



Konferenca Arnes 2011

KAJ NAM PRINAŠA RAČUNALNIŠTVO V OBLAKU?

Zbornik člankov

13. april 2011

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

KAZALO

Računalništvo v oblaku na Berkeleyu	6
Računalništvo v oblaku na Arnesu	7
Ali je kaj trden vaš oblak?	9
Varni na internetu	11
Zasebnost v oblaku	15
Slovensko omrežje grid: dostop do visokih računskih zmogljivosti v Sloveniji	20
Upravljanje z identitetami na Norveškem	24
Okrogla miza: Federativne storitve v slovenskem izobraževalnem prostoru	25
Spletni dnevnik in izmenjava datotek prek spleta	26
Nadgradnja gostovanja virtualnih strežnikov in dinamičnih spletnih strani	31
Novosti s področja večpredstavnosti na Arnesu	35
Okolje za konstruktivistično sodelovalno učenje z rabo infrastrukture v oblaku	37
Shranjevanje podatkov in označevanje "spama"	46
1, 2, 3, 4 – na IPv6	48
IPv6 – kaj pa storitve?	55

KONFERENCA ARNES 2011 KAJ NAM PRINAŠA RAČUNALNIŠTVO V OBLAKU?

Konferenca Arnes povezuje uporabnike s področja izobraževanja, raziskovanja in kulture. Naš cilj je zagotoviti aktualne in relevantne informacije s področja novih informacijsko-komunikacijskih tehnologij, omrežnih storitev in infrastrukture. Konferenca je namenjena širokemu krogu obiskovalcev, saj pokriva tako uporabniške kot tudi sistemske vidike uporabe novih tehnologij.

Glavna tema letošnje konference, ki v okviru konference SirIKT poteka že peto leto zapored, bo računalništvo v oblaku. Tuji in domači predavatelji bodo poskušali odgovoriti na vprašanja, kaj računalništvo v oblaku pravzaprav je in kako lahko koristi tudi vam, pa naj gre za znižanje stroškov ali pohitritev računskih operacij ter ali bi vaše raziskave morda lažje podprli z uporabo gridov. Računalništvo v oblaku pa poleg prednosti prinaša tudi določene pasti, povezane z izvozom podatkov v oblak tako na tehničnem nivoju kot tudi na zasebnosti v informacijski družbi. In kako se računalništva v oblaku lotevamo na Arnesu? Tudi mi za svoje uporabnike že pripravljamo »oblačno infrastrukturo«, seveda s poudarkom na varnosti podatkov. Trend vedno večje razpršenosti storitev in vse večjega števila uporabnikov nam prinaša dodatne izzive pri pomnjenju gesel in administraciji uporabnikov samih. Zato bomo plenarna predavanja povezali z okroglo mizo, na kateri bomo pogledali, ali lahko izzive razpršenosti presežemo ter katere izmed teh storitev naše organizacije (npr. univerze, šole in raziskovalni inštituti) dejansko uporabljajo.

Konferenco bomo zaključili z dvema vzporednima sklopoma predavanj, od katerih bo prvi sklop poljudne, drugi pa tehnične narave. V prvem sklopu bomo predstavili Arnesove nove storitve, kot so na primer spletni dnevnik in izmenjava datotek, ter opozorili na izboljšanje funkcionalnosti obstoječih storitev, kot so dinamično gostovanje spletnih strani in spletne konference VOX. Sklop bomo zaključili s predstavitvijo okolja za sodelovalno učenje. Drugi sklop predavanj bo namenjen predvsem tehnikom. Predstavili vam bomo novo možnost za označevanje »spama« na vaših lokalnih strežnikih ter shranjevanje večje količine podatkov, npr. za shranjevanje varnostnih kopij. Ker je v letu 2010 agenciji IANA dokončno zmanjkalo IPv4-naslovnega prostora, bomo sklop zaključili s praktičnimi nasveti, kako lahko administratorji prilagodite svoje omrežje in storitve na novi protokol IPv6.

Upamo, da vam bo vsebina tokratne konference privlačna in da boste konferenco izkoristili tudi za navezavo ali obuditev stikov tako z nami kot vašimi kolegi, saj nikakor ne smemo pozabiti, da življenje obstaja tudi zunaj interneta.

ARNES 2011 CONFERENCE

WHAT DOES CLOUD COMPUTING HOLD IN STORE?

