe aplikacije.

Prav tako pa lahko mnogi veliki ponudniki (založbe z online bazami podatkov, Google, Microsoft) ponudijo svoje storitve na ta način, če z njimi sklenemo ustrezen dogovor (gl. npr. (Arnes, [2])).

Tipični elementi e-identitete v federaciji

Identifikatorju oz. e-identiteti, s katero se prijavimo v neko storitev, pogosto rečemo *uporabniško ime* (username, UserID) in je po navadi sestavljena iz niza znakov (lahko tudi številk), ki nam ga dodelijo ob registraciji ali pa si ga lahko izberemo sami. To ime nas enolično določa znotraj storitve oz. organizacije, pri kateri smo registrirani.

Vsi ponudniki storitev, pridruženi določeni federaciji, prepoznajo vse e-identitete uporabnikov, ki prihajajo od kateregakoli ponudnika identitet. Verodostojna e-identiteta v federaciji je sestavljena iz dveh delov: t. i. »kraljestva« (realm), ki

[3] Za gostujoči Moodle v paketu »Polni« opravi to prilagoditev Arnes, gl. (Arnes, [1]).

pripada ponudniku identitet in združuje določeno skupino uporabnikov (en ponudnik lahko pokriva več kraljestev) ter uporabniškega imena, ki ga ponudnik dodeli vsakemu posameznemu uporabniku v svojem kraljestvu. E-identiteta, ki bi ji lahko rekli tudi »enotno uporabniško ime v federaciji AAI«, je torej sestavljena takole:

e-identiteta == Kdo + OdKod

ali zapisano drugače: NetID == UserID@Kraljestvo

Pri tem smo za »tehnično« oznako tega identifikatorja izbrali ime NetID, da poudarimo veljavnost razširjenega uporabniškega imena (UserID) v omrežju federacije. Kraljestvo pa ustreza kar eni od veljavnih internetnih domen, ki pripada ponudniku identitete. Primeri veljavnega NetID bi lahko bili naslednje oblike[4]:

jnovak2@neka.sola.si

janez.novak@pef.uni-lj.si

123456789@student.uni-lj.si

Opazimo, da je NetID po obliki zelo podoben naslovu za e-pošto. Opozorimo, da tu nastopa v drugi vlogi, prav tako ni nujno (celo praviloma ne), da bi NetID ustrezal nekemu dejanskemu naslovu e-pošte. Sicer pa nas ta dvojnost med uporabniškim imenom in e-naslovom ne bi več smela begati (prim. npr. prijavo v Google).

Ponudniki identitet v federaciji ArnesAAI

V federacijo ArnesAAI so vključene vse slovenske univerze, naraščajoče število šol in nekatere druge organizacije (mnogi so hkrati vključeni tudi kot ponudniki storitev, npr. lastnih spletnih učilnic, gl. http://aai.arnes.si/seznam.html). Vsi ti lahko svojim uporabnikom izdajo veljavno identiteto, ki jim med drugim omogoča uporabo vseh Arnesovih storitev, ne da bi za to morali registrirati uporabniško ime na Arnesu, za kar je sicer potreben postopek s potrjeno prijavnico. Večinoma so te organizacije tudi članice federacije Eduroam, zato praviloma velja isti NetID tudi za dostop do brezžičnega omrežja Eduroam doma in po svetu.

Gostujoča e-identiteta na Arnesu

Vsaka organizacija, ki želi svojim uporabnikom ponuditi dostop do storitev v federaciji ArnesAAI, mora torej najprej vzpostaviti standardiziran imenik svojih članov in ustrezen strežnik,[5] ki uporabniku omogoča prijavo na domači organizaciji. Da bi pri tem pomagali, smo na Arnesu omogočili gostovanje takšnih imenikov/strežnikov, organizacija mora torej poskrbeti le za ažuriranje podatkov.

[4] Zadnja dva primera prikazujeta kraljestvi, ki najbrž pripadata istemu ponudniku identitete (univerzi).

[5] Tak strežnik v e-svetu prav tako imenujemo »ponudnik identitete« oz. (Identiy Provider) in ga navadno označujemo s kratico IdP.

Da pa bi dostop do storitev omogočili tudi tistim uporabnikom, katerih matična organizacija (še) ni članica ArnesAAI, lahko imetniki uporabniških imen na Arnesu[6] uporabijo tudi ustrezno nadomestno ali gostujočo e-identiteto v federaciji ArnesAAI. Ta e-identiteta predstavlja razširitev uporabniškega imena (username) in ima obliko

NetID == username@guest.arnes.si

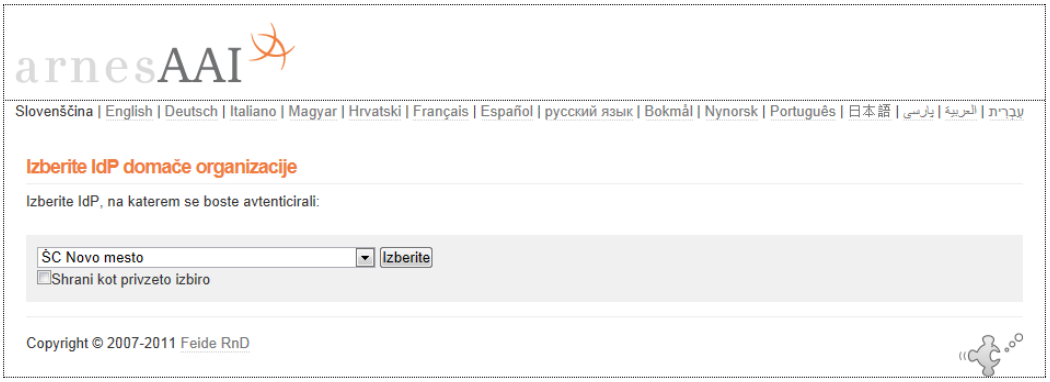
Tako se lahko npr. Janez, ki ima na Arnesu uporabniško ime »*jnovak2*«, predstavlja v federaciji ArnesAAI kot »*jnovak2@guest.arnes.si*«. Domena jasno nakazuje, da gre za gostujočo e-identiteto, zato tak uporabnik morda ne more izkoristiti vseh funkcionalnosti neke storitve, ki bi bile vezane na njegovo pripadnost določeni organizaciji. Vsekakor lahko uporablja storitve Arnesa, drugi ponudniki storitev pa mu lahko omogočijo uporabo pod svojimi pogoji.

Nova uporabniška izkušnja

Ker se storitve v federaciji AAI zanašajo na obstoječe e-identitete, je uporabniška izkušnja ob prijavi nekoliko drugačna, kot smo je vajeni oz. kot je opisana v uvodu, zato morda sprva deluje kot ovira. Zavedati se moramo, da nas storitev »ne pozna« – ne more preveriti našega gesla, zato se vedno najprej prijavimo svojemu *ponudniku identitete*, ki hrani naše podatke. Pri tem mu dovolimo, da storitvi posreduje tisti del naših podatkov, ki so za delovanje storitve potrebni; šele potem smo v storitev prijavljeni. Vendar pa se ob novih prijavah deli postopka preskakujejo, saj smo jih že opravili! Oglejmo si ta postopek podrobneje.

Postopek prijave v storitve federacije ArnesAAI

Začnemo torej z izbiro svojega *ponudnika identitete*, pri čemer nam bolj ali manj ustrežljivo pomaga vmesnik z menijem, kjer so našteti vsi člani federacije, ki nastopajo kot ponudniki identitet. Le-to je lahko videti npr. takole (slika 2):



SLIKA 2: PRVI KORAK PRIJAVE: IZBOR PONUDNIKA IDENTITETE

Ponudnik identitete pri tem pomeni organizacijo – načeloma našo matično, ki nam je izdala e-identiteto, lahko pa tudi Arnes, če uporabljamo gostujočo identiteto. Navodila za pravilno prijavo bomo vedno dobili od ponudnika identitete, torej tistega, od katerega smo e-identiteto (NetID in geslo) prejeli. Ker se bomo

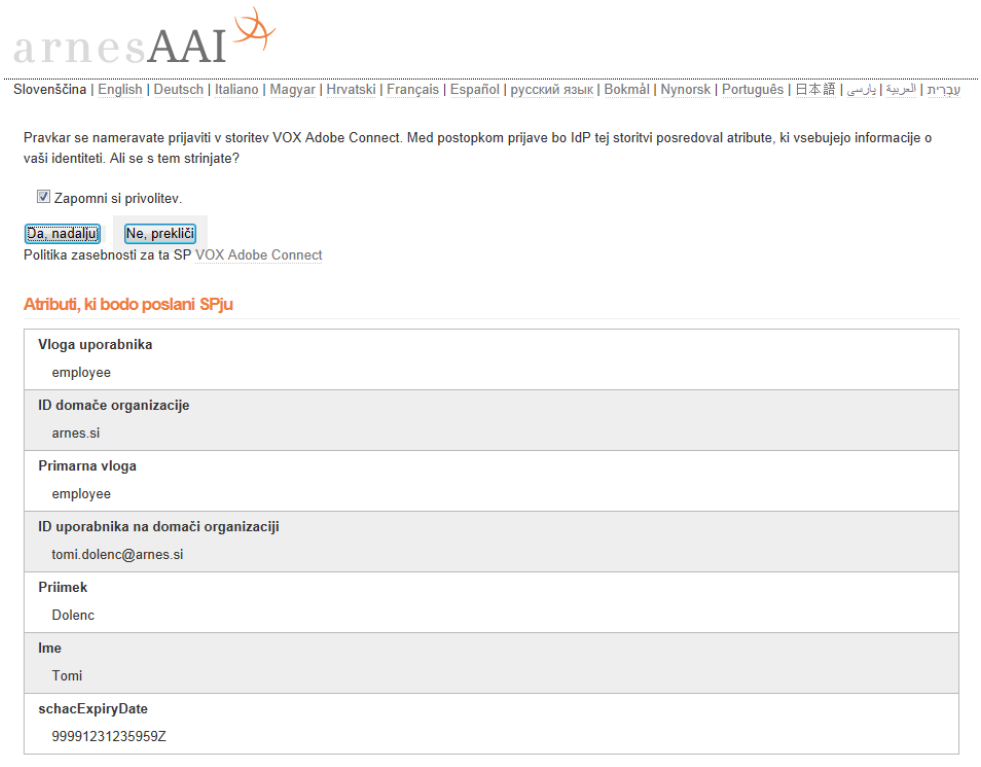
[6] http://www.arnes.si/storitve/storitve-za-posameznike/pridobitev-uporabniskega-imena.html

praviloma prijavili vedno preko istega ponudnika identitete (IdP), lahko nastavimo privzeto izbiro.

V naslednjem koraku se ponudniku identitete predstavimo s svojo e-identiteto, tako da vnesemo svoje »uporabniško ime v federaciji AAI«, torej NetID, in pripadajoče geslo. Primer na sliki 3 prikazuje vmesnik Arnesovega IdP, saj ima avtor svojo
e-identiteto na Arnesu. Vaš ponudnik identitete ima morda malce drugače oblikovan vmesnik.

SLIKA 3: DRUGI KORAK PRIJAVE: VNOS NETID IN GESLA NAŠEMU PONUDNIKU IDENTITETE

Naslednji korak nas vsaj prvič vizualno najbolj »prestraši«, čeprav je prav ta korak ključ do našega popolnega nadzora nad posredovanjem svojih osebnih podatkov posameznim storitvam. Ponudnik identitete (strežnik) nas namreč opozori, katere podatke iz imenika bo posredoval storitvi – praviloma lahko storitev zahteva le tiste podatke, ki jih potrebuje za svoje delovanje. V tem trenutku si lahko premislimo, če menimo, da storitev od nas zahteva preveč osebnih podatkov. Včasih storitvi popolnoma zadošča že sam NetID. Na primeru na sliki 4 lahko vidimo, da storitev VOX poleg NetID zahteva še ime, priimek, vlogo uporabnika v organizaciji (»employee«) ter datum poteka veljavnosti. Na podlagi teh podatkov namreč lahko upravlja z vsebinami, ki jih uporabnik hrani na strežniku.



SLIKA 4: TRETJI KORAK: PRIVOLITEV POSREDOVANJA OSEBNIH PODATKOV STORITVI

Po tem koraku smo v storitev prijavljeni in jo lahko začnemo uporabljati. Postopek je morda videti zapleten v primerjavi z »običajnim« vpisom uporabniškega imena in gesla na spletni strani storitve, vendar kmalu ugotovimo, da je pri večjem številu storitev prijaznejši, saj je ne glede na različne storitve vedno enak in nam tako postane domač, poleg tega pa se privzete izbire shranijo (gl. tudi sliko 3) in nam pri vseh naslednjih prijavah občutno skrajšajo pot. Zares pa nas razveseli to, da se nam naenkrat v različne storitve sploh ni treba več prijavljati, če smo že enkrat opravili prijavo s svojo e-identiteto, saj za storitve federacije velja načelo *enotne prijave* (Single-Sign-On), dokler se pač ne odločimo, da je za danes dovolj in se odjavimo.

Zaključek

Namen tega prispevka je trojen. Prva želja je bralca dovolj obširno in razumljivo seznaniti z vlogo in pomenom njegove nove e-identitete (NetID), ki predstavlja razširitev pojma uporabniškega imena, ki nam ga dodeli ponudnik (bodisi matična organizacija ali ponudnik gostujočih identitet). Ta e-identiteta namreč »velja« pri več različnih ponudnikih storitev v federaciji. Drugi je seznaniti imetnike ali upravičence do Arnesovega uporabniškega imena o novi funkcionalnosti (»moje uporabniško ime je lahko NetID«). Tretji pa je opozoriti vse imetnike veljavnih (ali bodočih) e-identitet v federaciji ArnesAAI na storitve, ki so jim na voljo, ne da bi zanje potrebovali nova gesla oz. registracijo.

Viri

1. Podbršček, M., (2012): Upravljanje z identitetami. V: Mednarodna multikonferenca Splet izobraževanja in raziskovanja z IKT – SIRikt 2012 (zbornik),Kranjska Gora 21. – 24. marec 2012. Ljubljana: Miška d.o.o.

2. Vreča, M., (2012): Nov osebni paket – naklikaj si svoj e-mail. V: Mednarodna multikonferenca Splet izobraževanja in raziskovanja z IKT – SIRikt 2012 (zbornik),Kranjska Gora 21. – 24. marec 2012. Ljubljana: Miška d.o.o.
3. Arnes, [1]: http://www.arnes.si/storitve/splet-posta-strezniki/dinamicno-gostovanje-phpmysql/paketi/polni.html (2011).
4. Arnes, [2]: http://www.arnes.si/obvestila/obvestilo/article/dostop-do-bibliografskih-baz-podatkov-web-of-science-tudi-z-arnesaai.html (8. 4. 2011).

Blaž Divjak, Arnes

Dobili smo ArnesAAI, kaj sledi?
We've got ArnesAAI, what next?

Povzetek

Arnes AAI pridruženim organizacijam poenostavlja upravljanje uporabniških imen in gesel ter njihovim uporabnikom daje možnost uporabe aplikacij, ki so vključene v ArnesAAI (npr. spletne konference VOX), ali katere izmed lastnih aplikacij, ki podpirajo tovrstno prijavo. Organizacije se lahko v Slovensko izobraževalno raziskovalno federacijo ArnesAAI pridružijo na več načinov, prav tako lahko uporabniki, če njihova organizacija ni članica federacije ArnesAAI, vseeno pridobijo uporabniško ime, ki jim nudi omejene funkcionalnosti.

Ključne besede: ArnesAAI, ponudnik identitet, ponudnik storitev, enotno uporabniško ime.

Abstract

ArnesAAI makes it easier for affiliated organisations to manage user names and passwords, and allows users to use applications bundled with ArnesAAI (e.g. Vox webconferences), as well as their own applications that support this type of login. Organisations have various options for joining ArnesAAI, the Slovenian education-research federation, and users can get limited-functionality NetIDs even if their organisation is not a member of the ArnesAAI federation.

Key words: ArnesAAI, identity provider, service provider, single sign-on

Uvod

Vse večja uporaba informacijskih tehnologij v raziskovalno-izobraževalni sferi s seboj prinaša veliko število uporabniških podatkov. Hramba, varovanje in osveževanje podatkov predstavlja za tehnično osebje na organizacijah velik zalogaj. Namesto izdajanja novih uporabniških imen in gesel za različne storitve lahko kot rešitev uvedemo centralizirane in enotno strukturirane zbirke uporabniških podatkov in infrastrukturo, ki bo omogočala sodelovanje med organizacijami. S tem je mogoče končnim uporabnikom nuditi enostavne in celovite rešitve za dostop do storitev znotraj meja domače organizacije in izven njih.

Kaj AAI-infrastruktura omogoča?

Enotna infrastruktura za overjanje istovetnosti in avtorizacijo vzpostavlja okolje, ki omogoča deljenje aplikacij in znanja med raziskovalno-izobraževalnimi organizacijami, ki so pridružene v slovensko izobraževalno federacijo ArnesAAI. Preverjanje istovetnosti uporabnikov ter hranjenje njihovih osebnih podatkov se izloči iz aplikacij (serviceProvider) in se izvaja na domači organizaciji uporabnikov (IdentityProvider).

ArnesAAI omogoča vzpostavitev enotne, centralizirane zbirke uporabniških podatkov v raziskovalno-izobraževalnih ustanovah. Takšni podatki na organizacijah običajno že obstajajo in jih je treba le ustrezno strukturirati. Tehničnemu osebju to poenostavlja dodeljevanje dostopa svojim članom

(študentom, učiteljem, zunanjim sodelavcem), njihove podatke pa vnesejo zgolj enkrat.

Organizacije lahko funkcionalnosti svojih aplikacij delijo tudi z uporabniki drugih organizacij ali pa svojo enotno zbirko uporabniških podatkov uporabijo za prijavo v lastne aplikacije (npr. spletne učilnice). Uporaba AAI-prijave je mogoča tudi na virtualnih strežnikih (GVS). Paket Polni omogoča AAI-prijavo v Moodle in Joomlo, paket Asistenca pa vsebuje vse potrebne komponente, da je tovrstna prijava mogoča tudi v aplikacijah, ki jo podpirajo. Ob vzpostavitvi infrastrukture omrežja Eduroam lahko organizacija uporabi isto zbirko uporabniških podatkov in tako svojim članom ponudi možnost uporabe tega izobraževalnega omrežja.

Končnim uporabnikom ArnesAAI omogoča uporabo enotnega uporabniškega imena in gesla za dostop do vseh storitev, ki jih nudi njegova domača organizacija (npr. spletne učilnice), kot tudi tistih, ki jih nudijo druge organizacije (npr. videokonference VOX, filesender, blog, Web of Science). Če ima organizacija vzpostavljeno infrastrukturo za omrežje Eduroam, lahko uporabljajo tudi brezžično omrežje Eduroam v Sloveniji ali tujini.

Ob prijavi v aplikacije se preverjanje pristnosti uporabnika vedno izvede na prijavnem strežniku domače organizacije. Spletna aplikacija nikoli ne vidi uporabnikovega gesla in pridobi vpogled zgolj v tiste osebne podatke uporabnika, ki so potrebni za nudenje storitve. Uporabnik ima ob prijavi popoln nadzor nad prenosom osebnih podatkov in lahko, če aplikaciji ne zaupa povsem, postopek prekliče.

Uspešna preverba pristnosti uporabnika je veljavna določeno časovno obdobje, kar pomeni, da se v tem časovnem obdobju pri dostopu do aplikacij prijava izvede samodejno, brez posredovanja uporabnika. Obdobje je odvisno od nastavitev prijavnega strežnika, lahko le nekaj ur, lahko pa cel dan.

Načini pridružitve v ArnesAAI

Organizacije se lahko v Slovensko izobraževalno raziskovalno federacijo ArnesAAI pridružijo na več načinov, prav tako lahko uporabniki, če njihova organizacija ni članica federacije ArnesAAI, vseeno pridobijo uporabniško ime, ki jim nudi omejene funkcionalnosti.

Vzpostavitev lastne infrastrukture na organizaciji

Takšno uporabo ArnesAAI priporočamo večjim organizacijam in tistim, ki že imajo Eduroam in s tem bazo uporabnikov. Takšen primer so šolski centri, univerze in podobni, ki lahko nastopajo kot skupen ponudnik identitet (IdP) za vse svoje članice. Organizacija potrebuje nekoga, ki jim infrastrukturo vzpostavi in vzdržuje, potrebna pa je tudi relativno hitra in zanesljiva povezava v internet.

Gostovanje LDAP + IdP+ RADIUS

Gostovanje na Arnesu je namenjeno manjšim organizacijam in organizacijam s slabšo infrastrukturo. Organizacija potrebuje nekoga, ki bo s pomočjo LDAP-urejevalnika urejal njihove uporabnike. Sama rešitev je ekvivalent vzpostavitvi lastne infrastrukture na organizaciji, organizaciji pa precej olajša vzpostavitev in vzdrževanje.

guest.arnes.si NetID

Guest.arnes.si NetID je zasilni izhod za vse, ki drugje ne morejo pridobiti uporabniškega imena (NetID). Uporabnost tega uporabniškega imena je omejena, saj uporabniki s tem uporabniškim imenom ne bodo mogli dostopati do določenih vsebin.

test.arnes.si NetID

Trenutno nadomešča guest.arnes.si, ki je opisan v prejšnji točki. V prihodnje bo takšno uporabniško ime (NetID) namenjeno tehničnemu osebju organizacij, ki skrbi in testira AAI-infrastrukturo na organizaciji.

Zaključek

Enotna infrastruktura za overjanje istovetnosti in avtorizacijo (AAI) je odlična alternativa izdajanju novih uporabniških imen in gesel ob vsaki novi storitvi ter ponuja dobre možnosti za medorganizacijsko sodelovanje. Z uvedbo AAI-infrastrukture organizacija močno poenostavi upravljanje z uporabniškimi podatki in svojim uporabnikom zagotovi enostavno uporabo storitev znotraj meja domače organizacije in izven njih.

Viri

1. Papež. Rok. 2008. Enotna prijava v spletne aplikacije. Ljubljana.
2. Arnes. 2012. ArnesAAI – vstopna stran. Dostop: aai.arnes.si (25. 1. 2012).

Milan Podbršček, TŠCNG

Upravljanje z e-identitetami
Identity managemet

Povzetek

Povezovanje storitev v zadnjem času vedno pogosteje rešujemo z imeniki (LDAP in AD, znotraj organizacije) in AAI-jem (zunaj organizacije). Upravljanje z identitetami znotraj imenikov ni enostavno rešljivo, zato smo se odločili razviti spletno aplikacijo, ki nam bo v pomoč pri tem delu. Kot dodano vrednost lahko aplikacija nudi vir podatkov o učečih in njihovih starših ter zaposlenih tudi drugim aplikacijam, ki jih uporabljamo pri našem delu.

Ključne besede: e-identiteta, LDAP, AD, infrastruktura

Abstract

In recent times, it has become increasingly common to link services using directories (LDAP and AD, within organisations) and AAI (outside organisations). Identity management within directories is not a trivial task, so we decided to develop a web application to make it easier. As added value, the application can provide a source of data on learners, parents and employees for other applications that we use in our work.

Key Words: e-identity, LDAP, AD, infrastructura

Uvod

Za uporabo storitev v poslovnem okolju in v spletu se mora uporabnik identificirati. Imeti mora uporabniški račun, ki je v večini primerov sestavljen iz uporabniškega imena in gesla. Le za nekatere storitve je prijava okrepljena z uporabo certifikatov (ravnateljski portal na MŠŠ, banke ipd.) ali gesel za enkratno uporabo (OTP – angl. One Time Password). Ker si je težko zapomniti množico uporabniških imen in gesel, bi uporabniki radi za več storitev uporabili isto identiteto (uporabniško ime in geslo).

Vzgojno-izobraževalni zavodi (v nadaljevanju VIZ) niso nobena izjema. Uporabljajo različne aplikacije za upravljanje procesov v šoli. Posplošeno lahko rečemo, da šole uporabljajo dve ključni kategoriji aplikacij:

1. aplikacije za spremljanje pedagoškega procesa
2. aplikacije za vodenje računovodsko/knjigovodsko-kadrovskega procesa

Ključne aplikacije so Lopolis in e-Asistent za spremljanje pedagoškega procesa ter SAOP in Vasco za vodenje računovodstva oz. knjigovodstva.

Lopolis kot primarna aplikacija za vodenje pedagoškega procesa je še posebej “močna” oz. pogosta v osnovnih šolah. V srednjih šolah se vedno bolj uveljavlja e-Asistent, zaslediti je mogoče tudi lastne rešitve, in sicer predvsem na informacijsko razvitejših šolah. Vsaka od aplikacij zahteva določene podatke, ki so enaki ali pa zelo podobni in bi lahko bili poenoteni.

Poleg upravljanja zgoraj navedenih procesov v zadnjem času na šolah vse pogosteje uporabljamo tudi sisteme za upravljanje z učnimi vsebinami (npr. Moodle) in sisteme za upravljanje z vsebinami (npr. Joomla). Vedno več je tudi različnih spletnih aplikacij, ki jih ponuja Arnes. Tudi te aplikacije potrebujejo zbiranje in vodenje povsem istih ali podobnih podatkov kot sistemi za upravljanje šole. Poleg tega te aplikacije zahtevajo vodenje uporabniških imen in gesel. Določene Arnesove storitve potrebujejo tudi podatke o preteku vpisa učenca/dijaka ter vlogo zaposlenega na šoli.

Rešitev

K reševanju problema bomo pristopili z dveh nivojev, eden je znotraj posamezne organizacije, drugi je povezan navzven.

Pod povezovanjem navznoter[1] razumemo povezovanje aplikacij znotraj šole. Aplikacije se bodo povezovale na skupno bazo, za katero skrbi sistem za upravljanje z identitetami (v nadaljevanju IdM). Iz njega bodo pobirali podatke različni imeniki, kot sta na primer imenika LDAP (Lightweight Directory Access Protocol) ali Microsoft AD (Active Directory), in aplikacije, ki so namenjene upravljanju učnega procesa in upravljanju poslovanja. Za imenike je razvit »push« način, način dela z drugimi aplikacijami pa je odvisen od aplikacij samih. Pripravljena je shema, po kateri bodo lahko te aplikacije dostopale do podatkov.

Spletne aplikacije na področju dela pri pouku se lahko povežejo na imenike (LDAP, AD). Nekatere aplikacije v upravnem procesu se ravno tako že povezujejo na obstoječe imenike. Za mnoge podatke, ki so v imenikih, ne zadostujejo, zato lahko pričakujemo, da se bodo povezale raje na IdM.

Pod povezovanjem navzven[1] razumemo povezovanje na aplikacije, ki niso v lasti šole, torej predvsem storitve, ki jih vzgojno-izobraževalnim zavodom nudi Arnes. Le-to je rešeno na nivoju AAI-ja[3] in ni predmet te razprave, čeprav AAI uporablja določene šolske imenike (LDAP in AD).

Predstavitev

Sistem za upravljanje z identitetami[4] je spletna aplikacija. Je odprtokodna rešitev, ki za bazo uporablja FireBird. V spodnji tabeli so našteti vsi atributi, ki jih vodi.

Uporabniški račun	Osebni podatki	Kontaktni podatki
Uporabnisko_Ime Uporabnisko_Ime_Polno Geslo St_Prijav St_Neuspesnih_Prijav St_Neuspesnih_Prijav_Sum St_Menjav_Gesla St_Ponastavitev_Gesla Datum_Prva_Prijava Datum_Zadnja_Prijava Datum_Zadnja_NeuPrijava Datum_Zaklenjeno Datum_Menjava_Gesla Datum_Ponastavitev_Gesla	Ime Priimek Priimek2 Spol EMSO Davcna_ST Datum_Rojstva Drzavljanstvo_ID Drzava_Rojstva_ID Kraj_Rojstva_ID Kraj_Rojstva	Telefon_Mobilni Telefon_Doma Telefon_Sluzba Email

Datum_Potek_Gesla Datum_PozGeslo_SKLIC		

Lokacijski podatki	Podatki učečega	Podatki učečega – razred	Podatki učečega – VIZ-program
Ulica Hisna_ST Posta_Kraj_ID Kraj Posta_ID Zacasno_Ulica Zacasno_Hisna_ST Zacasno_Posta_Kraj_ID Zacasno_Kraj Zacasno_Posta_ID	VPISNA_STEVILKA UDELEZENEC_ID_MSS DATUM_ZAVOD_VPISAN_OD DATUM_ZAVOD_VPISAN_DO DATUM_ZAKLJUCKA_IZ ZAKLJUCNA_STOPNJA_GL	RAZRED_LETNIK_ID DATUM_VPISAN_OD DATUM_VPISAN_DO NACIN_IZOBRAZEVANJA_ID STATUS_UDELEZBE_ID OBLIKA_IZOBRAZEVANJA_ID POVPRECNA_OCENA	VIZ_PROGRAM_ID DATUM_VPISAN_OD DATUM_VPISAN_DO

Namenjen je upravljanju podatkov učencev/dijakov, njihovih staršev in zaposlenih. Zajem podatkov je mogoč z masovnim ali individualnim vnosom. Mogoče je urejanje vseh podatkov (seveda glede na pravice posameznika). Trenutno so implementirani štirje nivoji varnosti[2] in s tem seveda tudi funkcije posameznika, kot jih ima v poslovnem procesu. Vzdrževalec sistema (root) lahko vidi in ureja vse podatke. Šolski upravljavec lahko vidi in ureja podatke svoje šole, urednik pa lahko ureja zgolj podatke o učencih/dijakih, starših in zaposlenih.

Vsak posameznik/uporabnik, ki je vključen v IdM, lahko vidi svoje podatke, nekatere med njimi lahko tudi popravi. Predvsem je tu mišljena sprememba gesla. Pomembna funkcija je ponastavitev pozabljenega gesla, poleg tega pa lahko vsak posameznik vidi tudi zgodovino sprememb svojih podatkov.

Spremenjeni podatki se sinhronizirajo s podatki v LDAP-u in AD-ju. Sistem omogoča izvoz podatkov v XML- in XLS-format. Dolgoročno je načrtovano tudi omogočanje neposrednega zajema (push ali pull) podatkov drugim aplikacijam. Prenosi podatkov se izvajajo s šifriranimi povezavami.

Zaključek

Z razvojem sistema za upravljanje z identitetami smo močno olajšali delo šolskemu osebju, ki skrbi za različne evidence, izrazito pa je olajšano tudi delo informatikom, ki skrbijo za uvajanje novih storitev v šolsko okolje. Uporabnikom smo zmanjšali število uporabniških imen in gesel.

Seveda to ni konec razvoja. Veliko bo treba narediti še na različnih izpisih in v prihodnosti tudi na uporabi osebnih certifikatov za povečano varnost dostopa do sistema.

Viri in literatura

1. Linden Mikael, Organisational and cross organizational identity management, Tempere univesity of Technology, pulication 779, Tempere 2009
2. Mark Bruhn, Michael Gettes, and Ann West, Identity and Access Management
   and Security in Higher Education,
   http://www.educause.edu/ir/library/pdf/eqm0342.pdf,
3. Avgust Jauk, AAI v slovenskem izobraževalno raziskovalnem okolju, http://www.sirikt.si/fileadmin/sirikt/predstavitve/2009/Arnes_federacija.pdf

Matej Breznik, Arnes

Zaščitimo svoje omrežje
Protect your network

Povzetek

Problematika omrežne varnosti je prisotna že dolgo. Z množičnim približevanjem medmrežja slehernemu posamezniku pa je postala še toliko pomembnejša. Priča smo širjenju medmrežja na vsakem našem koraku in s tem tudi prenosom za nas pomembnih informacij v medmrežje. Prav tako pa se spreminjajo tudi oblike običajnega druženja, saj dandanes posamezniki množično komunicirajo s pomočjo medmrežja. Zato sta naša spletna identiteta kot tudi omrežna varnost še posebej pomembni. V primeru slabe zaščite posameznika lahko zloraba privede do kraje identitete, podatkov, denarja ali celo česa hujšega.

Ključne besede: razvoj informacijske varnosti, informacijska ozaveščenost, novodobna varnostna tveganja.

Abstract

Network security problems have been around for some time. The mass adoption of the internet has increased their importance. The internet is becoming present everywhere, and information that is important to us is increasingly online. Even the ways we socialise are changing, so that today individuals communicate en masse over the internet. All of this makes web identities and network security even more important. If an individual is poorly protected, misuse could lead to the theft of identities, data, money or even something worse. The aim of the talk is to provide delegates with an insight into the threats facing network users in recent years. We will examine changes in recent years in the access points used by attackers, and will review the mechanisms that protect us. We will also study the methods used by modern attackers to gain access to our organisations' systems, and using case studies set out the key points where protection and attention are particularly important. The session will also cover modern methods of targeted attacks and refute certain myths about protection from them.

Key words: evolution of computer security, information security awareness, modern security threats

1. Uvod

S prihodom medmrežnih tehnologij v praktično vsak del našega življenja so se spremenile tudi naše vsakdanje navade. Tako danes vedno več časa preživimo na spletu, prek njega komuniciramo z znanci, splet je postal enostaven in ni več v domeni posameznikov, poznavalcev. Na ta način lahko prek medmrežja opravimo kopico reči, za katere smo v preteklosti potrebovali fizično prisotnost. Na družbenih omrežjih se srečujemo, prodajamo, česar ne potrebujemo, kupujemo, kar si želimo, ali prek medmrežja opravljamo bančne storitve. Prenos našega zasebnega življenja na medmrežje pa ni ostal neviden kriminalcem, ki se želijo z našim prihodom na splet okoristiti. Kriminalci torej bodisi izkoriščajo naše pretirano zaupanje bodisi nam podtaknejo škodljivo programsko opremo, ki jim omogoča dostop do naših najzaupnejših podatkov. Medmrežna varnost tako ni več le stvar strokovnjakov, pač pa do določene mere zadeva prav vsakogar. Če

ne sledimo in upoštevamo informacij o varni uporabi medmrežja, se nam lahko kaj hitro zgodi, da postanemo nemočna žrtev okužbe, posledično tudi kraje identitete ali morda celo denarnega oškodovanja.

2. Stanje

V preteklosti smo skrbniki omrežij doživljali omrežne napade v obliki omrežnih pregledovanj, zoper katere se je bilo mogoče zelo enostavno zaščititi s pomočjo omrežnih požarnih zidov, ki so že z enostavnimi pravili o dovoljevanju povezav le v eno smer omejili oziroma zavrnili večino škodljivega omrežnega prometa. Poleg tega je bilo mogoče okužbo sistema zelo enostavno odkriti, saj je le-ta v primeru povezovanj na svoj kontrolni strežnik uporabljala zelo enostavne nezaščitene protokole, večinoma razne derivate IRC-protokola.

V zadnjih letih pa je tako zaznava okužb sistemov kot tudi zaščita le-teh vedno večji problem. Škodljiva programska oprema namreč v vedno več primerih uporablja zapletene šifrirane mehanizme za komunikacijo s kontrolnim strežnikom. Tudi vektor vstopa škodljive programske opreme je v zadnih letih drugačen, saj je za namestitev škodljive programske opreme lahko odgovoren kar uporabnik sam oziroma njegov skrbnik sistema, ki ni poskrbel za ustrezno omejitev pravic ali opozarjanje uporabnika.

Ene najbolj znanih okužb so t. i. drive-by-download. O njih govorimo, kadar se na posameznikov sistem, ne da bi to sam želel ali vedel, sproži prenos škodljive programske opreme (t. i. malware). Treba se je zavedati, da ne gre le za ogroženost ob brskanju po straneh slabega slovesa. Napadalci namreč izkoriščajo zlorabljene uredniške dostope popolnoma legitimnih spletnih strani, ki jih najdemo ob običajnem brskanju oziroma jih morda celo redno obiskujemo. Z zlorabo dostopa ali ranljivostjo nameščene spletne aplikacije napadalci na stran podtaknejo škodljivo kodo, ki se nato izvrši na sistemu nič hudega slutečega obiskovalca.

Žal pa se je kljub skrbi uporabnika oziroma skrbnika sistema določenemu tipu ranljivosti v programski opremi le stežka izogniti; gre za t. i. zero-day ranljivosti. V tem primeru gre za ranljivosti, ki so bile odkrite in izpostavljene javnosti oziroma zaprti skupini, še preden jih je lahko proizvajalec programske opreme odpravil oziroma zanje izdal ustrezen popravek. Tako so te ranljivosti med napadalci najbolj priljubljene, saj zoper njih še ni na voljo popravkov in imajo tako za izkoriščevalce tudi določeno tržno vrednost. Posledice okužbe uporabnikovega sistema imajo lahko različne razsežnosti. Od nedolžnega poskusa prodaje lažne protivirusne programske opreme do v zadnjih letih vse pogostejše kraje podatkov z okuženega sistema uporabnika. Izpostavljena so predvsem shranjena gesla na uporabnikovem sistemu (denimo gesla za dostop do elektronske pošte, različnih spletnih storitev ...) kot tudi shranjeni podatki na uporabnikovem okuženem sistemu, ki omogočajo dostop do elektronskega bančništva.

V zadnjih letih je v javnosti veliko govora o t. i. APT-napadih,vendar je treba pri teh napadih opozoriti, da večinoma temeljijo na starih, že odkritih ranljivostih, proti katerim pa iz takšnih ali drugačnih razlogov ni bil nameščen popravek oziroma vzpostavljena ustrezna zaščita. V nekaterih primerih bi celo lahko trdili, da je edina razlika med t. i. APT-napadom in običajnim napadom v tem, da je okužba

sistema pri običajnem napadu zgolj naključje oziroma okužen sistem ni bil posebej izbran s strani napadalca. Pri APT-napadu pa gre tudi za odločenost napadalca, da bo na tak ali drugačen način vstopil v izbrani sistem. Seveda pa je treba izločiti APT-napade, pri katerih je škodljiva programska oprema prilagojena in posebej narejena za ranljivost žrtvinega sistema.

V porastu so tudi okužbe, ki se širijo prek družbenih omrežij, saj se na teh zadržuje vedno več uporabnikov. Načini okužb so različni: od škodljivih povezav, ki vodijo na prenos škodljive programske opreme, do oglasov, ki se ravno tako zaključijo s prenosom škodljive programske opreme. Postopek okužbe v tem pogledu ne predstavlja novosti, saj se ta sproži bodisi samodejno z izkoriščanjem znane ranljivosti sistema bodisi pa prepriča uporabnika, da prenese in namesti škodljivo kodo. Na ta način bi lahko prišli do zaključka, da se prevaranti in goljufi premikajo skupaj z večino uporabnikov ter obstoječe metode okužbe in prevare prilagajajo novim okoljem.

3. Ukrepi

Pred bodočimi omrežnimi tveganji se le stežka zaščitimo. Pri omrežni varnosti, kjer se grožnje in tveganja nenehno spreminjajo, je osrednjega pomena dobra informiranost omrežnega skrbnika, ki lahko s poznavanjem tendenc ustrezno zaščiti svoje omrežje in uporabnike pred okužbami, krajo gesel, osebnih podatkov in v končni fazi materialnega ali moralnega oškodovanja organizacije ali posameznika. Pri tem ne gre pozabiti tudi na osveščenost posameznikov, ki so zaposleni v organizaciji, saj lahko s svojimi dejanji v veliki meri prispevajo k varnosti organizacije ali pa jo po drugi strani ogrožajo. Zato je pomembno, da so posamezniki izobraženi vsaj do določene stopnje, na kateri so še sposobni prepoznati poskus socialnega inženiringa ter preprečiti, da bi sami postali žrtev prevare.

4. Viri

1. Bu, Z., Bueno, P., Kashyap, R., Wosotowsky, A.: The New Era of Botnets http://www.mcafee.com/in/resources/white-papers/wp-new-era-of-botnets.pdf.
2. Ducklin, P. (23. 12. 2010): Internet Explorer zero-day exploit – explanation and mitigation http://nakedsecurity.sophos.com/2010/12/23/internet-explorer-zero-day-exploit-explanation-and-mitigation/.
3. Naraine, R. (15. 4. 2009): Drive-by Downloads, The Web Under Siege http://www.securelist.com/en/analysis/204792056/Drive_by_Downloads_The_Web_Under_Siege.
4. Spletna stran: http://blog.7elements.co.uk/2011/06/apt-in-nutshell.html.

Ksenija Furman Jug, Arnes

Arnesov izobraževalni in raziskovalni internet: od 14 kb/s do nekaj 10 Gb/s
From 14 kb/s to 10 Gb/s with ARNES

Povzetek

V 20 letih se je kapaciteta mednarodne povezave omrežja ARNES povečala več kot 650.000-krat. Prenos multimedijskih vsebin zahteva vedno večje kapacitete prenosnih poti. Če želimo graditi računalništvo v oblaku, se moramo najprej lotiti gradnje zanesljive optične infrastrukture pod zemljo.

Potrebe torej rastejo in danes je prava ter dolgoročna rešitev optična povezava. Kakšne možnosti imajo zavodi za uporabo optičnih povezav? Kaj lahko storijo tisti, ki možnosti za optično povezavo (še) nimajo?

Ključne besede: optična povezava, internetna povezava, kapaciteta povezave, kakovost storitev, varnost omrežja, IPv6

Abstract

The capacity of ARNES' international links has increased by a factor of 650,000 in the last 20 years. The need for higher capacity connections is growing with the use of multimedia applications. When building cloud computing, we need to provide reliable optical infrastructure underground.

Optical fibre is the only long-term solution to growing demand. Can the available optical infrastructure meet the needs of user organisations? What options are there for those without access to optical fibre?

Keywords: optical link, local area network, link capacity, quality of service, network security, IPv6

Uvod

Uporabniki se pri svojem delu dnevno srečujejo z računalništvom v oblaku, prenašajo zvok, sliko ter video in se ne zavedajo, da vse to ni mogoče brez varnega, zanesljivega in zmogljivega omrežja naprav in bakrenih, optičnih ter brezžičnih povezav. Tehnologija in ponudniki nam ponujajo marsikaj. Strokovnjaki Arnesa pomagajo uporabnikom, da poiščejo in uporabijo potrebam primerne rešitve za povezovanje lokalnih omrežij zavodov v omrežje ARNES in poskrbijo, da so te povezave varne in optimalno izkoriščene. Le na ta način uporabniki pri svojem delu nimajo težav in v resnici lahko pozabijo na to, po kakšnih poteh potujejo »bitki«, preden pristanejo na njihovih računalnikih.

Izlet v preteklost

V večernih urah želim od doma prebrati elektronsko pošto. Kliknem na ikono za modemsko povezavo. Telefonska centrala ne podpira tonskega izbiranja, torej modem potrebuje pol minute, da odšteje pulze za izbor klicne številke. Zaslišim zlovešč zvok zasedene linije. In poskusim znova … in znova … Končno! Dobim odgovor prostega modema, ki si ga statistično delim še z 20 uporabniki. Ušesa mi napolni zvok cviljenja in piskanja. Po pol minute se javi Arnesov strežnik in mi

dodeli naslov IP. Celoten postopek modemskega povezovanja traja 5 minut. Zdaj upam, da bom na ekranu čim prej uzrla novo elektronsko sporočilo prijatelja iz Čila. Vendar ne – nocoj so se vsi spravili na net in prenos spet traja in traja. Končno! Bravo, rodil se mu je sin!

Moj modem zmore prenašati podatke s hitrostjo 14 kb/s. Piše se leto 1994.

Impresije sedanjosti

Danes pišemo leto 2012. Pri vsakodnevni komunikaciji čas ne mineva več v minutah, ampak v sekundah. Obkroža nas cela vrsta pametnih naprav, ki nam omogočajo komunikacijo preko bakrenih in optičnih vrvic ter celo po zraku. In to instantno! Čakati ne znamo več, potrpljenje smo vrgli v koš skupaj z modemi, ki so nam tako pomenljivo piskali. Živahna družbena omrežja so dokaz, da v omrežje niso povezane le naprave, ampak so omrežene naše misli. Vsakodnevno se nam predmeti in pojmi okoli nas v rokah razblinjajo in prehajajo iz realnega v virtualni svet. Živimo v iluziji, da bomo celotno resničnost pospravili v škatlico prostornine 2^{128}.

Ob tej primerjavi se mi pojavijo vprašanja: Ali lahko v teh časih znanstvenik deluje brez komunikacijskih orodij? Ali šola lahko izobražuje generacije prihodnosti z orodji in pripomočki preteklosti? Kdo si ob takem trendu drzne pogledati 20 let naprej?

Kje pa ste danes vi?

Po kratkemu izletu v preteklost in utrinkih iz sedanjosti vas vabim k razmisleku, kaj se v tem trenutku dogaja z lokalnim omrežjem na inštitutu ali fakulteti, v šoli, knjižnici ali muzeju, od koder prihajate. Ali natančneje, kaj se dogaja s povezavo, ki vaše lokalno omrežje povezuje v svetovni splet.

Ali spada vaš zavod v skupino 10 % srednjih šol, 20 % osnovnih šol ali 30 % knjižnic, ki še niso povezane v omrežje ARNES? Svetujem vam, da si čim prej zagotovite povezavo. V nadaljevanju vam bom poskusila pojasniti, kaj je za vaš zavod najboljša rešitev.

Če se nahajate v bližini ene od 63 Arnesovih točk priklopa v 30 krajih po Sloveniji, je za vas najboljša možnost optično vlakno do te točke. Optično vlakno je treba zakupiti, cene ponudnikov pa niso najnižje, zato je v mnogih primerih smiselna investicija v lastno optično infrastrukturo. Danes lahko preko optičnih vlaken prenašamo podatke s hitrostjo nekaj 10 Gb/s. Tehnološki razvoj terminalnih naprav omogoča nenehno povečevanje hitrosti prenosa podatkov. To dejstvo dokazuje, da je naložba v optična vlakna učinkovita in da bodo taka vlakna ob morebitni menjavi terminalne opreme zagotavljala zmogljivo povezavo še nekaj let ali celo desetletij. Več kot polovica zavodov, ki so povezani v Arnesove točke priklopa, uporablja optične povezave, ki so jih sami zgradili.

Ne smemo pozabiti že zgrajenega dela optičnih omrežij, ki je največkrat v lasti lokalnih skupnosti. Skrivnost recepta za optimalen izkoristek obstoječe optične infrastrukture presenetljivo ne temelji na tehničnih pripomočkih, ampak na človeški naravi, ki še zna sodelovati; sodelovati z ostalimi zavodi in z lokalnimi skupnostmi. S sodelovanjem se da preseči marsikatero oviro in predvsem prihraniti precejšen del sredstev, potrebnih za investicije. Sodelovanje omogoča

tudi gradnjo kampusov, ki omogočajo skupno rabo strežnikov in ostalih informacijskih storitev ter tudi prihranke človeškega dela in stroškov. Vzorčni primer dobrega sodelovanja med zavodi in lokalnimi skupnostmi je uspešno zaključen projekt Kočevje, kjer se je v začetku leta ob podpori občine preko optike povezalo v omrežje ARNES 10 zavodov.

Če ste oddaljeni od 30 krajev, kjer je prisoten Arnes, si na http://www.arnes.si/storitve/dostop/pridobitev-dostopa.html lahko ogledate ponudbo ostalih možnosti. Z nekaterimi ponudniki je Arnes sklenil dogovor o posebnih pogojih. Ta ponudba je prikazana v tabeli 1. Na tehnologiji FTTH lahko dosežemo hitrosti do 100 Mb/s, na bakrenih žicah pa pod ugodnimi pogoji do 65/20 Mb/s.

Tehnologija/Ponudnik	AMIS	Stelkom	Telekom	T-2
ADSL	X		X	
VDSL			X	X
SHDSL	X			
FTTH			X	X
WiFi		X		

Tabela 1: Ponudniki in tehnologije – zelena polja označujejo pakete, za katere ponudniki zagotavljajo kvaliteto storitev

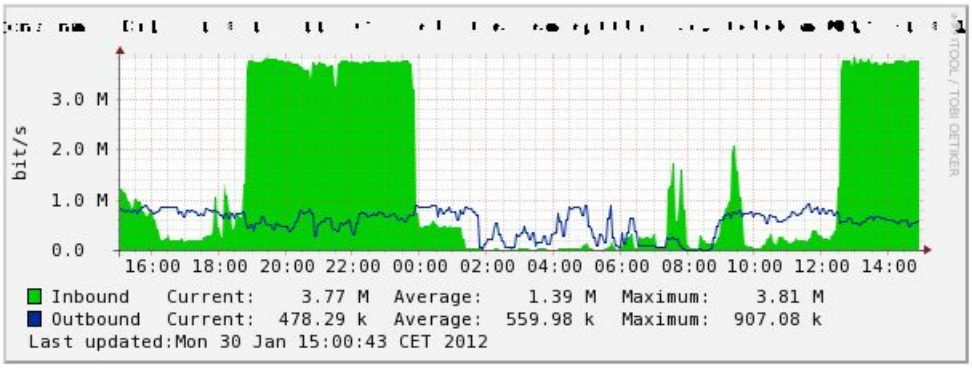
Za kakovost storitve je pomembno, da ponudniki zagotavljajo prenosne parametre pri prenosu preko njihovega omrežja. Koliko časa je lahko povezava neuporabna, koliko podatkov se lahko izgubi na poti, v kolikšnem času mora podatek prepotovati pot od enega do drugega konca povezave, v kolikšnem času mora ponudnik odpraviti napako na povezavi? Če vam ponudnik zna odgovoriti na ta vprašanja, pomeni, da si resno prizadeva za kakovost storitve, ki jo ponuja. Če se dogovorjenega ne drži, vam mora zmanjšati znesek mesečnega plačila. Trenutno so taki ponudniki za uporabnike omrežja ARNES Amis, T-2 in Stelkom.

Po letu 2007 je pod okriljem Ministrstva za visoko šolstvo, znanost in tehnologijo z javno-zasebnim partnerstvom in prispevkom sredstev Evropskega sklada za regionalni razvoj preko 40 slovenskih občin zgradilo lastno optično infrastrukturo. Gradnja je potekala izven urbanih področij na tako imenovanih »belih lisah«, kjer ponudniki niso izrazili tržnega interesa za samostojne naložbe. S tem so se za zavode na teh območjih odprle nove možnosti za zmogljive in cenovno ugodne povezave. Glede na geografski položaj je ponudba najzanimivejša za podružnične šole, saj jim omogoča tesnejšo vez z matičnimi enotami.

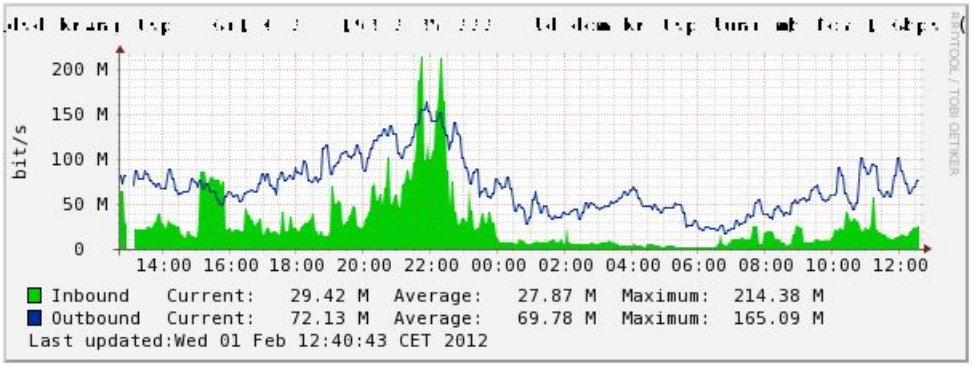
Kaj se dogaja v cevi?

Povezavo, po kateri se prenašajo podatki med lokalnim omrežjem zavoda in omrežjem ARNES/internetom, lahko ponazorimo kot dve cevi. Imamo eno cev, po kateri se prenašajo podatki proti lokalnemu omrežju zavoda, in drugo cev, kjer se prenašajo podatki v nasprotni smeri. Po navadi je prva cev debelejša od druge, lahko pa sta tudi enake debeline. Če sta obe cevi dovolj debeli, podatki potujejo neovirano. Kaj pa se zgodi, če si želi ravnatelj prenesti pomembne podatke s spleta v trenutku, ko učenci na dvajsetih računalnikih v računalniški učilnici zavzeto brskajo po spletu in iščejo odgovore na zastavljena vprašanja? Ali pa želi računovodja vnašati podatke o plačah v trenutku, ko v učilnici glasbe spremljajo

prenos koncerta s spleta? In ko se poleg vsega naštetega aktiv slavistov želi videokonferenčno povezati z aktivom slavistov na drugi šoli? In cev se zamaši! Posledica je veliko nezadovoljnih uporabnikov in kup neopravljenega dela. Primer preozke cevi je prikazan na grafu 1. Pa vendar ni pravega razloga, da bi se to zgodilo. Pri uporabi optične infrastrukture je cev zagotovo dovolj debela. Primer dovolj debele cevi je prikazan na grafu 2. Če pa optično vlakno vaše stavbe ne doseže, se morate zadovoljiti z bakrenim kablom – torej tanjšo cevjo. Pa nič zato – tudi v tem primeru obstaja rešitev. Oprema za dostop, ki jo upravlja Arnes, omogoča mehanizem – tako imenovanega policista. Ta razvršča podatke glede na njihovo pomembnost in omejuje količino določene vrste podatkov. Ali bo imelo prednost nemoteno delo ravnatelja ali so pomembnejše pravočasno nakazane plače ali pa je najpomembnejši koncert, saj želimo učencem predstaviti glasbeni užitek in jim ne želimo predvajati zvočnega skropucala. O tem, kaj je najpomembnejše, odločite vi, nastavi pa Arnes. Ti mehanizmi so predvsem pomembni pri prenosu zvoka in slike, za kar moramo rezervirati precejšnji delež cevi. Torej debelina rezerviranega dela cevi določa kakovost pri uporabi videokonferenc. Zadovoljivo kakovost lahko dosežemo pri cevi debeline 1 Mb/s in več v smeri od lokalnega omrežja zavoda proti Arnesu. Verjemite, da si slabe izkušnje s kockasto sliko in popačenim in prekinjenim zvokom pri videokonferenci nihče ne želi ponoviti.



Graf 1: Promet na povezavi 4/1 Mb/s – povezava je v obeh smereh prezasedena in delo je nemogoče



Graf 2: Promet na povezavi 1/1 Gb/s – kapacitete je dovolj, delo je nemoteno

Česa se bojimo?

V resničnem svetu se bojimo, da bi se roparji sprehajali po naši stavbi, da bi učenci spreminjali ocene v redovalnici, da bi imeli dijaki v rokah testne pole še pred preverjanjem znanja. Kakšno zmedo bi naredil v ravnatelja preoblečeni

posameznik, ki bi se s slabimi nameni sprehajal po šoli. V virtualnem svetu pa se nam vse to lahko dogaja in mi tega sploh ne zaznamo. Virtualnim nepridipravom se vsak dan utrinjajo nove ideje za svoja dejanja in če želimo biti varni pred njimi, moramo tem trendom slediti. Absolutna varnost ne obstaja niti v realnem niti v virtualnem svetu. Se ji pa lahko čim bolj približamo. V računalniškem svetu obstaja kar nekaj orodij za povečanje varnosti. Če ste povezani v omrežje ARNES, ste deležni visoke stopnje zaščite hrbtenične in druge omrežne infrastrukture ter uporabe varnih brezžičnih omrežij Eduroam. Prav tako varujemo vaš predal elektronske pošte pred virusi in neželeno pošto. Arnesovi strokovnjaki poskrbijo za varnostne nastavitve dostopovne opreme in jih glede na vaše želje in potrebe tudi prilagodijo. Pomembna je tudi varnostna ločnica med pedagoškim in administrativnim delom lokalnega omrežja, ki pomaga krotiti nevarne ideje nadobudne mladeži.

Nikakor pa ne smete pozabiti, da je najšibkejši člen omrežne varnosti človek. Zato mora zaposlenim nekdo povedati, zakaj ne smejo imeti listka z geslom zataknjenega za monitor, da je nevarno shranjevati varnostno občutljive podatke na vsem dostopne računalnike, da morajo razmisliti, preden odprejo priponke neznanega pošiljatelja in da niso vsi podatki primerni za objavo na domači strani. In na vse to je treba misliti tudi pri vzgoji mladih.

4:6

V zelo bližnji prihodnosti nas vse čaka skupni zalogaj – prehod z naslovov IP verzije 4 na verzijo 6. In tukaj je strah odveč. Vendar je treba o tem začeti razmišljati že danes. Arnes vam bo z znanjem in izkušnjami nudil pomoč, da bo prehod čim manj boleč.

Zaključek

Naj zaključim z računalniškim rekom: Samo, če ste trdno in skrbno zakopali v zemljo svoje kable, boste nemoteno jahali na oblakih. ☺

Viri

1. Arnes. 2012. Interna dokumentacija Arnesa.
2. Arnes. 2012. Prikazovalnik grafov in statistik Cacti.

Maja Vreča,
Arnes

Novi osebni paket – naklikaj si svoj mail
New personal package – click for your mail

Povzetek

Uporabniki storitev si vedno želimo, da nam za uporabo posameznih storitev ne bi bilo treba izpolnjevati raznih obrazcev. Želimo si, da bi bilo vse, kar potrebujemo, oddaljeno le nekaj klikov. Če ste tudi vi naveličani prijavnic in obrazcev za podaljševanje, vas bo gotovo zanimalo, kako bi lahko prešli na nov, hitrejši brezpapirni način ustvarjanja in podaljševanja Arnesovih elektronskih naslovov.

Ključne besede: uporabniško ime, elektronski naslov, storitve, vmesnik, imenik, e-identiteta

Abstract

Service users always want to use individual services without filling in various forms. We want everything we need just a few clicks away**.** If you too are tired of application forms and requests for extensions, you'll certainly be interested in how you can switch to a new, faster, paperless method of creating and extending ARNES electronic addresses and usernames.

Key words: username, e-mail, services, interface, directory, e-identity

Uvod

Arnes je že pred časom omogočil vključevanje organizacij v federacijo ArnesAAI.[7] Mogoče je tudi gostovanje imenikov organizacij na namenskem Arnesovem strežniku (po protokolu LDAP), ki poleg tega omogoča še postavitev strežnika organizacije za AAI-prijavo (IDP).

V razvoju je spletna aplikacija za upravljanje z identitetami, ki bo olajšala ažuriranje podatkov v imenikih (IDM). Razvoj poteka v okviru projekta E-šolstvo v sodelovanju z Arnesom.[8]

Vse to služi kot podlaga novim storitvam, ki bodo tako lažje in pregledneje dostopne končnim uporabnikom.

Vmesnik za kreacijo osebnega paketa

Ena izmed takšnih storitev je novi vmesnik, ki bo uporabnikom olajšal pridobivanje elektronskih naslovov in prostora na Arnesovih strežnikih ter podaljševanje njihove veljavnosti. Ta storitev je v pripravi in pričakujemo, da bo v kratkem vstopila v pilotno fazo.

Ta novi vmesnik omogoča, da si lahko vsak izmed naših potencialnih uporabnikov, ki na svoji matični organizaciji pridobi e-identiteto,[9] sam in z le nekaj

[7] Več o tem in o pojmu E-identitete si lahko preberete v članku z naslovom »Z E-identiteto do storitev«, ki ga ravno tako najdete v tem zborniku.

[8] Podrobnejšo predstavitev tega vmesnika najdete v članku »Upravljanje z identitetami«.

[9] Za razlago pojma priporočam v branje članek »Z E-identiteto do storitev«.

kliki na Arnesovem strežniku odpre lastni e-poštni predal in prostor za svoje datoteke ter za postavitev statične domače strani, torej ustvari svoj »osebni paket«.

Za pridobitev uporabniških imen in elektronskih naslovov je bilo do sedaj potrebno izpolnjevanje prijavnic in za večino uporabnikov tudi letno podaljševanje veljavnosti teh uporabniških imen. Arnes namreč zaradi narave svojega omrežja ne more komercialno nuditi svojih storitev, pri čemer bi se preverjalo le plačilo računa za pridobitev določene storitve. Ker gre za omrežje, ki je namenjeno izključno zaprtemu krogu upravičencev, je preverjanje identitete uporabnika ključnega pomena.

Z vstopom organizacij v federacijo AAI bo to preverjanje postalo veliko lažje, tako za končnega uporabnika, saj mu ne več treba potrjevati in pošiljati obrazcev, kot tudi za njegovo matično organizacijo. Z vzpostavitvijo novega sistema bo organizacija zgolj z vnašanjem v imenike svojim članom (zaposlenim, študentom, dijakom ...) le-tem omogočila, da si sami preko svoje e-identitete uredijo dostop do storitev, ki jih potrebujejo.

Organizacija bo sama upravljala s podatki svojih članov v imeniku in na ta način zanje tudi določala trajanje veljavnosti Arnesovih uporabniških imen. Ob spremembi statusa ali izbrisu uporabnika iz imenika matične organizacije se bo ob njegovi naslednji prijavi v omrežje tudi samodejno nastavil datum poteka njegovega uporabniškega imena.

Vmesnik bo ob tem uporabniku omogočil prenos njegovega uporabniškega imena na e-identiteto, ki jo bo pridobil na svoji novi organizaciji (npr. dijak ob prehodu na fakulteto). Če se bo uporabnik preselil na organizacijo, ki še ni vključena v federacijo ArnesAAI, pa bo moral uporabnik preiti na papirni način dokazovanja svoje istovetnosti.

Na Arnesu si želimo, da bi čim več organizacij, vključenih v omrežje ARNES, pristopilo k federaciji ArnesAAI in s postavitvijo imenikov svojih zaposlenih in učencev, študentov oz. dijakov le-tem omogočilo lažji dostop do Arnesovih storitev. To je v skladu z našo vizijo postopnega prehoda v bolj ali manj brezpapirni način komuniciranja z uporabniki, pri čemer pa se ohranja verodostojnost njihove identitete.

Ali to sploh potrebujemo?

Elektronska pošta je (še vedno) ena izmed internetnih storitev, brez katere ne moremo. Hkrati pa v poplavi brezplačnim komercialnih strežnikov, ki ponujajo to storitev, postaja vedno močnejša potreba po »resnih« in kredibilnih elektronskih naslovih.

Uporabniki se namreč čedalje bolj zavedajo implikacij manjšega varovanja zasebnosti v teh omrežjih. Večina tovrstnih strežnikov je locirana izven Evropske unije, kar zaradi manj rigorozne zakonodaje omogoča večje posege v zasebnost posameznikov za razne namene, lahko pa pride celo do zlorab. V primeru zlorab in kraj identitete je v takih primerih težko dokazati lastništvo vaših podatkov na strežnikih.

Poleg tega postaja tudi močnejša težnja po elektronskih naslovih, ki so manj generični in so bolj vezani na pripadnost določeni organizaciji oz. skupnosti.

Preko Arnesovega vmesnika si uporabnik lahko odpre poštni predal, v katerega bo poleg osnovnega elektronskega naslova ime.priimek@guest.arnes.si vodilo tudi več psevdonimov (aliasov), ki si jih uporabnik sam ustvari pod domeno matične organizacije (npr. ime.priimek@vasa-sola.si) ali pod Arnesovo domeno za gostovanje.

To uporabniku omogoča večjo prepoznavnost in uporabo njegovih elektronskih naslovov v namene, kjer je raba »brezplačniških« elektronskih naslovov nezaželena, kot so npr. določene strokovne publikacije.

Za konec

Na Arnesu si želimo, da bo tudi naš novi vmesnik za osebni paket nekoliko pripomogel k temu, da bo dostop do naših storitev lažji in uporabniku prijaznejši.

Viri:

1. Dolenc, T. (2012): Z E-identiteto do storitev. V: Mednarodna multikonferenca Splet izobraževanja in raziskovanja z IKT – SIRikt 2012 (zbornik),Kranjska Gora 21. – 24. marec 2012. Ljubljana: Miška d.o.o.
2. Podbrščček, M. (2012): Upravljanje z identitetami. V: Mednarodna multikonferenca Splet izobraževanja in raziskovanja z IKT – SIRikt 2012 (zbornik),Kranjska Gora 21. – 24. marec 2012. Ljubljana: Miška d.o.o.

Mitja Mihelič, Arnes

Arnes Planer – vedno usklajeni in Blog.arnes – spletna stran v desetih minutah
Arnes Planner – always coordinated – and Blog.arnes – website in ten minutes

Povzetek

Usklajevanje skupnih časovnih terminov ali različnih vsebin je običajno zahtevalo veliko izmenjanih elektronskih sporočil med sodelujočimi. Arnes Planer postopek usklajevanja močno poenostavi. Udeleženci le vpišejo svoje ime in izberejo časovne termine ali druge ponujene možnosti, ki jim ustrezajo. Planer sproti sešteva glasove in prikazuje rezultate za posamezne časovne termine in ostale možnosti.

Spletni dnevnik oz. blog omogoča enostavno objavo vsebin na spletu. Svoj blog lahko na enostaven način prilagodite in ga uporabite za osebno spletno stran, spletno stran organizacije ali projekta. Uporabniki boste izbrali obliko in pripravili vsebine ter z vtičniki razširili funkcionalnost svojega bloga, Arnes pa bo poskrbel za nemoteno delovanje storitve.

Ključne besede: planer, usklajevanje, blog, dinamične spletne vsebine

Abstract

Coordinating group schedules and various content usually required many exchanges of electronic messages among participants. The ARNES Planner greatly simplifies the coordination process. Participants enter their name and choose a schedule or other option that suits them. The Planner compiles the votes and shows the results for individual schedules and other options.

The web journal or blog makes it simple for users to publish web content. You can customise your blog easily, and use it for a personal, organisation or project website. Users can choose their design, prepare content, and use plugin to extend the functionality of their blog. ARNES will ensure that the service operates uninterrupted.

Key words: scheduler, coordination, blog, dynamic web content

Uvod

Usklajevanje skupnih časovnih terminov ali različnih vsebin je običajno med sodelujočimi zahtevalo izmenjavo večje količine elektronskih sporočil. Arnes Planer postopek usklajevanja močno poenostavi. Udeleženci le vpišejo svoje ime in izberejo časovne termine ali druge ponujene možnosti, ki jim ustrezajo. Planer sproti sešteva glasove in prikazuje rezultate za posamezne časovne termine in ostale možnosti.

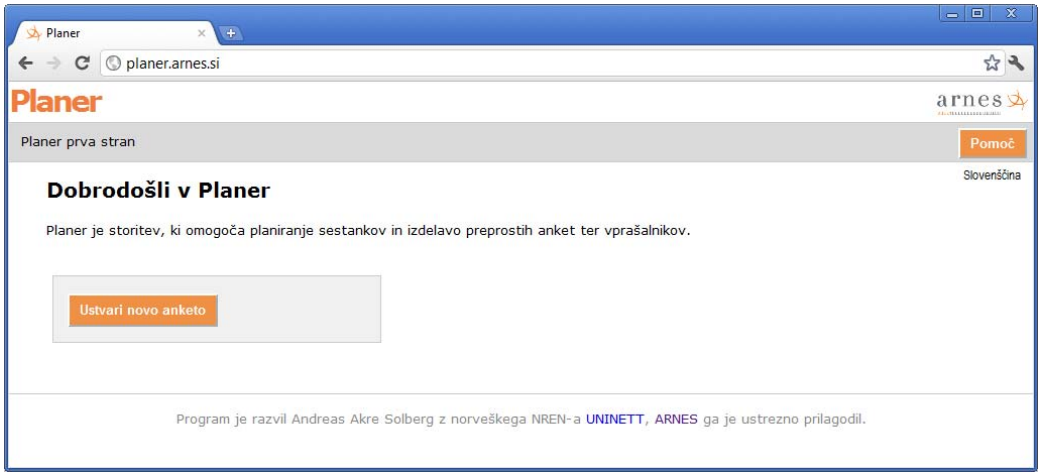
Na Arnesu smo sredi septembra 2011 za naše uporabnike pripravili novo storitev Blog.arnes. Temelji na odprtokodni platformi WordPress in uporabnikom nudi možnost objavljanja dinamičnih spletnih vsebin v obliki spletnega dnevnika ali

bloga. V začetku se je le-ta uporabljal kot osebna spletna stran, namenjena pisanju spletnega dnevnika, komentiranju in opisu dogodkov. Prispevki blogov so običajno prikazani v obratnem kronološkem zaporedju. S časom je uporaba bloga postala enostavnejša, saj so na voljo platforme, ki za uporabo ne zahtevajo veliko tehničnega znanja. Teme in vtičniki omogočajo uporabo spletnega dnevnika tako za osebno kot poslovno rabo.

Arnes Planer

Za usklajevanje različnih predlogov med seboj smo po navadi uporabljali elektronsko pošto ali pa smo se dogovarjali po telefonu. Sporočila elektronske pošte so krožila med nami, včasih smo naše odgovore celo pozabili poslati vsem sodelujočim. Na koncu smo večkrat ugotovili, da nimamo časa takrat kot ostali sodelujoči.

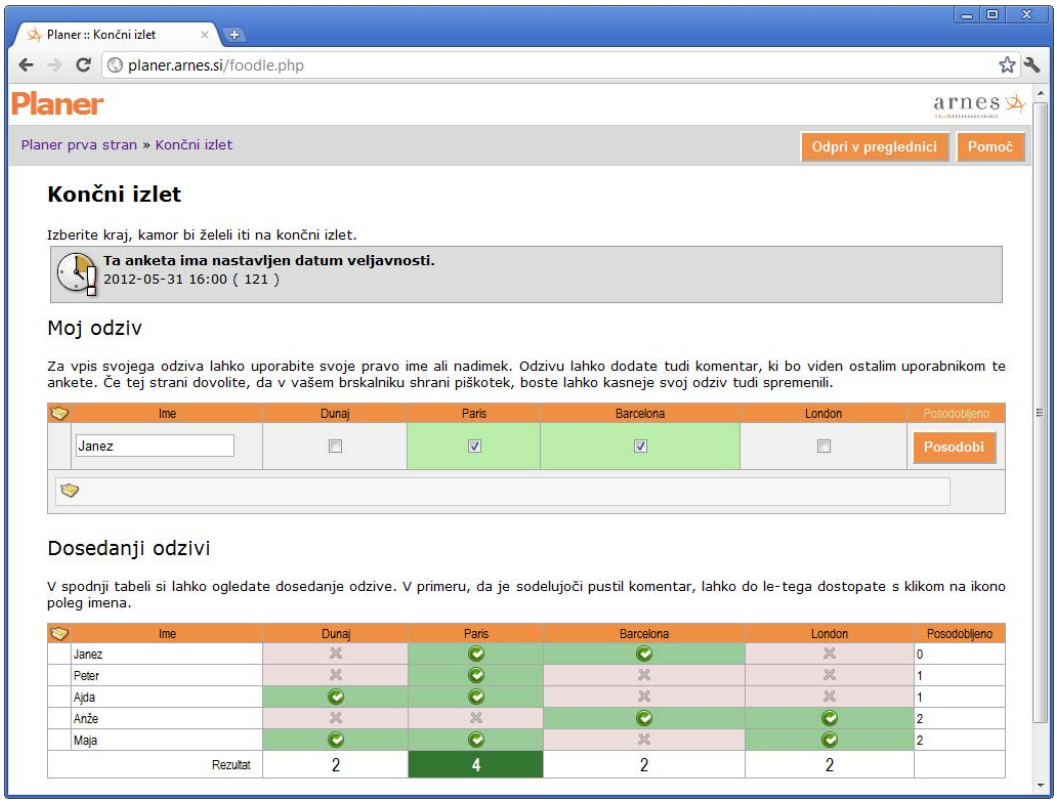
Arnes Planer omogoča enostavno planiranje sestankov z več časovnimi termini znotraj enega dneva, načrtovanje družabnih dogodkov (npr. športni dan, piknik), izdelovanje anket (npr. kam na izlet). Postopek usklajevanja je zdaj močno poenostavljen. Uporabnik na spletni strani planer.arnes.si začne s klikom na gumb "Ustvari novo anketo".



Slika 5: Planer – vstopna stran

Dovolj je, da v spletni obrazec vpiše ime ankete in njen opis. Če želi, lahko izbere tudi datum poteka in na ta način doseže, da je sodelovanje v anketi mogoče le do izbranega datuma. Na naslednjem zavihku ročno vpiše datume ali jih doda s klikom na koledarček. Za vsak datum lahko nastavi poljuben časovni termin. Če gre pri anketi za planiranje izleta, lahko uporabnik namesto datuma v izbor ponudi mogoče destinacije. Predogled prikaže, na kakšen način bo anketa prikazana sodelujočim. Po končanem postopku Planer vrne spletno povezavo, ki jo uporabnik pošlje sodelujočim. Če gre za splošno anketo, lahko povezavo tudi objavi na svoji spletni strani.

Udeležencem se po kliku na povezavo odpre stran, na kateri oddajo svoj odziv. Tu vpišejo le svoje ime in izberejo časovne termine ali druge ponujene možnosti, ki jim ustrezajo. Če želijo, lahko v polje pod svoj odziv napišejo tudi krajši komentar. S klikom na gumb "Potrdi" se njihov odziv shrani.



SLIKA 6: PLANER – REZULTATI GLASOVANJA

Planer sproti sešteva glasove in prikazuje rezultate za posamezne časovne termine in ostale možnosti. Sodelujoči lahko kadarkoli odprejo anketo in vidijo trenutno stanje glasovanja. Po datumu poteka je anketa s končnimi rezultati še vedno vidna, le novih odzivov ni mogoče dodajati.

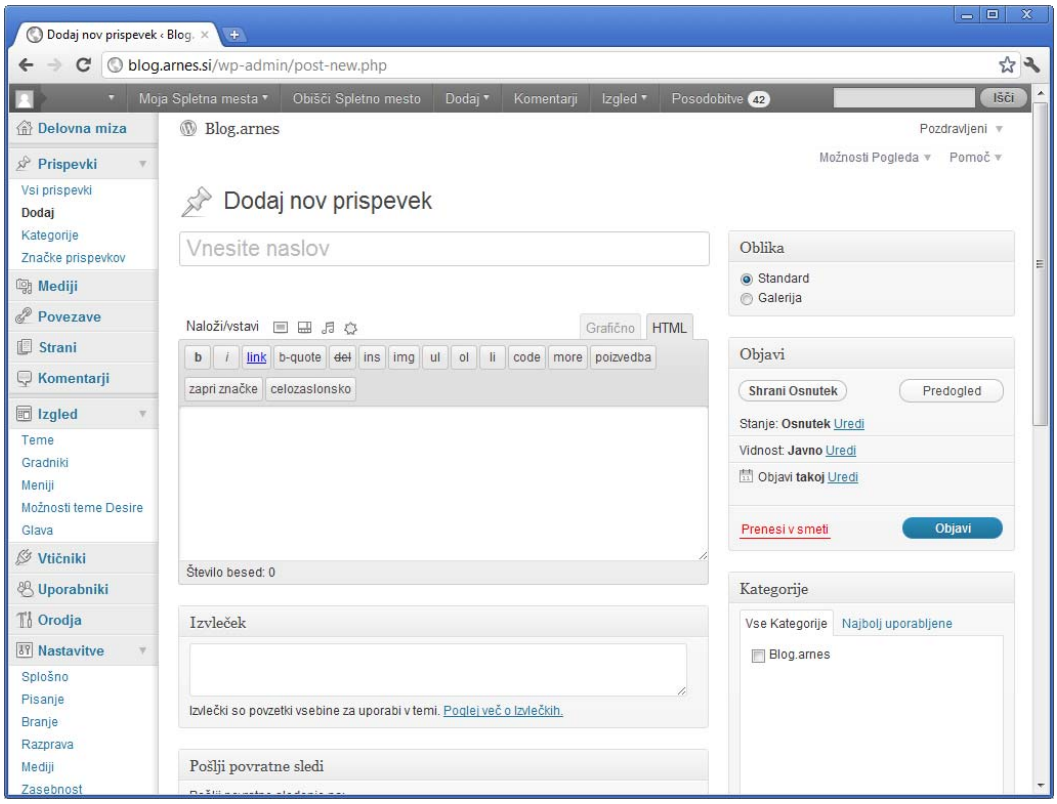
Blog.arnes

Blog ali spletni dnevnik se je najprej uporabljal kot osebna spletna stran, namenjena pisanju spletnega dnevnika, komentiranju in opisu dogodkov. Vsebina je bila obogatena le s slikami, kasneje sta se jim pridružila še zvok in video. V zadnjem času je vse bolj popularna integracija z družbenimi omrežji. Prispevki blogov so po navadi prikazani v obratnem kronološkem zaporedju. Tako obiskovalcem ob vsakem ogledu postrežejo z najnovejšimi objavami. Večina blogov je interaktivnih in obiskovalcem omogoča npr. komentiranje prispevkov, sodelovanje v anketah, nekateri tudi nalaganje slik. S časom je postala uporaba bloga enostavnejša, saj so na voljo platforme, ki za uporabo ne zahtevajo veliko tehničnega znanja. Blog je iz platforme za osebni spletni dnevnik prerasel v vsesplošno orodje za enostavno pripravo dinamičnih spletnih vsebin. Številne teme in vtičniki omogočajo spremembo videza in funkcionalnosti bloga ter ga naredijo uporabnega tako za osebno kot poslovno rabo.

SLIKA 7: BLOG.ARNES.SI

Blog.arnes je na voljo vsem uporabnikom Arnesovih storitev in omogoča prijavo z uporabniškim računom guest.arnes.si ali ArnesAAI. S klikom na gumb "Ustvarite novo spletno mesto" se sproži postopek registracije novega spletnega mesta oz. bloga. Uporabnik po prijavi s svojim uporabniškim imenom in geslom vpiše le še poddomeno spletnega mesta, njegovo ime in klikne na gumb za potrditev. Spletno mesto je takoj pripravljeno za uporabo.

Za pripravo novega prispevka uporabnik vpiše naslov, doda vsebino prispevka, ki jo lahko obogati s slikami ali videom, in ga objavi na svojem spletnem mestu.



SLIKA 8: BLOG.ARNES – PRISPEVEK

Obiskovalci, ki želijo redno spremljati dogajanje na blogu, se lahko naročijo na vire RSS. RSS je protokol za objavo in razpošiljanje spletnih vsebin v zapisu XML. Tako lahko kar v svojem odjemalcu e-pošte spremljajo nove prispevke z želenih spletnih dnevnikov.

Nekateri uporabniki bodo najprej spremenili izgled bloga, da bo bolje ustrezal vsebini, ki jo bodo objavljali. Ker so naši uporabniki različni in ima vsak svojo predstavo o tem, s kakšnim blogom se bo predstavil na svetovnem spletu, smo dali na izbiro teme: od enostavnih ali minimalističnih do osebnih ali poslovnih. Menjava tem je zelo enostavna. Dovolj je klik na povezavo "Vključi" pri posamezni temi in rezultat je takoj viden na blogu.

Del strani, ki sestavljajo blog, so tudi gradniki. Njihova uporaba da obiskovalcem na voljo nekaj dodatnih možnosti za navigacijo po blogu, kot npr. prikaz:

- seznama strani bloga,
- najpopularnejših prispevkov,
- zadnjih 5 prispevkov,
- največkrat komentiranih prispevkov,
- zadnjih komentarjev in
- polja za iskanje po blogu.

Podobno kot teme omogočajo spremembo izgleda, vtičniki dopolnjujejo in razširjajo obstoječo funkcionalnost spletnega mesta. Z njimi smo na primer dodali galerijo z možnostjo urejanja slik, v pripravi prispevkov smo omogočili neposredno iskanje in vključevanje povezav, slik ali videa kar s spleta. V času pisanja so v pripravi vtičniki za preusmeritev lastne domene na blog, Google Analytics in Facebook Like.

Zaključek

Planer omogoča planiranje sestankov, časovno usklajevanje in izdelavo preprostih anket, torej razpošiljanje elektronskih sporočil udeležencem in ročno zbiranje odgovorov ni več potrebno. Vsi odzivi se zbirajo na enem koncu in pregled rezultatov je takojšen.

Blog je iz platforme za osebni spletni dnevnik prerasel v vsesplošno orodje za enostavno pripravo dinamičnih spletnih vsebin. Uporaba spletnega dnevnika uporabnikom prinese novo dimenzijo objavljanja svojih vsebin na internetu. Objavljanje prispevkov na Blog.arnes je enostavno, besedilo pa je lahko dodatno popestreno s slikami ali video vsebino. Velika izbira preoblek oz. tem omogoča, da spletni dnevnik spremeni svoj izgled in postane spletna stran organizacije, projekta ali osebna spletna stran. Arnes sproti pripravlja nove teme in vtičnike ter jih postopoma vključuje v storitev. Z Blog.arnes so naši uporabniki dobili sodobno in enostavno orodje za izdelavo svoje spletne predstavitve.

Viri

1. Arnes. 2012. Planer – vstopna stran. Dostop: planer.arnes.si (30. 1. 2012).
2. Arnes. 2012. Blog.arnes – vstopna stran. Dostop: blog.arnes.si (30. 1. 2012).

Jure Kranjc,
Arnes

Webmin – spletni vmesnik za upravljanje Arnesovih strežnikov GVS
Webmin – Arnes virtual servers managment web interface

Povzetek

Storitev gostovanje virtualnih strežnikov, ki jo ponujamo na Arnesu, vsako leto pridobiva nove uporabnike. Storitev redno nadgrajujemo in posodabljamo ter iščemo dodatne rešitve, ki bi uporabniku omogočale lažjo in varnejšo uporabo strežnikov. V začetku leta 2012 smo na virtualne strežnike namestili spletno orodje Webmin, ki uporabnikom omogoča večjo svobodo pri upravljanju s strežniki. Preko spletnega vmesnika je mogoče spremljati porabo sistemskih virov, pregledovati dnevniške datoteke, dodajati navidezne gostitelje, spreminjati gesla sistemskim uporabnikom in spreminjati pravice datotek in map. Doslej smo lahko nekatere operacije izvajali le na Arnesu, danes pa lahko uporabniki sami uredijo več nastavitev in tako skrajšajo čas, ki je potreben za vzdrževanje spletnih aplikacij.

Ključne besede: virtualni strežnik, Webmin, grafični vmesnik.

Abstract

Arnes' virtual server hosting service is becoming increasingly popular every year. We regularly upgrade and modernise the service, seeking additional solutions making it easier and safer for users to use servers. In early 2012, we installed the Webmin web tool on the server, offering users greater freedom in managing servers. The web interface allows users to change the use of systems resources, review daily logs, add virtual hosts, change system user passwords and alter file and folder rights. Previously some operations could only be carried out at Arnes, but today users themselves can do more of the configuration, cutting the time needed to maintain web applications.

Key words: virtual server, Webmin, web administration

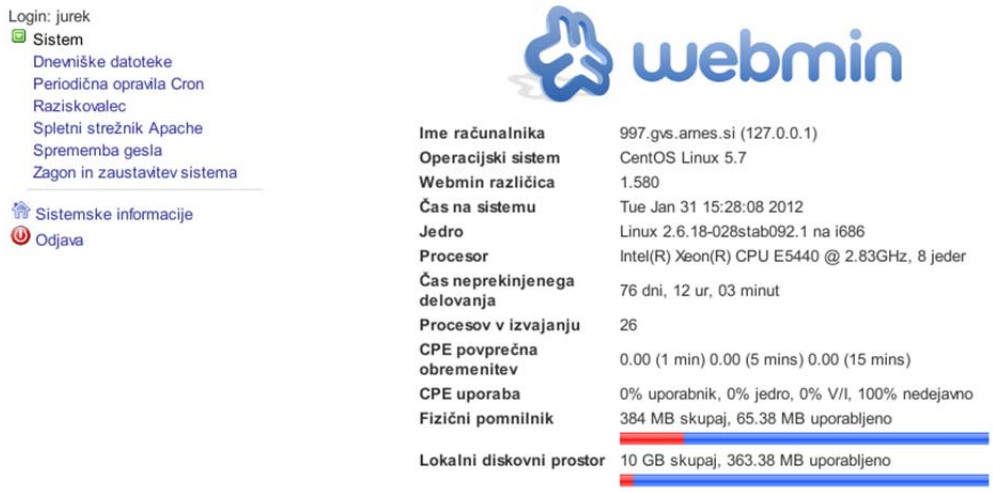
Uvod

Gostovanje virtualnih strežnikov vključuje tri pakete gostovanja, ki se razlikujejo glede na aplikacije, ki so nameščene na sistemu, in glede na pravice, s katerimi uporabnik razpolaga na strežniku. Uporabniki najbolj razširjenega paketa, tj. Asistenca, lahko na strežnik nameščajo poljubne spletne aplikacije, vendar so omejeni pri spreminjanju nastavitev operacijskega sistema. Težave predstavlja tudi uporaba operacijskega sistema Linux, ki zahteva poznavanje različnih sistemskih orodij za opravljanje enostavnih nalog. S spletnim orodjem Webmin je administracija virtualnega strežnika lažja in hitrejša.

Webmin

Veliko uporabnikov virtualnih strežnikov za svoje učne potrebe na strežnike namesti spletno stran in spletne učilnice. Čeprav so namestitve aplikacij postale zelo enostavne, mora skrbnik spletne strani za vzdrževanje in napredno uporabo

aplikacij poznati vsaj osnovne ukaze za delo z operacijskim sistemom Linux, omrežne protokole, DNS in podobne omrežne rešitve. Preusmerjanje domen in poddomen zahteva poznavanje spletnega strežnika (Apache). Včasih je potrebno tudi spreminjanje lastništva datotek, da lahko uporabljamo vse funkcionalnosti spletnih aplikacij.



Webmin je modularno zasnovana platforma, ki preko grafičnega spletnega vmesnika predstavlja konfiguracijske datoteke strežnika Linux. Vsak modul je odgovoren za svojo storitev, module lahko napišemo in dodajamo tudi sami. Zaradi takšne zasnove je lahko glavni program zelo majhen in porabi malo sistemskega pomnilnika. Program teče pod uporabniškim imenom korenskega uporabnika in tako uporabnikom, ki sicer nimajo pravic za spreminjanje nastavitev sistema, omogoča, da le-te spreminjajo.

Webmin je nameščen na vse virtualne strežnike – paket Asistenca, uporabniki do vmesnika dostopajo z obstoječim uporabniškim imenom in geslom za operacijski sistem. Na teh virtualnih strežnikih so najbolj uporabne operacije spreminjanja pravic datotek in map spletnih aplikacij, preusmerjanje poddomen v različne mape na strežniku ter spremljanje dnevniških datotek ob nadzoru delovanja storitev in odpravljanju napak na strežniku.

Zaključek

Skrbniku spletne strani poleg oblikovanja spletnih strani ali urejanja spletnih učilnic prestavlja dodatno delo skrb za sistem, ki ga je za zanesljivo delovanje spletne strani treba opraviti. Nepoznavalcem operacijskega sistema Linux vzame precej časa, da se naučijo novih operacij, ki jih morajo obvladati za nameščanje aplikacij, njihovo vzdrževanje in odpravljanje napak. S spletnim vmesnikom Webmin smo uporabnikom približali upravljanje sistema in skrajšali čas, potreben za vzdrževanje. Zaradi zasnove vmesnika pa lahko v prihodnje funkcionalnosti brez težav razširimo.

Viri

1. Arnes. 2012. Dinamično gostovanje (PHP/MySQL). www.arnes.si/gvs. Dostop:
   1. 2. 2012.
2. Webmin. 2011. Webmin – vstopna stran. Dostop: 1. 2. 2012.

David Vrtin,
Arnes

Nov Arnesov videokonferenčni portal MCU
New ARNES MCU videoconferencing portal

Povzetek

Arnes od l. 2003 nudi vsem organizacijam s sobnimi videokonferenčnimi sistemi H.323 celovito storitev, ki vključuje večtočkovne videokonference, snemanje videokonferenc in s pretočnim videom prenos videokonferenc na splet ter vključitev videokonferenčnih sistemov organizacij v mednarodno videokonferenčno omrežje. Z nadgradnjo osrednjega videokonferenčnega strežnika v l. 2011 videokonference podpirajo visokokvalitetno sliko do vključno ločljivosti FullHD 1080p, osveževanje slike do 60 slik/s in prenos zvoka, primerljivega s kvaliteto glasbe z zgoščenk. Konec leta 2011 smo uporabnikom ponudili nov videokonferenčni portal MCU, na katerem lahko uporabniki samostojno upravljajo s svojimi videokonferenčnimi sobami ter snemajo in prenašajo dogajanje v videokonferenci v živo na splet. Vse to poteka na Arnesovih strežnikih. Nov spletni vmesnik olajša in poenostavi uporabo videokonferenc, saj le-tega ni več treba urejati z elektronsko pošto in telefonskimi klici na Arnes.

Ključne besede: videokonference, MCU, H.323, SIP, HD, FullHD.

Abstract

Since 2003, ARNES has offered all organisations with H.323 videoconferencing room systems a comprehensive service covering multipoint videoconferencing, videoconference recording and web streaming of videoconferences, as well as connecting organisations' videoconferencing systems to the international videoconferencing network. The upgrade of the main videoconferencing server in 2011 means that videoconferences now support high-definition pictures up to FullHD 1080p resolution, 60 frames/s refresh rates and CD-quality sound. At the end of 2011, we launched a new MCU videoconferencing portal allowing users to manage their videoconferencing rooms themselves and record and broadcast videoconference events live on the web. All of this takes place on ARNES servers. The new web interface makes it easier and simpler to use videoconferences, as they no longer need to be organised by email and telephone calls to ARNES.

Key words: video conference, MCU, H.323, SIP, HD, FullHD.

Videokonferenca, kaj je to?

Z videokonferencami smo se v tem času tako ali drugače srečali že vsi. Marsikdo jih tudi precej pogosto uporablja – najverjetneje bolj za osebno uporabo in običajno na svojem priljubljenem računalniku. Z njimi smo večinoma kar zadovoljni, še posebej, če so brezplačne in lahko z njimi privarčujemo pri telefonskih klicih, predvsem pri mednarodnih. Pravzaprav tukaj niti ne govorimo o videokonferencah v osnovni funkciji, saj je poudarek predvsem na prenosu zvoka, torej na telefoniji. Video je tukaj le dodaten »bombonček«, saj pride prav, ker lepo izgleda, ni pa nekaj, kar dejansko zahtevamo. Zakaj, kako dolgo še in kdaj se

bomo končno navadili, da bomo zahtevali bistveno več in vedeli, zakaj to zahtevamo?

Za osnovno igračkanje z videokonferencami je več kot dovolj vsaka poceni spletna kamera in brezplačen program na računalniku. Vendar na tak način ne moremo opraviti prehoda na višji nivo uporabe prave videokonferenčne tehnologije. Šele ko bomo uvideli, da nam je pri pogovoru pomembna tudi dobra slika sogovornika, in sicer ne iz radovednosti, temveč zgolj zaradi boljše, hitrejše in temeljitejše komunikacije in da lahko začutimo sogovornikove misli tudi v videu, v kretnjah, v obrazni mimiki itd., bomo na pravi poti, da bo videokonferenčna tehnologija uporabljena v vseh svojih možnostih.

Navajeni smo že, da videokonference uporabljamo tudi za skupno delo z dokumenti, s skupnimi datotekami, slikami ipd. ter prikazom posameznih aplikacij ali celotnega namizja sogovornikovega računalnika. Ta del videkonferenčne tehnologije je še posebej razvit pri rešitvah, ki temeljijo na spletni tehnologiji in zato tudi deluje tako, kot smo že navajeni iz brskanja po spletnih straneh.

Tudi na mobilnih telefonih imamo že kar nekaj let kamere, telefoni so večinoma povezani v dovolj hitro UMTS-omrežje in z enakim stroškom kot za običajno telefoniranje lahko z njim pokličemo na drug telefon z video klicem, z živo sliko. Čeprav za takšno video telefoniranje nimamo nič večjih stroškov kot za običajno telefoniranje in imamo vso potrebno opremo že pripravljeno, se ta storitev le redko uporablja in smo nanjo že skoraj pozabili. Zakaj ni uspešnejša? A res nočemo, da se s sogovornikom vidimo (da sogovornik ne vidi nas?) ali so vzroki drugje, je slika premajhna in preslaba?

Vrnimo se nazaj na video komunikacijo s pomočjo računalnikov. Začetki prvih videokonferenc z računalniki segajo v sredino 90-ih let prejšnjega stoletja. Od takrat je bilo zelo veliko sprememb na bolje. Računalniki so postali več kot dovolj zmogljivi tudi za video, spletne kamere so postale cenovno ugodne, so barvne in zelo kvalitetne, tudi s sliko polne visoke ločljivosti (FullHD), omrežne povezave so hitrejše, ... Imamo sploh še kakšne resne tehnične ovire? Seveda nekaj še. Precej programov za videokonference ima še vedno težave zaradi varnostnih politik omrežij (požarni zidovi) in privatnih omrežij (NAT). Boljši programi se tudi s tem problemom že precej dobro spopadajo.

Pa vendar, treba se je vprašati, o katerih programih dejansko govorimo. Vsakomur je eden ljubši od drugega in različni programi praviloma med seboj niso združljivi, ne znajo med seboj komunicirati. Na voljo imamo dve možnosti – počakati, da bo en sam program prevladal (in bomo imeli monopol enega podjetja) ali pa se zateči k standardom, kjer so programi, ki se pogovarjajo z istim jezikom (z istim standardom), med seboj združljivi in smo zato seveda neodvisni od enega proizvajalca, saj je le-teh več in si celo konkurirajo.

Najstarejša klasična telefonija, od analogne naprej, je standardizirana in zato nihče niti ne pomisli, da telefoniranje s telefona enega proizvajalca preko omrežja na telefon drugega proizvajalca ne bi delovalo. Tudi za pošiljanje in sprejemanje kratkih sporočil (SMS) med mobilnimi telefoni je samo po sebi umevno, da so vsi telefoni združljivi. Tudi zato nas zgodovina uči, da je pot, ki je usmerjena k standardizaciji komunikacij, pravilna pot.

Zato je za videokonference Arnes že leta 2003 začel s standardnimi, t. i. klasičnimi videokonferencami, ki za komunikacijo uporabljajo mednarodni standard H.323, sprejet v okviru ITU-T (International Telecommunication Union - Telecommunication Standardization Sector, http://www.itu.int/ITU-T).

Arnes in videokonference

Arnesove videokonferenčne storitve se izvajajo po standardu H.323, H.320 in SIP. H.323 je osnovni protokol za videokonference preko IP/internetnega omrežja, SIP pa se kaže kot njegov naslednik in ga podpirajo predvsem novejši videokonferenčni sistemi. H.320 je protokol za videokonference preko digitalnega telefonskega omrežja ISDN, ki se je uporabljal predvsem, preden je bilo mogoče učinkovito množično uporabljati H.323-videokonference. Sedaj je v uporabi le še izjemoma, predvsem ko zaradi določenih razlogov internetnega prenosa še vedno ni mogoče uporabiti, uporablja pa se tudi za povezavo običajnih telefonov (stacionarnih PSTN in ISDN ter mobilnih GSM/UMTS) v skupne videokonference.

Arnesovi strežniki omogočajo medsebojno povezavo vseh zgoraj omenjenih videokonferenčnih sistemov na organizacijah tako v eno skupno kot v več ločenih videokonferenc. Z nadgradnjo osrednjega videokonferenčnega strežnika za večtočkovne videokonference (MCU, Multipoint Control Unit) v l. 2011 Arnes omogoča uporabo naslednjih naprednih videokonferenčnih funkcionalnosti:

- podpora videu za prikaz žive slike uporabnikov z videokonferenčnimi sistemi, ki pošiljajo sliko od standardne ločljivosti SD (Standard Definition) CIF 352 x 288 točk do videa polne visoke ločljivosti FullHD (Full High Definition) 1080p30 1920 x 1080 točk;
- podpora tekoči sliki z osveževanjem slike do vključno 60 slik/s;
- podpora uporabi drugega video kanala za posredovanje video namizja računalnika v videokonferenco (PowerPoint, Impress predstavitve ipd.) z uporabo standarda H.239 (za uporabnike H.323) in BFCP (za uporabnike SIP). Zaradi zahtevane berljivosti računalniške slike preko videokonferenčne povezave mora biti prenos videa v drugem video kanalu v dovolj visoki ločljivosti, tudi že pri najstarejših H.323-sistemih, ki podpirajo H.239, da ne prihaja do popačitve slike. Priporočljiva ločljivost računalniške slike je XGA, 1024 x 768 točk. Starejši in s tem manj zmogljivi sistemi dosegajo to ločljivost na račun nižje hitrosti osveževanja slike (do 8 slik/s) in zato ta kanal ni primeren za prikaz video posnetkov. Arnesov MCU-strežnik sicer omogoča v drugem video kanalu tudi ločljivost 720p30 (1280 x 720 točk, 30 slik/s) in 1080p15 (1920 x 1080 točk, 15 slik/s), kar se uporablja v najnovejših sobnih videokonferenčnih sistemih;
- inteligentno višanje ločljivosti (angl. upscaling) slike starejših (SD) videokonferenčnih sistemov za izboljšano sodelovanje z novejšimi (HD in FullHD) videokonferenčnimi sistemi;
- podpora videokonferenčnim hitrostim do 4 Mb/s za vsako videokonferenčno točko, neodvisno od povezav drugih videokonferenčnih točk, ki so priključene v isto videokonferenco;
- samodejna pretvorba med različnimi avdio in video kodeki ter hitrostmi video točk v isti videokonferenčni sobi omogoča, da se vsaka video točka priključuje z njej optimalnimi parametri;

- uporabljena pasovna širina do posamezne video točke se ne povečuje, tudi če se povečuje število sodelujočih video točk v videokonferenci;
- podpora priklopu slike namizja računalnika v videokonferenco z VNC-programi, kar je uporabno predvsem za uporabnike s starejšimi sobnimi sistemi, ki nimajo podpore za uporabo drugega video kanala;
- podpora dostopu do videokonferenc na Arnesovih MCU-strežnikih s prostodostopnim brezplačnim programom ConferenceMe, ki omogoča priklop (do 12 hkratnih uporabnikov na MCU) v videokonferenco tudi z omrežij, ki so zelo omejene s požarnim zidom, tudi s komunikacijo s tunelom samo preko vrat TCP 80, ki se uporablja za spletne strani in je zato najpogosteje dovoljen način komunikacije na internetu;
- podpora prenosu zvoka od kvalitete, ki jo poznamo v klasični telefoniji (frekvenčna širina 3,4 kHz), preko 7 kHz frekvenčne širine do kvalitete zvoka, ki je že primerljiva s kvaliteto predvajanja glasbe z zgoščenk (frekvenčna širina 14 kHz);
- podpora naprednim, zelo učinkovitim in procesorsko zahtevnim video kodekom (H.264) brez omejitve funkcionalnosti videokonferenc;
- združljivost najsodobnejših H.323- in SIP-videokonferenčnih sistemov z najstarejšimi H.323- in H.320-videokonferenčnimi sistemi;
- podpora H.323- in SIP-videokonferencam za uporabnike, ki so priključeni samo na IPv6-omrežje. S tem se lahko v isti videokonferenčni sobi na Arnesovem MCU hkrati vidijo in slišijo uporabniki, ki se povezujejo tako preko IPv4 kot tudi IPv6.

Videokonferenčna oprema na organizacijah

Videokonferenčno opremo delimo na sobne (skupinske, strojne) in namizne (osebne, programske) videokonferenčne sisteme.

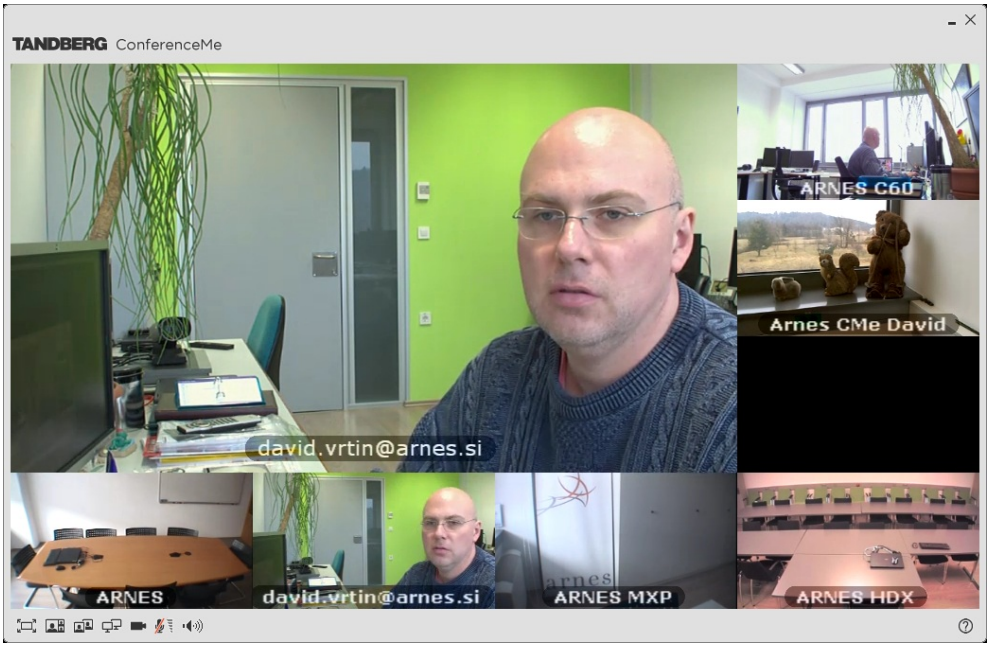
Za sobne videokonferenčne sisteme je značilno, da:

- vključujejo dobro kamero in dober namizni mikrofon;
- potrebujejo le priklop na projektor, plazma ali LCD-zaslon in zvočnike (kot priklop računalnika);
- namenjeni so za množico ljudi z ene lokacije (učilnica, predavalnica, sejna soba);
- uporaba je udobna in slušalke niso potrebne;
- praviloma ni nobenih težav z zvokom (odmev ...);
- so za pogosto uporabo stalno nameščeni in priključeni;

Slika 1: Sobni videokonferenčni sistem s kamero in namiznimi mikrofoni, ki je priključen na LCD TV

Za namizne videokonferenčne sisteme je značilno, da:

- potrebujejo USB ali podobno spletno kamero (25–100 €) na računalniku in mikrofon, ki je običajno že vgrajen v spletno kamero;
- potrebujejo H.323- ali SIP-videokonferenčni program (brezplačni preiskusni, sicer od 30 € naprej);
- priporočljiva je uporaba slušalk;
- namenjene so bolj za osebno uporabo;
- z nekaj truda in dodatne opreme (zunanja kamera, mikrofon) se približajo skupinskim sistemom.



Slika 2: Namizni videokonferenčni sistem, priključen v večtočkovno videokonferenco

Snemanje in prenos videokonferenc na splet

Celotno dogajanje v videokonferencah, vključno z drugim video kanalom (H.239, BFCP), je mogoče preko Arnesovih strežnikov spremljati v živo tudi brez uporabe videokonferenčne opreme, in sicer z uporabo tehnologije pretočnega videa, s spletnim brskalnikom in uporabo programov Microsoft WindowsMedia, Apple QuickTime ali RealNetworks RealOne na strežniku VCR (http://vcr.arnes.si).

Videokonferenco je mogoče z Arnesovim VCR-strežnikom tudi posneti, posnetek videokonference pa je na spletu na voljo za ogled takoj po koncu videokonference, na enak način kot prenosi v živo. Glede na želje organizatorjev posameznih videokonferenc je dostop do posnetkov izbranih videokonferenc mogoče zaščititi z geslom.

Ob glavnem video kanalu (slike iz kamer) in zvoku iz videokonference je tako pri prenosu v živo kot pri posnetkih tudi drugi video kanal (slika predstavitve iz računalnika) samodejno sinhroniziran z glavnim video kanalom in zvokom.

Z nadgradnjo Arnesovega MCU-strežnika v l. 2011 je mogoče Arnesov VCR-strežnik uporabljati tudi v načinu, ki omogoča snemanje videokonferenc tako, da je tudi posnetek videokonferenc v visoki ločljivosti HD (1280 x 720 točk).

Posnetki nekaterih videokonferenc so objavljeni na spletu v Arnesovem arhivu videokonferenc kot video na zahtevo na http://www.arnes.si/video/vod/ (VoD, Video On Demand).

Mednarodna povezljivost

Arnesovi strežniki vratarji (angl. gatekeepers) omogočajo polno vključitev H.323-videokonferenčnih sistemov organizacij v mednarodno videokonferenčno klicno omrežje GDS (Global Dialing Scheme) pod številčnim prostorom »00386«. V začetku leta 2012 je bilo pod predpono 00386 registriranih 182 videokonferenčnih sistemov.

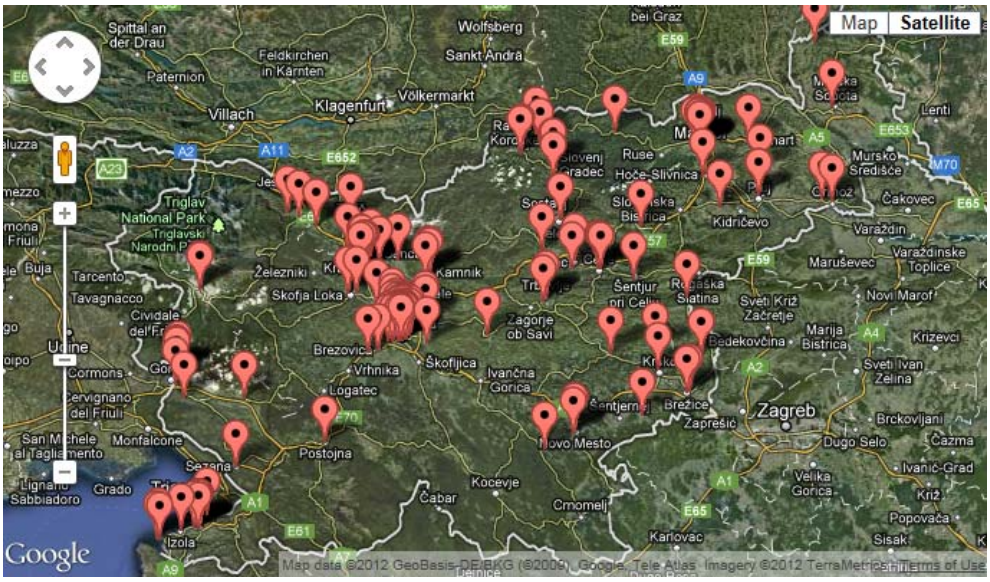
S tem so Arnesove videokonferenčne storitve, vključno z večtočkovnimi strežniki, enostavno povezljive s podobnimi videokonferenčnimi sistemi v tujini.

Uporabniki Arnesovih videokonferenčnih storitev

V videokonferencah najpogosteje sodelujejo osnovne in srednje šole ter fakultete, ki običajno že imajo namenske skupinske/sobne videokonferenčne sisteme H.323 (133 organizacij). Večina (126) sobnih sistemov je bila pridobljena preko petih javnih razpisov, ki jih je izvedlo Ministrstvo za šolstvo v letih od 2000 do 2009 (proizvajalci VCON, Aethra, Tandberg in LifeSize). Tako je sobne sisteme pridobilo 48 osnovnih in 37 srednjih šol.

Organizacije, ki sobnih sistemov še nimajo, se lahko v videokonference povezujejo z osebnimi/namiznimi videokonferenčnimi sistemi, s spletno kamero (angl. USB webcam) in H.323- ali SIP-odjemalcem na osebnem računalniku (komercialni Cisco Jabber Video/Movi, Polycom m100, Polycom PVX, Mirial SoftPhone in Spranto ter brezplačnim Cisco/Tandberg ConferenceMe).

Konec leta 2010 je Arnes na spletni strani http://www.arnes.si/video/h323 objavil imenik vseh 161 organizacij s H.323-videokonferenčno opremo.



Slika 3: Imenik organizacij s H.323-videokonferenčno opremo, http://www.arnes.si/video/h323

Videokonference se najpogosteje uporabljajo za:

1. redna predavanja v okviru mednarodnih projektov in delovne sestanke (profesorji, študenti);
2. izvedbo predavanja, pri čemer so študenti zbrani v predavalnicah v različnih krajih po Sloveniji;
3. pouk v srednjih šolah v okviru medpredmetnega sodelovanja med šolami;
4. za večje videokonferenčne dogodke, kjer nekaj 10 organizacij predstavlja in razpravlja o svojih projektih;
5. omogočanje sodelovanja (predavanje) na konferencah z oddaljenih lokacij preko videokonferenčnih povezav;
6. prenos dogajanja z lokacij konferenc in drugih zanimivih dogodkov na splet.

Arnesov MCU-portal

V letu 2011 je Arnes razvil lasten spletni portal http://mcu.arnes.si, ki uporabnikom H.323- in SIP-videokonferenčnih storitev omogoča spletni dostop do upravljanja z Arnesovimi večtočkovnimi MCU-strežniki in strežniki za snemanje, prenos v živo in objavo posnetkov videokonferenc na spletu.
MCU-portal je od decembra 2011 v pilotnem obratovanju in uporabnikom s prijavo preko infrastrukture ArnesAAI omogoča, da:

- samostojno ustvarjajo in rezervirajo videokonferenčne sobe;
- upravljajo s svojimi videokonferenčnimi sobami in s tistimi sobami, za katere so jim drugi uporabniki dovolili upravljanje;
- ročno ali samodejno snemajo celotno dogajanje v videokonferenčnih sobah;
- vzpostavljajo videokonferenčne klice z MCU-strežnika k uporabnikom in prekinjajo videokonferenčne klice povezanim video točkam;
- izklapljajo in vklapljajo sprejem zvoka in videa priključenim video točkam;

- prenašajo celotno dogajanje v videokonferenčnih sobah v živo na splet (pretočni video);
- na spletu objavljajo posnetke dogajanj v videokonferenčnih sobah.

V decembru 2011 je bilo na lokaciji Arnesa izvedeno prvo izobraževanje za uporabnike Arnesovega MCU-portala. Izobraževanje, ki je namenjeno predvsem uporabnikom sobnih videokonferenčnih sistemov, se bo praviloma enkrat mesečno izvajalo tudi v letu 2012.

V letu 2012 se bo portal še dopolnil:

- z naprednimi funkcionalnostmi, ki jih omogočajo MCU-strežniki;
- s samodejno pretvorbo posnetkov videokonferenc v Flash video format;
- s samodejnim nalaganjem posnetkov videokonferenc na Arnesov video portal http://video.arnes.si/;
- s prenosom videokonferenc v živo v Flash video formatu;
- z implementacijo servisne strani za upravljanje registracij GDS-številk.

S podporo standardom H.460.18/H.460.19 in H.460.23/H.460.24 se bo v letu 2012 izboljšala in poenostavila uporaba videokonferenc iz zaprtih in/ali privatnih omrežij (NAT).

Jasmina Mešić,
Arnes, SI-CERT

Program Varni na internetu – ob letu osorej
Safe on the Internet Program – One Year Later

Povzetek

Leto dni je že minilo od predstavitve projekta ozaveščanja Varni na internetu slovenski javnosti. 7. februarja 2012, ob svetovnem dnevu varne rabe interneta, smo lahko rekli, da se že okroglo leto trudimo z najrazličnejšimi aktivnostmi dvigniti stopnjo informiranosti o varni rabi interneta. Kratek zasuk v leto 2011 bo pokazal, kako je spletna javnost sprejela naš izobraževalni portal www.varninainternetu.si, katere spletne goljufije so najbolj odmevale, katera komunikacijska orodja smo uporabili za doseganje ciljnih javnosti in zakaj se je sovražnik Facebook izkazal za odličnega zaveznika našega projekta.

Ključne besede: program ozaveščanja, varna raba interneta, spletne goljufije, komunikacijska kampanja.

Abstract

It's one year since the Safe on the Internet public awareness campaign was introduced to the Slovenian public. On February 7 2012 – World Safer Internet Day – we marked the first year of activities aimed at raising public awareness of information security. A brief review of 2011 will show how the web public has accepted our educational portal www.varninainternetu.si, and reveal the most common online frauds, the communications tools we used to reach our target audience, and why the enemy – Facebook – has proven to be an excellent ally of our project.

Key words: awareness raising program, safe use of the Internet, online frauds, communication campaign

Uvod

SI-CERT, slovenski center za posredovanje pri omrežnih incidentih, je v začetku leta 2011 prevzel koordinacijo nacionalnega programa ozaveščanja javnosti o informacijski varnosti – Varni na internetu. Inicializacija projekta je odziv na naraščajoče število različnih oblik spletnih goljufij – tudi takšnih, katerih posledica je finančno oškodovanje. Gotovo je pomemben vidik programa opozarjanje in svetovanje o zaščiti pred zlonamernimi programi, vendar danes spletne nevarnosti prevzemajo vedno bolj človeško podobo. Ravno zato s programom Varni na internetu ne poudarjamo zgolj tehničnih vidikov zaščite, ampak je na prvem mestu izobraževanje spletnih uporabnikov. Cilji programa so:

- poučiti spletne uporabnike o različnih oblikah spletnih goljufij – kako jih lahko prepoznajo in kako se pred njimi zavarujejo,
- informirati o varni uporabi spletnega bančništva in varnem spletnem nakupovanju,
- poučiti spletne uporabnike tudi o tem, kako naj zavarujejo svojo osebno identiteto na spletu, predvsem na družbenih omrežjih.

Vsebine programa Varni na internetu naslavljajo široko slovensko spletno javnost, ciljamo pa predvsem na uporabnike, starejše od 25 let, saj ta populacija že uporablja storitve spletnega bančništva in tudi opravi največji delež spletnih nakupov. Kampanja torej cilja predvsem na odrasle uporabnike interneta. Poseben sklop vsebin namenjamo manjšim podjetjem, ki pri svojem poslovanju prav tako uporabljajo spletno bančništvo in spletne trgovine.

1. Komunikacijske aktivnosti

Poglavitno sporočilo programa Varni na internetu smo strnili v slogan »Od mene je odvisno vse.«, saj spletni uporabniki lahko sami storijo največ za zmanjšanje tveganja. Vendar potrebujejo jasna, natančna in razumljiva navodila, kako naj zavarujejo svojo spletno identiteto, računalniško opremo in ne nazadnje tudi svoj bančni račun. In ravno to je naša naloga zadnje leto dni – s pomočjo različnih komunikacijskih kanalov in aktivnosti izobraževati, pomagati, obveščati, opozarjati in deliti znanje s široko spletno javnostjo.

1.1 Izobraževalni portal in prijavna točka

V središče programa ozaveščanja postavljamo izobraževalni portal www.varninainternetu.si, na katerem gradimo bazo znanja s področja informacijske varnosti. Problematiko varnosti na spletu obravnavamo celostno. Podajamo definicije izrazov, opise spletnih prevar, študije konkretnih primerov, usmeritve na relevantne zunanje vire, nasvete – tudi v obliki video navodil. V letu 2011 smo portal oblikovno in funkcionalno nadgradili. Zaživela je tudi prijavna točka oz. spletni obrazec na portalu, preko katerega lahko oškodovanci prijavijo omrežni incident (vdor, goljufija, kraja identitete itd.).

1.2 Družbeni mediji – v središču dogajanja

Številne organizacije, ki delujejo na področju informacijske varnosti, pogosto opozarjajo na pasti družbenih omrežij. Ogromna, medsebojno povezana množica uporabnikov družbenih omrežij omogoča še hitrejše širjenje zlonamerne kode in spletnih prevar, problematično pa je tudi zelo nekritično deljenje osebnih informacij s strani samih uporabnikov. Vendar se je izkazalo, da omrežje Facebook ni zgolj vir težav, ampak je lahko tudi zelo učinkovit medij za posredovanje informacij. Ravno povezanost ljudi omogoča hitro obveščanje o različnih odkritih prevarah, kar smo obrnili v korist programa ozaveščanja. Facebook stran Varni na internetu in Twitter račun @varninanetu nam omogočata, da smo v središču dogajanja in hitro posredujemo obvestila o novo odkritih spletnih nevarnostih.

1.3 Nasvet iz prve roke – z informacijsko točko Varni na internetu po Sloveniji

Mesec maj je bil v znamenju varne rabe interneta. Z mobilno info točko smo obiskali večja nakupovalna središča v Celju, Ljubljani in Mariboru, naše vodilo pa je bilo – nasvet iz prve roke. Obiskovalci so lahko izvedeli vse o kraji gesel, lažnih Facebook profilih, spletnih goljufijah ter drugih spletnih nevarnostih. Vsak obiskovalec je dobil posebno darilo – zobno ščetko z enkratno zgodbo.

1.4 Medijska kampanja

Ena najpomembnejših aktivnosti na področju informiranja javnosti je gotovo medijska kampanja. Oglaševalska kampanja Varni na internetu je potekala v tradicionalnih (tisk, radio, televizija) in tudi digitalnih medijih (medijski portali, družbena omrežja), z integriranim pristopom smo težili k čim večjemu dosegu ciljnih javnosti, torej tako starejših kot mlajših spletnih uporabnikov.

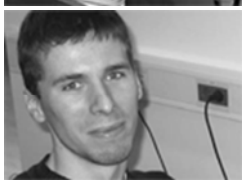
2. Izpostavljeni primeri

Najodmevnejši primeri, ki smo jih obravnavali v sklopu programa Varni na internetu, so bili povezani s spletnimi nakupi in prodajo. Povzamemo lahko, da so v letu 2011 spletni goljufi odkrili slovenske posredniške portale (bolha.net, avto.net, nepremicnine.net) in forume, ki so jih uspešno izkoristili za širjenje nigerijskih prevar. Eno najzanimivejšo obliko nigerijske prevare pa smo predstavili tudi v oddaji Odmevi, saj so prevaranti na spletnih forumih ponujali celo ugodne kredite. Škornji Uggice pa so se izkazali kot odlična krinka za privabljanje kupcev v lažne spletne trgovine. Tako smo razkrinkali lažno spletno trgovino uggbootseurope.com – obvestili smo ponudnika gostovanja spletne trgovine in dosegli njen umik, prav tako smo vzpostavili kontakt z Zvezo potrošnikov Slovenije. Sodelovanje z ZPS nadaljujemo tudi v prihodnje, saj imamo skupen cilj – opozarjati na pasti spletnega nakupovanja.

**Miha Dimec,
Aleš Zavodnik,
Matjaž Straus Istenič,
Miha Jemec,
Matej Vadnjal,
vsi Arnes**







Od optičnega vlakna do kakovostne komunikacije
From optical fibre to quality communication

Povzetek

Kakovostno komunikacijo omogoča zapleten splet različnih tehnologij. Omrežna storitev je nanizana v plasteh in sestavljena iz različnih elementov – od ustreznega prostora, električnega napajanja, bakrenih kablov ali optičnih vlaken, povezovalnih tehnologij do kompleksnejših omrežnih protokolov in programske opreme. Uporabniku je ta struktura skrita, kljub temu pa vsi njeni gradniki neposredno vplivajo na uporabnikovo izkušnjo pri uporabi omrežne storitve.

Prispevek in predavanja predstavljajo to sestavljenko s primeri iz prakse. Opisani so mehanizmi, s katerimi zagotavljamo in nadziramo kakovost komunikacije in omrežnih storitev: osnovna komunikacijska infrastruktura, tehnologija namenskih povezav ”točka–točka”, mehanizmi QoS in varna uporaba protokola IPv6 v lokalnih omrežjih. Prispevek zaključuje kratka predstavitev nekaterih orodij, s katerimi nadziramo in upravljamo Arnesovo omrežje.

Ključne besede: ustrezen prostor, infrastruktura, dokumentacija, optično vlakno, DWDM, CWDM, točka–točka, kakovost storitev, kakovost komunikacije, QoS, IPv6, samodejne nastavitve, SLAAC, DHCPv6, varnost omrežja, upravljanje omrežja, nadzor omrežja

Abstract

Systems engineers and network administrators acknowledge that quality assurance for network services is not straightforward. This group of talks will explore the daily challenges. A complex mesh of varied technologies enables quality communication. Network services are linked in layers and consist of various elements – suitable premises, electricity supply, copper cables or optical fibres, connection technologies for complex network protocols, and software. This structure is hidden from users, although all of its elements directly affect their experience of network services. The article and the conference talks describe this combination through practical examples. We will show the mechanisms we use to ensure quality communication and network services. We will describe the technology for dedicated point-to-point connections for services that require high quality, secure and private communications. We will emphasise the importance of the modern, easy-to-use IPv6 protocol. The talk concludes with an outline of a subset of tools used to monitor key connection parameters in the ARNES network.

Key words: proper conditions, infrastructure, documentation optical fibre, DWDM, CWDM, point-to-point, quality of service, quality of communication, QoS, IPv6, stateless autoconfiguration, SLAAC, DHCPv6, network security, network management

Kakovostna infrastruktura

Quality begins within the infrastructure

Miha Dimec

Kakovost komunikacije in storitve ni povezana zgolj s pretokom IP-paketkov, nastavitvami opreme in nadzorom. Kakovost storitve začnemo zagotavljati na področjih, ki na prvi pogled niso povezana z informacijsko tehnologijo:

- ustrezen prostor z vso potrebno infrastrukturo;
- zanesljiva povezljivost do ponudnika interneta;
- izdelan scenarij dogodkov, ki se lahko zgodijo in ki vplivajo na našo storitev;
- dokumentacija, ki poleg stanja vsebuje tudi vse pomembne kontaktne podatke.

The quality of communication depends not only on the configuration and monitoring of routers and switches. The work of providing quality communications begins in areas which many IT staff believe are not related to the quality of communications at all:

- Ensure that your IT equipment is located in a suitable room or place;
- Ensure that your connectivity to the ISP meets all the conditions for reliability and stability;
- Be prepared for many situations that may arise and affect the quality of your communications. Prepare procedures to solve the problem in advance;
- Documentation, documentation, documentation and documentation.

Pri zagotavljanju kakovostne komunikacije pogosto pozabljamo ali zanemarjamo pomembnost infrastrukture, na kateri gradimo in ponujamo svoje storitve. Na kakovost komunikacije posredno vplivajo vsi parametri prostora, v katerem se nahaja naša oprema, fizični potek povezljivosti do našega internetnega ponudnika, urejenost in vodenje naše dokumentacije ter usposobljenost in znanje naših ter zunanjih vzdrževalcev. V praksi ugotavljamo, da se ta problematika pogosto težko obrazloži projektantom, vodjem finančnega sektorja in (pri dokumentaciji) vzdrževalcem stavbe. Zato je namen tega prispevka izboljšanje stanja na omenjenem področju.

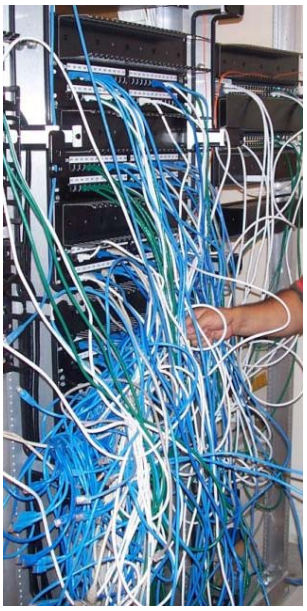
Komunikacijska in strežniška oprema, s katero izvajamo storitve, mora nekje imeti svoj prostor. Za tak prostor pa ne sme biti edini pogoj zgolj električni priključek. Prostor mora biti dovolj velik za vsa vzdrževalna dela, omogočati mora ustrezno klimo, imeti mora ustrezne električne priključke, zanesljive komunikacijske vode do ponudnika interneta, onemogočati dostop za nepooblaščene osebe in imeti vsaj osnovno protipožarno zaščito. Bo kakovostna komunikacija sploh še mogoča, če se bo oprema poleti pregrevala in zaradi tega nehala delovati? Bo oprema pravilno delovala, če bo njeno napajanje preobremenjeno z drugimi porabniki, kot so npr. sesalec, električni kuhalnik ipd.

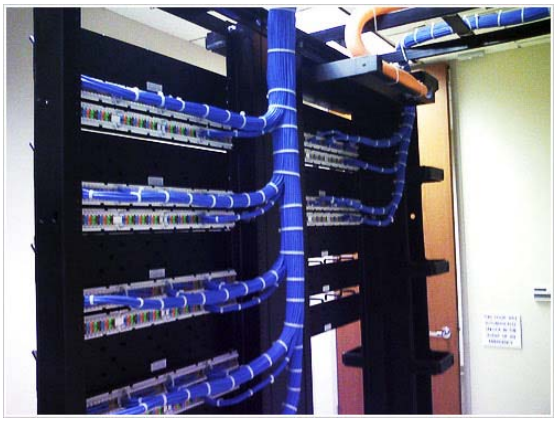
SLIKA 9: SODOBNA OMREŽNA INFRASTRUKTURA?

Prostor naj bo ustrezno velik, da so v njem mogoča vzdrževalna dela, da je prezračevanje ustrezno in ni »toplih con«, da lahko kasneje v njem montirate klimatsko napravo (mogoča montaža zunanje enote, odtok kondenza).

SLIKA 10: DOVOLJ PROSTORA ZA NEMOTENO DELO

Vzor za urejenost kablov naj ne bodo špageti v posodi kot tudi ne »state of the art«.





SLIKA 11: "ŠPAGETI" OMREŽJE ALI UMETNOST?

Povezava do ponudnika interneta bo omogočala kakovostnejšo storitev, če bo znano, kje poteka. Če nimate podatkov, kdaj se bodo izvajala določena vzdrževalna dela v vaši stavbi oz. njeni bližnji okolici, ali če nimate podatkov, ali se bodo dela izvajala na področju, kjer potekajo kabli od vas do vašega ponudnika interneta, vas lahko posledično preseneti nepričakovan daljši izpad vaših storitev. Povezava z dvema različnima ponudnikoma interneta še ne zagotavlja, da le-ta ne poteka po istem kablu, po istem kanalu ali isti ulici.

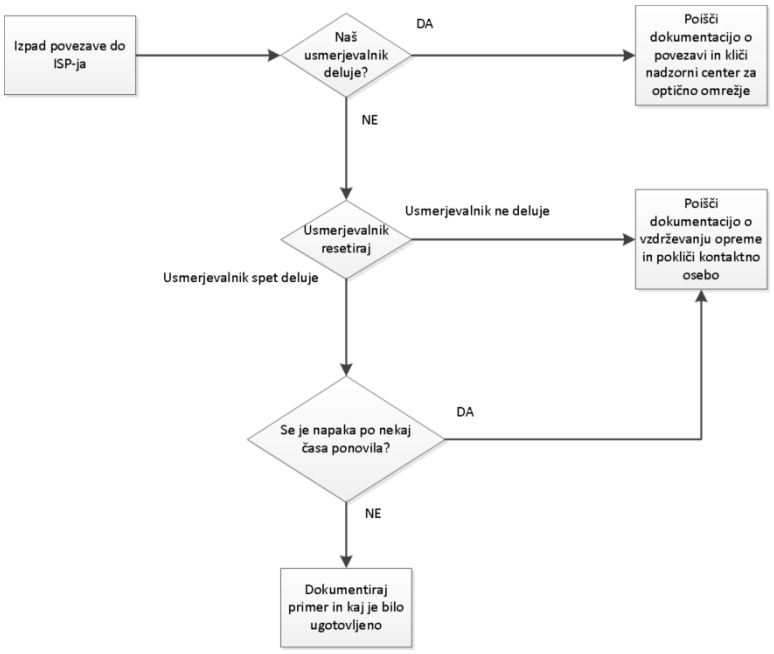
SLIKA 12: ZDAJ VEMO, KJE POTEKAJO NAŠE OPTIČNE POVEZAVE.

Dokumentacija je ključ do kakovostne storitve. Če nimate dokumentirane opreme, nastavitev, kontaktov ponudnika interneta, vzdrževalcev opreme, hišnikov, vzdrževalnih pogodb, garancij in odgovornih oseb, bo lahko izpad storitev dolgotrajen in bo negativno vplival na izkušnjo vaših uporabnikov.

Ob vzpostavitvi storitve predvidevajte mogoče dogodke, ki lahko vplivajo na njeno kakovost in pripravite scenarije, kako se jih lotiti; na primer v primeru okvare usmerjevalnika:

- Katere uporabnike moram o tem obvestiti in kako?
- Kje je rezervna oprema?
- Kje je shranjena konfiguracija?
- Kje je opisan postopek, kako shranjeno konfiguracijo postaviti na rezervno opremo?
- Ali za usmerjevalnik še velja garancija?
- Ali imamo za usmerjevalnik podpisano pogodbo o vzdrževanju?
- Kontaktni podatki servisne službe.
- Ali smo zabeležili vse podatke o izpadu storitve za kasnejša poročila?

Izdelajte graf poteka, ki naj bo čim bolj pregleden in enostaven. V krizi bo vaš zaveznik.



SLIKA 13: PRIMER GRAFA POTEKA, KAKO RAVNATI V PRIMERU TEŽAV V OMREŽJU

Na praktičnih primerih bo na predavanju razložena pomembnost dobrega načrtovanja, razgledanosti, dobrega dokumentiranja in postopkov ob težavah. Zagotavljanje kakovostnih storitev se začne pri infrastrukturi.

Viri

- Arnesova dokumentacija
- www.fotosearch.com
- spletni viri

Sodoben transport paketkov

Modern transport of packets

Aleš Zavodnik

Z naraščanjem prometa morajo ponudniki omrežij IP poiskati načine, kako zagotoviti zadostne kapacitete in prilagodljivost omrežij glede na zahteve uporabnikov. Skoraj vsi paketki v svetovnem spletu danes prepotujejo večji del svoje poti po optičnih vlaknih. Za zagotavljanje zanesljive poti najprej potrebujemo kakovostno optično vlakno. Ko nam optično vlakno ne nudi več zadostnih kapacitet, lahko uporabimo dodatna vlakna ali pa eno od WDM-tehnologij.[10] Trenutno nam na Arnesu
WDM-tehnologije omogočajo zagotavljanje več hkratnih 10-gigabitnih povezav, v načrtu pa imamo tudi že prve povezave prepustnosti 40 Gb/s, po potrebi pa bomo lahko podprli tudi 100 Gb/s.

Poseben poudarek je podan namenskim povezavam za posamezne zahtevnejše projekte, kar na Arnesu dosežemo z opremo, katere osnovni gradniki so obstoječa WDM-omrežja.

In dealing with increasing traffic, IP network providers need to find new ways to ensure sufficient network capacity and flexibility to meet user requirements. Today almost all packets travelling over the Internet are routed through optical fibres. To ensure reliable transport, you must first provide high quality optical fibre. When a fibre no longer offers sufficient capacity, we can use additional fibres or a WDM technology. ARNES WDM technology currently provides multiple concurrent 10-gigabit links, and we plan to upgrade some links to 40 Gbps. If required, we can also support 100 Gbps.

Particular emphasis is given to dedicated links for more complex and specific projects.

Equipment to support these new features was actually an upgrade of the existing ARNES WDM network.

Optično vlakno

Enorodovno optično vlakno je danes najbolj razširjeno. Ima zelo tanko sredico, narejeno iz čistega silicija, plašča in ovoja proti mehanskim poškodbam. Njihova prednost pred bakrenimi vodniki je predvsem v veliko večjih kapacitetah, nižji ceni, majhnih izgubah in lažjem vzdrževanju.

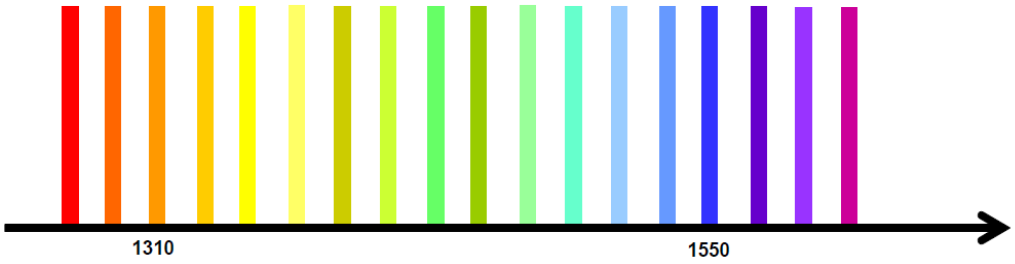
Za osvetlitev optičnega vlakna običajno uporabljamo dve valovni dolžini – 1310 nm in 1550 nm. Implementacija je preprosta, diode ali laserji svetijo v širokem pasu in niso temperaturno občutljivi.

[10] WDM ali Wavelength-division Multiplexing je tehnologija, ki omogoča prenos več signalov preko enega samega optičnega vlakna, tako da se za posamezne signale uporabi svetloba z različno valovno dolžino.

SLIKA 14: VALOVNE DOLŽINE SVETLOBE V OPTIČNEM VLAKNU.

CWDM – coarse wavelength division multiplexing

Ta tehnologija uporablja več valovnih dolžin s širino signala 20 nm. ITU-standard predvideva 18 kanalov v pasu od 1271 nm do 1611 nm. Uporablja se predvsem za krajše razdalje in je še vedno cenovno ugodna.



SLIKA 15: VALOVNE DOLŽINE KANALOV CWDM

DWDM – dense wavelength division multiplexing

Le-ta uporablja tako imenovani C-pas od 1530 nm do 1565 nm. ITU-standard predvideva različne širine signalov. Najpogosteje je uporabljena širina 0,8 nm, kar nam omogoča do 40 hkratnih kanalov. Ker so širine kanalov majhne, morajo biti komponente natančneje izdelane in temperaturno stabilne. Posledica je seveda višja cena gradnikov.

SLIKA 16: VALOVNE DOLŽINE KANALOV DWDM

Kakovostne storitve v omrežju ARNES

Za posebne projekte ali specifične želje lahko vzpostavimo posebne povezave znotraj Slovenije in tudi v tujino, kjer nam to omogoča infrastruktura evropskega

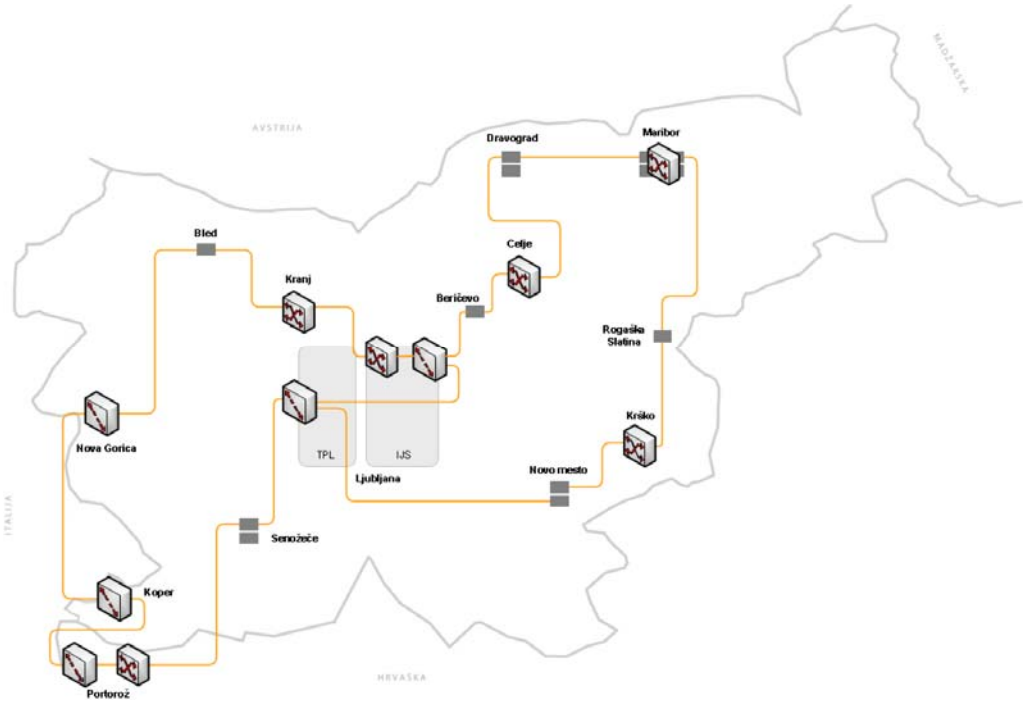
omrežja GÉANT. Takšne namenske povezave so ločene od produkcijskega IPv4- in IPv6-prometa. Uporabimo jih lahko za potrebe omrežij ”grid”, 3D-vizualizacij, omrežij v ”oblaku”, zahtevnih projektov v kemiji, genetiki, astronomiji, zdravstvu. Drugo področje uporabe je povezovanje redundantnih računalniških centrov in povezovanje fakultet v enotna omrežja.

Omrežje ARNES omogoča dva načina za vzpostavljanje tovrstnih povezav:

- Povezave prepustnosti 10 Gb/s vzpostavimo s pomočjo ločenih svetlobnih poti. Če potrebujemo večjo zanesljivosti, je treba vzpostaviti dve povezavi, vsako po svoji poti.
- Povezave prepustnosti 1 Gb/s lahko vzpostavimo s posebno opremo, ki omogoča zagotavljanje zasebnih ethernet povezav po dveh ločenih poteh skozi hrbtenico omrežja. V primeru prekinitve primarne poti se promet v manj kot 50 milisekundah samodejno preusmeri na rezervno pot.

Slika 17 prikazuje topologijo DWDM-omrežja in vozlišča, kjer je na voljo tovrstna oprema.

Seveda je treba tovrstne povezave speljati vse do ustrezne točke v omrežju priključene organizacije. Za ta namen priporočamo zakup dodatnih optičnih vlaken do hrbtenice omrežja ARNES ali pa uporabo tehnologije CWDM, ki poleg IP-povezave omogoča preko obstoječih optičnih vlaken vzpostavitev tudi namensko povezavo ”točka–točka”.



SLIKA 17: ZAGOTAVLJANJE NAMENSKIH POVEZAV V OMREŽJU DWDM

QoS – kakovost storitve

Just another word for dropping packets?

Miha Jemec

Ustrezno zagotavljanje kakovosti storitve posameznim tipom aplikacije (QoS) je v Arnesovem omrežju polno podprto. V prispevku si bomo podrobneje pogledali, kako so mehanizmi implementirani in kaj je bilo narejenega v zadnjem letu.

The ARNES network fully supports the provision of quality of service (QoS) to different kind of applications. This article examines how QoS is implemented and what has been done in the last year.

Kakovost storitve ima v omrežju ARNES že dolgo zgodovino. In veliko končnih uporabnikov, katerim omenjeni mehanizem (morda nevede) služi, bi lahko samo potrdilo, da so zadovoljni s storitvami, ki jih imajo, kar je ne nazadnje tudi najpomembnejše za zadovoljstvo uporabnikov omrežja. Mehanizmi zagotavljanja QoS namreč skrbijo, da imajo različni tipi aplikacij različne prioritete pri prenosu podatkov v omrežju in s tem dajejo uporabniku izkušnjo, da vse "pravilno" deluje. Bolj ali manj vsi poznamo motnje pri prenosu in gledanju IPTV, saj točno vemo, kako mora izgledati izkušnja pri gledanju televizije. Hkrati ne opazimo, če se prenos elektronske pošte ali odpiranje spletne strani zakasni za nekaj desetink sekunde. Zato lahko mirno odgovorimo, da je QoS na povezavah do Arnesovih članic nuja in daleč od naključnega odmetavanja paketov pri polnih povezavah.

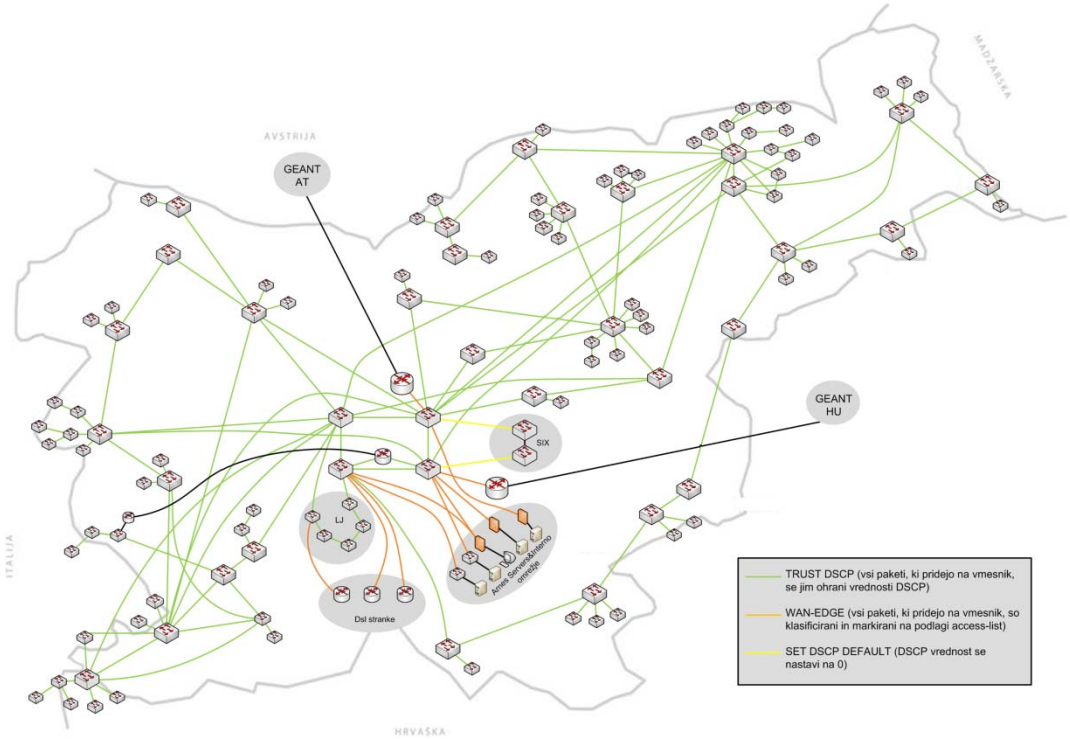
V primeru Arnesovih članic igra QoS najpomembnejšo vlogo pri končnih povezavah do članic, kadar je povezava narejena preko DSL-tehnologij. V vlogi IPTV v našem primeru večinoma nastopajo videokonference, v zadnjem času je vse več tudi telefonije (VoIP – *voice over IP*). Omenjeni dve storitvi imata pri prenosu paketov preko Arnesovega omrežja do članice (in obratno) vedno zagotovljeno najvišjo prioriteto. Sledijo jim storitve, ki jih razvrščamo med pomembnejše, med katere uvrščamo aplikacije tipa spletne pošte, oddaljenih dostopov (*telnet*, *ssh*), šifriranega spletnega prenosa (*https*) in raznih kontrolnih protokolov.

Do lanskega leta je v zadnji razred padel ves preostali promet, vendar smo lani zaradi povečanega prometa neposredne izmenjave datotek (”peer-to-peer”) ta razred razdelili. Tako imamo po novem razred ”best effort”, kamor spada običajen spletni promet in nekateri prenosi podatkov (npr. *ftp*), dodaten razred pa je namenjen prometu ”peer-to-peer” in raznim odjemalcem za neposredno izmenjavo datotek, ki uporabljajo protokol *BitTorrent*. Na tak način lahko poskrbimo, da imamo količinsko najagresivnejši promet pod kontrolo in predvsem da ne povzroča degradacije ostalega prometa. Promet delimo v naslednje razrede:

- PIP – razred ”Premium IP” z najvišjo prioriteto za potrebe videokonferenc ter VoIP-prometa;
- MC – razred ”Mission Critical”, namenjen protokolom: DNS, TELNET, RDP, SSH, MAIL, IMAP, IMAPS, POP3S, LDAP, LDAPS in RADIUS;
- MC-HTTPS – poseben razred za promet HTTPS;
- BE – ”Best Effort” – običajni internetni promet;

- LBE – ”Less than Best Effort” – promet ”peer-to-peer” prenosov.

Dodatno je bilo v lanskem letu z mehanizmi QoS nadgrajeno tudi omrežje v hrbtenici. Čeprav so hitrosti in kapacitete povezav v hrbtenici večinoma krepko nad povprečnim prometom, je vseeno življenje za sistemske inženirje mirnejše ob zavesti, da bi tudi v primeru izrednega in nenavadnega povečanja prometa, raznih anomalij ali morda celo prekomernega prometa kot posledice DoS-napadov omrežje še vedno bilo sposobno zagotavljati ustrezen nivo kakovosti storitve.



SLIKA 18: SHEMA OBMOČIJ KAKOVOSTI (DIFFSERV) V OMREŽJU ARNES

V omrežju ARNES uporabljamo za zagotavljanje kakovosti storitev model DiffServ. Slednji omogoča nivojsko obravnavo različnega tipa prometa in s tem zagotavljanje primerne obdelave prometa znotraj QoS-omrežja. Paketi določenega tipa storitve pripadajo ustrezni "klasi", posamezna "klasa" pa dobi določeno obravnavo na vsaki napravi (PHB – per hop behaviour). Ta model je enostaven, saj zagotavlja ustrezno obravnavo paketov brez potrebe poznavanja stanja prometnih tokov v omrežju na vsakem mrežnem elementu in brez dodatne signalizacije med napravami.

Prednosti tega modela so:

- razširljivost in neodvisnost (ni potrebe po informaciji o stanju prometnih tokov);
- zmogljivost (za potrebe klasifikacije je paket pregledan samo enkrat, in sicer na meji QoS-omrežja);
- združljivost (tehnologijo podpirajo vsi proizvajalci);
- prilagodljivost (vsaka naprava lahko uporablja različne načine določene funkcionalnosti glede na to, kaj naprava podpira).

Med slabosti lahko uvrstimo, da zaradi ne-End-to-End modela rezervacije pasovne širine lahko pride do napak, če katera izmed vmesnih naprav ni pravilno nastavljena. Prav tako ni mehanizma CAC (*Call Admission Control*), ki bi zagotavljal, da npr. visokoprioritetne aplikacije ne bi odžirale pasovne širine ena drugi. Le-to je treba zagotoviti z dodatnimi mehanizmi.

Celotno funkcionalnost zagotavljanja kakovosti storitev zagotovimo z:

- razvrščanjem in označevanjem paketov (classification and marking),
- mehanizmi omejevanja in glajenja prometa (policing and shaping),
- selektivnim odmetavanjem paketov (congestion avoidance),
- mehanizmi obravnavanja vrst (congestion management – queuing).

V omrežju ARNES se trudimo uporabnikom zagotoviti najboljše, kar tehnologija trenutno omogoča, zato sledimo razvojnim smernicam in omrežje nenehno prilagajamo potrebam in zahtevam uporabnikov.

Enostavno in varno na IPv6

The easy and safe way to IPv6

Matjaž Straus Istenič

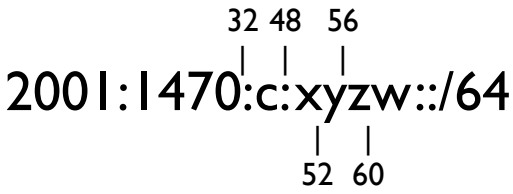
IPv6 je bil zasnovan z mislijo na skrbnika lokalnega omrežja. Delitev IPv6-omrežja je enostavnejša in preglednejša. Samodejna nastavitev omrežnih naprav je s primernimi orodji lahko dobro varovana in nadzorovana. Zavedati se moramo, da imajo nove in spremenjene lastnosti IP-protokola, ki sicer olajšajo delo skrbniku, velik vpliv na varnost v lokalnem omrežju. V praksi bomo morali znati združiti prednosti IPv6 z novimi varnostnimi izzivi in posodobiti svoja omrežja za sodobno in varno komunikacijo. IPv6 nam ponuja novo priložnost, da odpravimo pomanjkljivosti, ki so se prikradle v naša omrežja in storitve med dolgotrajnim krpanjem starega
IP-protokola.

IPv6 was designed with local systems administrators in mind. IPv6 subnetting is simple, transparent and straightforward. Autoconfiguration features that simplify the setup of IPv6 hosts can be properly secured and controlled with appropriate tools. As ever, new features and modified properties create new challenges, of which first hop security is one of the most important. Our goal is to use all the benefits of the new IP protocol, confront and solve the new security issues, and successfully upgrade our networks to provide modern, secure communications. IPv6 offers a new opportunity to correct deficiencies that have crept into our networks and services while mending the old IP protocol.

Enostavna delitev omrežja

Organizacija – članica omrežja ARNES pridobi del naslovnega prostora iz Arnesovega bloka `2001:1470::/32` v obsegu /48, npr. `2001:1470:c::/48`.[11] Tako velik segment naslovov zadošča za naslavljanje sistemov v več kot 65.000 lokalnih omrežjih, kar nam omogoča, da ga pregledno razdelimo po lokalnih omrežjih glede na njihovo namembnost. Sisteme v IPv4-omrežjih smo *številčili*, običajno v naraščajočem vrstnem redu, od IPv4-naslova prehoda, za katerega se zelo pogosto izbere prvi mogoči IPv4-naslov v omrežju, naprej. Z IPv6 je drugače – sisteme v IPv6-omrežjih pa *označujemo* s 64-bitnimi oznakami. Naslovni prostor organizacije delimo hierarhično na enako velike dele in se pri tem ne oziramo na varčevanje z naslovi. V taki delitvi se držimo pravila, po katerem naslovni prostor razmejimo tako, da je dolžina manjših delov vselej mnogokratnik štirih ali osmih bitov. Spodnja slika prikazuje, na katerih mestih se lahko odločimo za delitev naslovnega prostora /48 na lokalna omrežja /64.

[11] Večjim organizacijam, npr. univerzi, Arnes dodeli obseznejši blok IPv6-naslovov, tako da vsaka manjša enota, npr. fakulteta, dobi svoj /48.

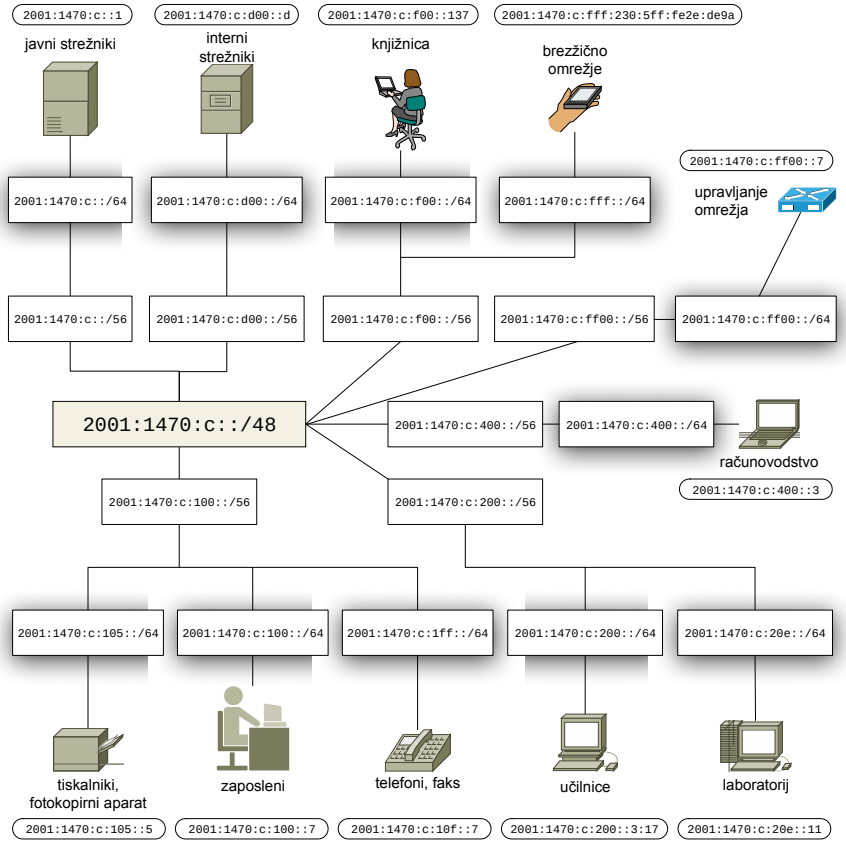


SLIKA 19: SHEMA IPV6-NASLOVA LOKALNEGA OMREŽJA. BLOK /48 RAZDELIMO HIERARHIČNO NA MANJŠE DELE, BODISI /52, /56 BODISI /60.

Zelo pregledna, praktična in razširljiva je delitev v treh nivojih. V prvem nivoju se odločimo za uporabo ene šestnajstine naslovnega prostora, drugo šestnajstino uporabimo za upravljanje omrežnih naprav, ostale pa prihranimo za morebitne oddaljene organizacijske enote, mobilne sisteme in druge razširitve v prihodnosti. Prostor nato razdelimo po skupinah uporabnikov, ki imajo skupno varnostno politiko. Štirje biti, ki jih uporabimo v tej delitvi, zadoščajo za delitev v 16 skupin. IPv6-naslov zapišemo takole:

`2001:1470:c:`*LSNN*`:`<64-bitna oznaka sistema>,

pri čemer za omrežja v organizaciji opustimo oznako *L* (*L* = 0), za omrežno infrastrukturo nastavimo *L* = f, ostalih oznak pa ne uporabimo. *S* je oznaka skupine in *NN* oznaka lokalnega omrežja. Primer take delitve prikazujeSlika 20.



SLIKA 20: PRIMER DELITVE IPV6-NASLOVNEGA PROSTORA: OMREŽJE ORGANIZACIJE `2001:1470:C::/48` JE RAZDELJENO NA 6 PODOMREŽIJ /56 ZA UPORABNIKE IN STREŽNIKE TER ENEGA ZA UPRAVLJANJE OMREŽNIH NAPRAV. IZ TEH DELOV JE IZBRAN NASLOVNI PROSTOR ZA POSAMEZNA LOKALNA OMREŽJA /64 (NA SLIKI SO NARISANA OSENČENO) IN KONČNE SISTEME.

Samodejna nastavitev omrežnih naprav

Z novo zasnovo delovanja v lokalnem omrežju prinaša IPv6 nekaj prednosti, ki poenostavljajo priklop in nastavitve omrežnih naprav:

- namesto posebnega protokola ARP (Address Resolution Protocol) so v IPv6 vgrajeni mehanizmi ND (Neighbour Discovery), ki slonijo na ICMP;
- IPv6 z mehanizmom SLAAC (Stateless Address Autoconfiguration) napravam omogoča samodejno določitev IP-naslova;
- iskanje usmerjevalnika in nastavitev privzetega prehoda poteka samodejno s poizvedbami po usmerjevalnikih RS (Router Solicitation) in oglaševanji usmerjevalnikov RA (Router Advertisements);
- z ND je predvidena tudi samodejna nastavitev DNS-strežnikov in domene;[12]
- protokol za samodejne nastavitve omrežnih naprav DHCP je temeljito predelan in posodobljen za IPv6.

Največjo poenostavitev za uporabnika prinaša mehanizem SLAAC z elementi ND, ki se pri tem uporabljajo (Hagen, 2006). Omrežna naprava si po priklopu v omrežje sama nastavi IPv6-naslove in privzeti prehod (nekoliko poenostavljen opis tega postopka je v okvirju 1), kar je očitna prednost pred IPv4, ob kateri pa se hitro sprožijo pomisleki glede varnosti. Kakšen IPv6-naslov ima določena naprava ob določenem času? Ali lahko sledimo spremembam tega naslova? SLAAC omogoča tudi delno anonimnost z izbiranjem naključnega IPv6-naslova (*Privacy Extension Address*). Le-to je dvorezen meč (Vyncke: IPv6 Security) – po eni strani ščiti anonimnost uporabnika, po drugi pa skrbniku otežuje sledljivost IPv6-naslovov in njihovih uporabnikov.

Z mehanizmi SLAAC ni mogoče nastaviti vseh parametrov omrežne naprave. Manjka celo nastavitev IP-naslovov rekurzivnih strežnikov DNS, ki je sicer že definirana kot standardna razširitev sporočil usmerjevalnikov (RA), vendar je v praksi zelo redko realizirana. To in pa želja po večjem nadzoru dodeljevanja IPv6-naslovov je pogost vzrok, da se v lokalnem omrežju omogoči DHCPv6. Poudarimo, da samodejna nastavitev z DHCPv6 ne deluje brez SLAAC, saj se omrežna naprava odloči za uporabo DHCP šele na podlagi sporočil usmerjevalnika (RA). Poleg tega DHCPv6 ne posreduje privzetega prehoda in velikosti omrežja.

[12] RFC 6106 (IPv6 Router Advertisement Options for DNS Configuration), nov. 2010.

1. Naprava določi svojo 64-bitno identifikacijsko oznako (ID) bodisi tako, da jo zgradi iz svojega omrežnega naslova (MAC), bodisi jo ustvari naključno. Za primer vzemimo ID `a:b:c:d`.
2. Naprava določi svoj lokalen (*link-local*) IPv6-naslov, tako da ID dopolni s predpono `fe80::/10`, npr. `fe80::a:b:c:d`. Zaradi enostavnosti bomo namenoma zamolčali preverjanje enoličnosti IPv6-naslovov (*Duplicate Address Detection*).
3. Naprava pošlje poizvedbo RS po usmerjevalnikih (*Router Solicitation*) na lokalen skupinski naslov "vsi usmerjevalniki" `ff02::2` (*all-routers link-local multicast address*). Če na poizvedbo ne dobi odgovora, se SLAAC zaključi in naprava ima zgolj lokalen naslov.
4. Naprava dobi odgovore RA-usmerjevalnikov v lokalnem omrežju (*Router Advertisements*). Za privzeti prehod nastavi lokalen naslov enega od njih.
5. Naprava zbere vse veljavne IPv6-predpone, ki so jih v svojih RA-sporočilih posredovali usmerjevalniki, in si za vsako od teh nastavi globalen IPv6-naslov, tako da predpono dopolni s svojim ID. Primer: s predpono `2001:1470:c:100::/64` se naprava naslovi z `2001:1470:c:100:a:b:c:d`.
6. Naprava preveri vsak RA, ali ima morda nastavljeni oznaki M (*managed address configuration flag*) ali O (*other configuration flag*).
    a. Če sta oznaki M in O obe enaki 0, se SLAAC zaključi brez uporabe DHCP.
    b. Če sta oznaki M in O obe enaki 1, je v lokalnem omrežju DHCPv6-strežnik ali posrednik za DHCPv6. Naprava pošlje DHCP-poizvedbo na skupinski naslov "vsi DHCP-posredniki" `ff02::1:2` (*all-DHCP-agents_and_servers link-local multicast address*). Če dobi odgovor, si nastavi dodatne IPv6-naslove in parametre, npr. naslov DNS-strežnika in zaključi s samodejnimi nastavitvami.
    c. Če je M = 1 in O = 0, je postopek podoben primeru M = O = 1, le da se DHCPv6 uporabi zgolj za nastavitev IP6-naslova in ne za druge nastavitve. Ta možnost je malo verjetna, saj je prednost DHCP prav v nastavitvah drugih omrežnih parametrov, kot npr. IPv6-naslova DNS-strežnika.
    d. Če je M = 0 in O = 1, potem je v lokalnem omrežju t. i. "stateless" DHCPv6-strežnik ali posrednik, ki skrbi le za dodatne omrežne parametre, npr. IPv6-naslov DNS-strežnika, in ne streže z IPv6-naslovi. Naprava pošlje DHCP-poizvedbo in če dobi odgovor, nastavi ustrezne parametre. Samodejne nastavitve so zaključene.

OKVIR 1: POTEK SAMODEJNE NASTAVITVE OMREŽNIH PARAMETROV IPV6-NAPRAVE

Zdi se, da smo ob vse prednosti samodejnih nastavitev, ki jih prinaša IPv6. Namesto DHCP, kot smo ga vajeni v IPv4-omrežjih, bomo morali skrbeti za dodaten
DHCP-strežnik za IPv6 ter za pravilno in kontrolirano delovanje samodejnih mehanizmov, kot je SLAAC. Brez skrbi – rešitev je v postopnosti uvajanja IPv6 skladno s tehničnim napredkom orodij za pomoč skrbnikom lokalnih IPv6-omrežij. V začetnih korakih se bomo odločili za:

- statične nastavitve omrežnih parametrov na strežnikih;
- statične nastavitve omrežnih parametrov na stacionarnih računalnikih;
- na vseh sistemih (Windows 7 in Vista, Mac OS X Lion) izklopimo naključno izbiranje IPv6-naslovov;
- na sistemih Windows izklopimo vmesnike tunelov (glej okvir 2).

```
netsh interface ipv6 set privacy state=disable
netsh interface ipv6 set global randomizeidentifiers=disabled
netsh interface ipv6 6to4 set state disabled default
netsh interface ipv6 isatap set state disabled
netsh interface ipv6 set teredo disabled
```

OKVIR 2: IZKLOP GENERIRANJA NAKLJUČNIH IPV6-NASLOVOV IN TUNELOV NA SISTEMU WINDOWS

S kontroliranimi ročnimi nastavitvami računalnikov v omrežje nismo vnesli dodatnega tveganja, vendar smo posodobitev na IPv6 morali omejiti zgolj na sisteme, ki so v našem upravljanju.

V naslednjem koraku bomo v omrežju omogočili samodejne nastavitve z mehanizmom SLAAC brez DHCPv6. Pred tem moramo poskrbeti za nadzor uporabe IPv6-naslovov na sistemih, ki jih upravljajo uporabniki sami, kot so prenosni računalniki, naprave v brezžičnem omrežju ipd. V času priprave tega prispevka je tak nadzor mogoč le na redki in dragi omrežni opremi, na voljo pa je tudi odprtokodni programski paket NDPMon (5), s katerim lahko učinkovito nadziramo samodejne nastavitve IPv6-naprav v lokalnem omrežju.[13]

Posodobitev na IPv6 zaključimo s postopno vpeljavo DHCPv6. V predhodnih korakih smo pridobili vse potrebne podatke za nastavitve DHCP-strežnika, predvsem ethernet naslove (MAC) vseh omrežnih naprav.

Varnost v lokalnem omrežju

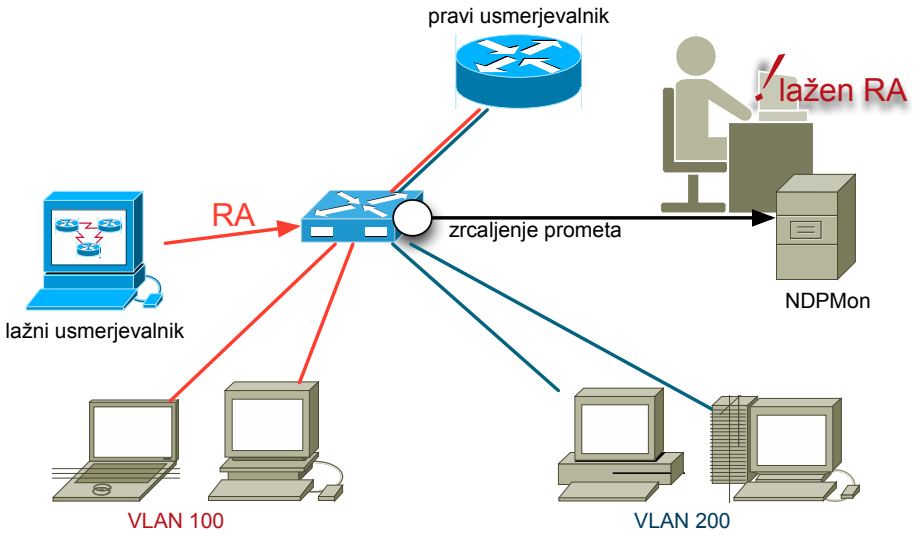
V IPv6 je vgrajenih veliko mehanizmov, ki omogočajo uporabo IPv6 v lokalnih omrežjih *ethernet*. Najpomembnejši so del protokola ND (*Neighbour Discovery Protocol*). Ti mehanizmi so preprosti in kot taki lahka tarča zlonamernih aktivnosti. SLAAC nima preverjanja identitete in overjanja ND-sporočil. Mogoče zlorabe se kar vrstijo (BRKSEC 3003):

[13] Delovanje NDPMon bomo prikazali na predavanju na Arnesovi konferenci v sklopu SIRikt 2012.

- lažni usmerjevalnik (do tega ”napada” pogosto pride nevede in ne zlonamerno, npr. sistem Windows z vključenim ”*Internet Connection Sharing*” se v omrežju lahko predstavi kot usmerjevalnik);
- lažna omrežna predpona med samodejno nastavitvijo naslova SLAAC;
- kraja IPv6-naslova med iskanjem sosedov (NS) in preverjanjem enoličnosti naslova (DAD) – sistem se ”zlaže”, da ima nek naslov;
- preusmerjanje prometa na napadalca (*Redirect*) – prisluškovanje;
- poplavljanje tabele sosedov (*Neighbour Cache Flooding*).

Proizvajalci omrežne opreme obljubljajo varovanje pred temi napadi, predvsem s posebno programsko opremo na (dragih!) stikalih, ki bo zagotavljala varnost IPv6-naprav na centraliziran način. Na seznamu lastnosti takega ”pametnega” stikala najdemo (v oklepaju navajam težko prevedljive angleške izraze):

- varovanje oglaševanja usmerjevalnika (RA-guard);
- nadzor NDP (NDP address glean/ inspection);
- skrb nad lastništvom naslovov (Address watch/ownership enforcement);
- spremljanje aktivnih naprav (Device Tracking);
- nadzor nad naslovi DHCP (Address Glean);
- varovanje DHCP (DHCP-guard);
- posrednik preverjanja enoličnosti naslova in iskanja sosedov (DAD/Resolution proxy);
- overjanje izvornega naslova (IP-Source-guard, SAVI);
- overjanje ciljnega naslova (IP-Destination-guard);
- posrednik DCHP (DHCP L2 relay).



SLIKA 21: NDPMON NADZIRA SPOROČILA V LOKALNEM OMREŽJU, ZAZNA IN SPOROČA NEPRAVILNOSTI.

Dokler te funkcije ne bodo podprte v cenovno dostopni komunikacijski opremi, se bomo morali zadovoljiti z nadzorom, kakršnega omogoča že prej omenjeni NDPMon (5). To orodje nadzira kontrolni promet v lokalnem omrežju (Slika 21) in zaznava ter sporoča naslednje nepravilnosti:

- napačen par naslovov ethernet MAC in IPv6;

- napačen ethernet MAC-naslov usmerjevalnika;
- napačen IPv6-naslov usmerjevalnika;
- napačno omrežno predpono;
- napačno preusmerjanje (*Redirect*);
- sporočilo lažnega usmerjevalnika;
- napad na mehanizem iskanja dvojnikov (*Duplicate Address Detection DoS*);
- menjave ethernet MAC-naslovov.

Poudariti moramo, da NDPMon zgolj nadzira omrežje in sporoča odkrite nepravilnosti, ne more pa jih preprečiti, kot to lahko storijo posebna stikala. Res je – varnostni izzivi v IPv6 so izjemno obsežni (Vyncke, BRKSEC 2003) (6), vendar ne smemo dovoliti, da postanejo ovira za uspešen prehod na novi IP-protokol. Začnimo postopoma, pridobivajmo znanje z uporabo dostopnih odprtokodnih rešitev in stopimo v korak z razvojem komercialne omrežne opreme. Na ta način bomo pravočasno pripravljeni za IPv6.

Viri

- Knjiga: Hagen, S. (2006): IPv6 Essentials, O'Reilly Media, Sebastopol, CA.
- Knjiga: Hogg S., Vyncke, E. (2009): IPv6 Security, Cisco Press, Indianapolis, USA.
- Predavanje: Vyncke, E., Cisco (2008): BRKSEC 2003, IPv6 Security Threats and Mitigations, Cisco Networkers, Barcelona, Španija (2009).
- Predavanje: Cisco (2010): BRKSEC 3003, Advanced IPv6 Security: Securing Link- Operations at First Hop, Cisco Live, London, UK (2011).
- Spletna stran: NDPMon http://ndpmon.sourceforge.net/ https://github.com/ayourtch/ndpmon-dot1q (31. 1. 2012).
- Spletna stran: The Hackers Choice http://freeworld.thc.org/thc-ipv6/ (31. 1. 2012).
- Spletna stran: Svetovna ”izstrelitev” IPv6 http://www.worldipv6launch.org/ (26. 1. 2012).

Sodobno upravljanje in nadzor omrežja

Network management and monitoring

Matej Vadnjal

Sodobno omrežje mora delovati zanesljivo. Zato moramo imeti dober pregled nad infrastrukturo in dogajanjem v omrežju, za kar potrebujemo kakovostna nadzorna orodja. V tem poglavju si bomo ogledali nekaj takih orodij, ki temeljijo na odprti kodi in s katerimi imamo izkušnje na Arnesu.

A modern network must also be reliable. We therefore need a good overview of what is happening in our network. To do so, we need quality monitoring tools. In this section we will examine some of those tools that are all *open source* and used by ARNES.Preverjanje delovanja omrežnih virov

Za vsako storitev in napravo v sodobnem omrežju moramo vedeti, ali deluje in ali deluje pravilno. Zato je treba delovanje teh virov redno preverjati. Icinga (1) je nadzorni sistem, ki ta preverjanja izvaja samodejno in operaterja obvešča o napakah.

Preverjanje je zasnovano modularno, tako da lahko nadzorujemo delovanje poljubne omrežne storitve ali naprave. Icinga že privzeto vsebuje precej modulov (v jeziku Icinge modulu rečemo *plugin*) za preverjanje najpogosteje uporabljanih omrežnih storitev, še veliko več pa jih lahko najdemo v spletni shrambi Monitoring Exchange (2). Če tam modula za svoje potrebe ne najdemo, ga lahko napišemo tudi sami.

Podobna modularna zasnova se uporablja tudi za obveščanje o napakah. Najpogosteje se uporabljajo moduli za pošiljanje elektronske pošte in SMS-sporočil , najdemo pa lahko tudi vrsto drugih bolj ali manj uporabnih vtičnikov.

Icinga administratorju omogoča nastavitev kupa parametrov, med pomembnejšimi pa so interval preverjanja, število neuspešnih rezultatov preverjanja za sprožitev alarma ter pogostost in časovna obdobja, v katerih se pošiljajo obvestila o alarmih.

Najpogostejša uporaba Icinge je preverjanje dosegljivosti omrežnih naprav. Na Arnesu za to uporabljamo modul *check_icmp*, ki na IP-naslov omrežne naprave pošlje ICMP-paket *echo-request* in čaka na ICMP-odgovor *echo-reply* – t. i. *ping*. Če naprava dve zaporedni minuti ni dosegljiva, se sproži alarm. Reakcija Icinge na alarm je odvisna od kategorije pomembnosti naprave. Ta kategorija vpliva na to, kako bo dežurni operater obveščen o alarmu. Za alarm na zelo pomembni napravi Icinga pošlje SMS na mobilni telefon dežurnega kadarkoli – podnevi ali ponoči. Pri srednje pomembnih napravah se pošlje SMS le podnevi, v nočnem času pa se pošlje elektronsko sporočilo, na katerega se dežurni odzove zjutraj. Za alarme na manj pomembnih napravah pa se vedno pošlje le elektronsko sporočilo.

Icinga v dnevniške zapise beleži vse spremembe stanj preverjanih storitev ali naprav. Iz teh zapisov lahko nato tudi pridobi podatke o razpoložljivosti storitve ali naprave in jih predstavi v poročilu (slika 14).

Host State Breakdowns:

State	Type / Reason	Time	% Total Time	% Known Time
UP	Unscheduled	6d 21h 16m 43s	92.612%	92.612%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	6d 21h 16m 43s	92.612%	92.612%
DOWN	Unscheduled	0d 13h 11m 6s	7.388%	7.388%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	0d 13h 11m 6s	7.388%	7.388%
UNREACHABLE	Unscheduled	0d 0h 0m 0s	0.000%	0.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	0d 0h 0m 0s	0.000%	0.000%
Undetermined	1.5.1 Not Running	0d 0h 0m 0s	0.000%	
	Insufficient Data	0d 0h 0m 0s	0.000%	
	Total	0d 0h 0m 0s	0.000%	
All	Total	7d 10h 27m 49s	100.000%	100.000%

SLIKA 22: POROČILO O RAZPOLOŽLJIVOSTI NAPRAVE

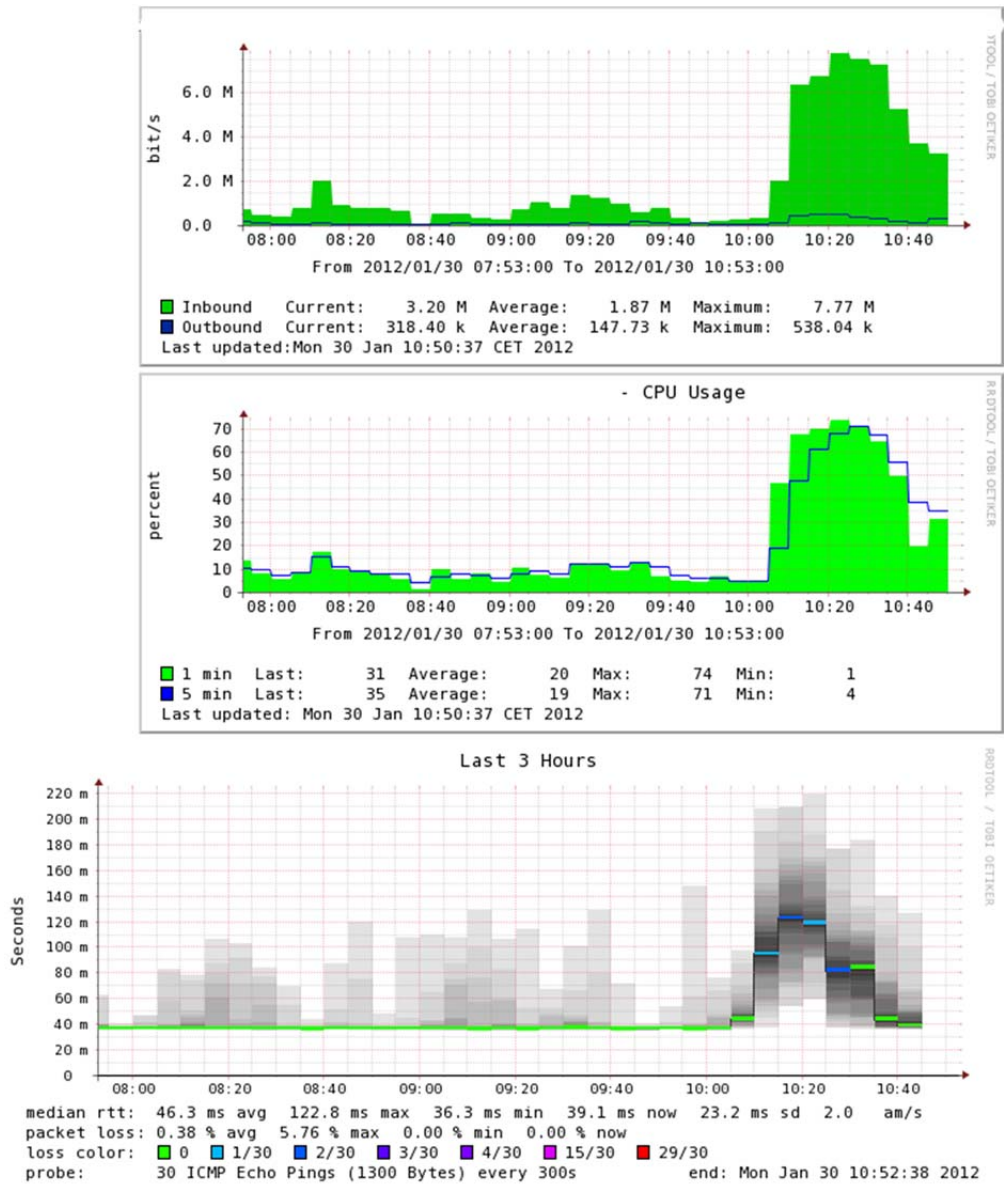
Obremenitev omrežnih virov

Za zagotavljanje kakovostnih storitev ni dovolj le, da vemo, ali storitev deluje ali ne, temveč moramo vedeti tudi, koliko je uporabljana. Lep primer je zasedenost povezave iz omrežja v internet. Če to količino narišemo na grafu, lahko hitro razberemo povprečno obremenitev povezave skozi čas in tako predvidimo, kdaj bo potrebna nadgradnja povezave.

Na Arnesu za zbiranje in prikaz takih podatkov uporabljamo Cacti (3). Cacti je primarno orodje za risanje grafov različnih omrežnih parametrov, kot bomo videli kasneje, pa zna še veliko več. S spletnim vmesnikom določimo, kateri omrežni parameter bi radi spremljali, in Cacti začne v ozadju pobirati podatke iz omrežne naprave ter jih shranjuje v datoteke RRD (4). Na grafu lahko nato spremljamo, kako se vrednost tega parametra spreminja skozi čas.

Najpogosteje uporabljamo Cacti, ko bi radi videli, koliko prometa se pretaka skozi omrežne vmesnike naših stikal in usmerjevalnikov. Seveda pa Cacti podpira risanje tudi vrste drugih parametrov, na primer obremenitev procesorja (CPU), zasedenost diska, avtonomijo brezprekinitvenega napajanja in še veliko drugih (slika 15). Cacti pridobiva te vrednosti iz omrežnih naprav prek protokola SNMP (5), lahko pa tudi napišemo lastno funkcijo, ki bo prišla do rezultata na poljuben način in ga vrnila Cactiju.

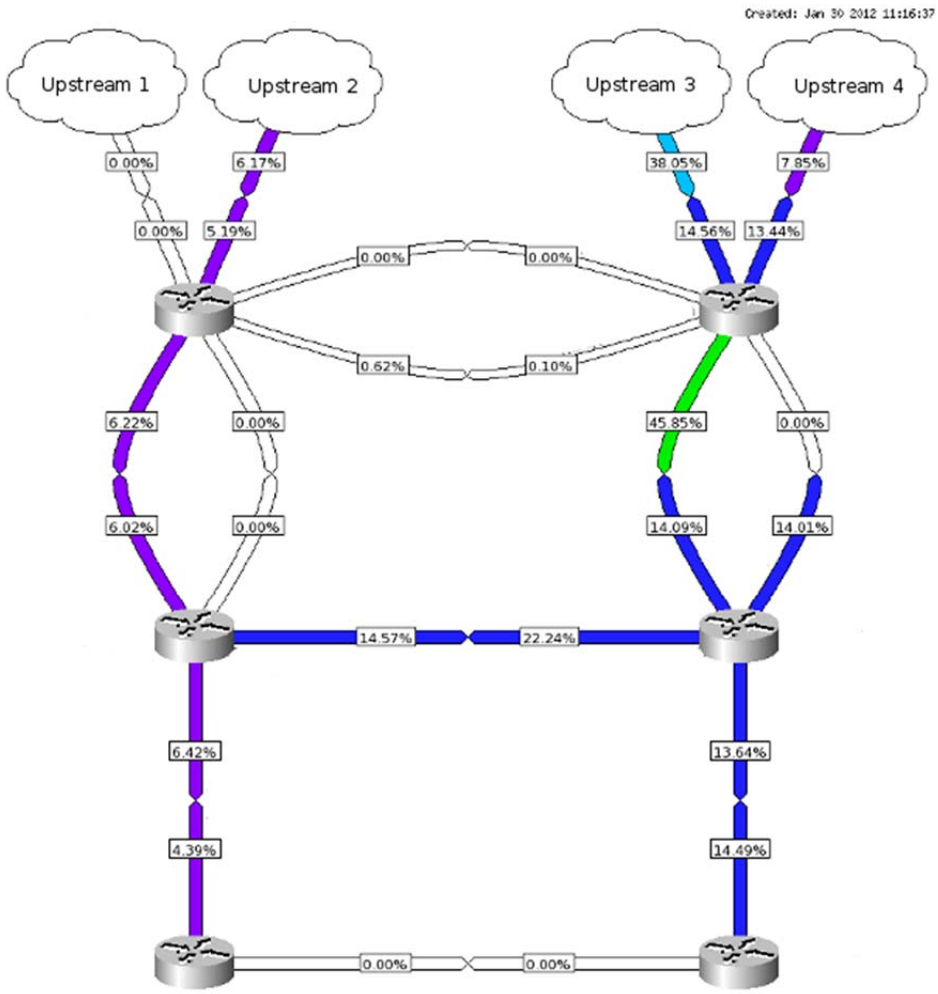
Z vgrajenim spletnim vmesnikom lahko pregledujemo grafe. Omogoča nam, da izbor prikazanih grafov omejimo z iskalnimi parametri in da izberemo časovno obdobje, ki naj bo prikazano. Tako lahko hitro primerjamo odčitke različnih grafov v časovnem intervalu, ki nas zanima, kar je zelo uporabno, kadar poskušamo odkriti vzrok slabšega delovanja v delu omrežja.



Slika 15: Primerjava različnih veličin v istem časovnem obdobju. Na prvem grafu je promet n vmesniku usmerjevalnika, na drugem obremenitev procesorja, na tretjem pa zakasnitev in izgube na povezavi do usmerjevalnika. Jasno je razvidno, da ima večja količina prometa negativen vpliv na obremenitev procesorja usmerjevalnika, zaradi česar se začnejo pojavljati tudi izgube paketov.

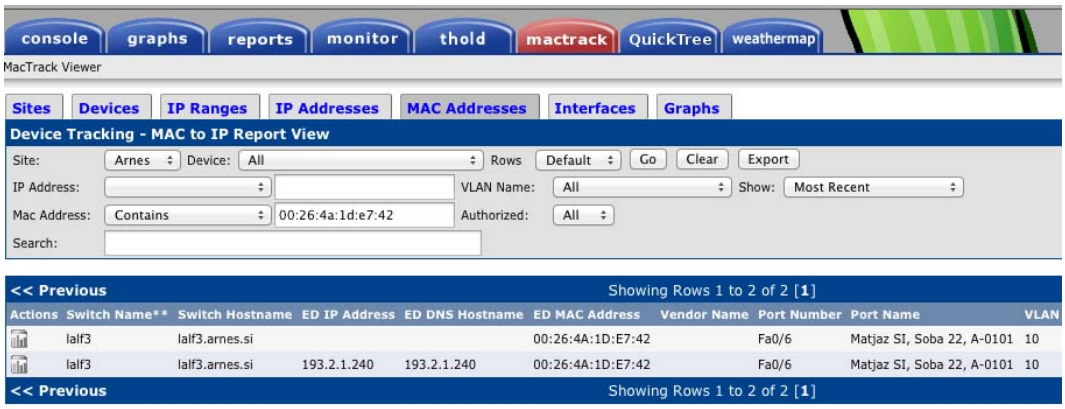
Cacti podpira tudi dodatne module, ki razširijo njegovo funkcionalnost. Nekaj popularnejših, ki jih uporabljamo tudi na Arnesu:

- Network Weathermap – vrednosti parametrov, ki jih Cacti zbira, prikaže na shemi omrežja. S tem orodjem na sliki določimo usmerjevalnike in povezave med njimi. Cacti nato vsako povezavo med usmerjevalniki obarva v barvi, ki ustreza zasedenosti povezave. Tako lahko hitro opazimo, če je katera povezava v omrežju preobremenjena (slika 16).



Slika 23: Trenutna zasedenost povezav v delu omrežja ARNES

- **ReportIt** – dodatek, ki generira tabele s poročili iz podatkov, zbranih v Cactiju. Tipičen primer uporabe je poročilo o prenesenem prometu v omrežje in iz njega v danem obdobju. ReportIt lahko nastavimo tudi tako, da nam sam periodično pripravi poročilo za pretekli mesec in ga pošlje po elektronski pošti.
- **Mactrack** – orodje, ki pobira podatke o vmesnikih, ethernet MAC in IP-naslovih ter DNS-zapisih iz omrežja in jih poveže v skupne zapise. Tako lahko z iskanjem po DNS-imenu naprave najdemo njen IP- in MAC-naslov ter vmesnik stikala, na katerega je priključena (slika 17).



SLIKA 17: CACTI MACTRACK

V tem delu smo na kratko predstavili dve orodji, ki upravljavcu omrežja lajšata zagotavljanje kakovostnih storitev. Seveda je na voljo tudi precej alternativnih rešitev, tako komercialnih kot tudi brezplačnih. Opisani orodji po Arnesovem mnenju ponujata najboljše razmerje med enostavnostjo uporabe in fleksibilnostjo.

Spletni viri

1. http://www.icinga.org/
2. https://www.monitoringexchange.org/
3. http://www.cacti.net/
4. http://www.rrdtool.org/
5. https://en.wikipedia.org/wiki/SNMP

Zaključek

Prispevek smo začeli s skrbjo za urejenost omrežne infrastrukture in dokumentacije, nadaljevali s kratkim opisom sodobne prenosne tehnologije s tehnologijo WDM in se nato posvetili zagotavljanju kakovosti komunikacije z mehanizmi QoS. Kakovostna komunikacija je tudi sodobna in varna, zato smo v nadaljevanju opisali nekaj osnovnih lastnosti novega protokola IPv6 s poudarkom na varovanju lokalnega omrežja. V vseh opisanih plasteh, od električnega napajanja preko optičnega vlakna do internetnega protokola, je potreben zanesljiv nadzor. Zato zaključujemo z opisom nekaj odprtokodnih upravljavskih in nadzornih orodij.

V omrežju ARNES uspešno združujemo opisano tehnologijo v enovito storitev z imenom ”kakovostna komunikacija”.

Ljubljana, marec 2012

KONFERENCA ARNES 2012
20 LET INTERNETA LJUDI
ZBORNIK ČLANKOV
UREDIL: Domen Božeglav
LEKTORIRALA: Tjaša Žorž
PREVOD: Amidas

Arnes
p.p. 7, 1001 Ljubljana
T: 01 479 88 77
F: 01 479 88 78
E. arnes@arnes.si
www.arnes.si