The ARNES Conference brings together users in the education, research and culture sectors. Our aim is to provide up-to-date, relevant information on new information-communications technologies, network services, and infrastructure. The conference is aimed at a broad range of delegates, covering both user and systems aspects of the use of new technologies.

The main theme of this year's conference – held for the fifth successive year as part of the SirIKT conference – is cloud computing. Foreign and Slovenian speakers will attempt to answer the question of what cloud computing actually is and how it can help, either by cutting costs or speeding up computing operations, or making it easier to support your research by using grids. As well as its benefits, cloud computing also brings certain pitfalls linked to exporting data to the cloud, both on the technical level and in terms of privacy in the information society. How does ARNES deal with cloud computing? We are already preparing “cloud infrastructure” for our users, with the emphasis of course on data security. The trend of increasing dispersion of services and increasing user numbers bring additional challenges in terms of remembering passwords and user administration. We will therefore link plenary talks with a round table, which will examine whether the challenge of dispersion can be overcome, and which services our organisations (e.g. universities, schools and research institutes) actually use.

The conference will end with two parallel sets of talks, the first general and the second technical. The first set will present ARNES' new services, such as blogs and file exchanges, and will highlight the improved functionality of existing services, such as dynamic web hosting and VOX web conferences. This will conclude with a presentation of a collaborative learning environment. The second set of talks will mainly be aimed at technical staff. We will describe new options for tagging “spam” on your local servers and for storing more data such as backups. Since IANA finally exhausted the IPv4 address space in 2010, we will end this set of talks with some practical advice on how administrators can adapt their networks and services to the new IPv6 protocol.

We hope that you will find the content of this year's conference interesting, and that you will take the opportunity to establish or enhance contacts with us and with your colleagues. After all, we mustn't forget that there is life offline as well as on the Internet.

RAČUNALNIŠTVO V OBLAKU NA BERKELEYU

A BERKELEY VIEW OF CLOUD COMPUTING



ANTHONY D.
JOSEPH,
BERKELEY

POVZETEK

Računalništvo v oblaku – dolgoletne sanje o računalništvu kot storitvi – lahko povsem spremeni informacijsko tehnologijo in naredi programsko opremo kot storitev še privlačnejšo, hkrati pa oblikuje način razvoja in kupovanja računalniške strojne opreme. Za uresničitev inovativnih zamisli pri novih internetnih storitvah velika vlaganja v strojno opremo niso več potrebna, stroški z upravljanjem teh storitev pa so nižji. Podjetja so pri izvajanju obsežnih paketnih opravil omejena zgolj z razširljivostjo svojih programov, saj je strošek enourne uporabe 1000 strežnikov enak strošku uporabe enega strežnika za 1000 ur. Takšne elastičnosti sredstev na področju informacijske tehnologije še ni bilo. V tem predavanju bom razpravljal o najpomembnejših dejavnikih, ki omogočajo računalništvo v oblaku, in nekaterih ovirah za njegovo uvedbo.

KLJUČNE BESEDE: OBLAK, STORITEV

ABSTRACT

Cloud Computing, the long-held dream of computing as a utility, has the potential to transform the IT industry, making software even more attractive as a service and shaping the way IT hardware is designed and purchased. Developers with innovative ideas for new Internet services no longer require large capital outlays in hardware to deploy their service or the human expense to operate it. Companies with large batch-oriented tasks can get results as quickly as their programs can scale, since using 1000 servers for one hour costs no more than using one server for 1000 hours. This elasticity of resources, is unprecedented in the history of IT. In this talk, I will discuss key enablers for Cloud Computing and several barriers to adoption.

KEY WORDS: CLOUD, SERVICE

RAČUNALNIŠTVO V OBLAKU NA ARNESU CLOUD COMPUTING AT ARNES



JERNEJ PORENTA,
ARNES

POVZETEK

Vedno več Arnesovih storitev temelji na računalništvu v oblaku. Poleg virtualnih strežnikov, ki jih nudimo v okviru spletnega gostovanja, bo v letu 2011 zahtevnejšim uporabnikom na voljo tudi gostovanje strežnikov v oblaku, kar poznamo pod kratico IaaS - Infrastructure as a Service. Takšne rešitve uporabnikom omogočajo samostojni nadzor nad delovanjem posameznega strežnika, samostojno kreiranje novih instanc, neodvisno izbiro operacijskega sistema in večje diskovne kapacitete. Uporabniki bodo lahko te storitve uporabljali za enostavne premostitve začasno povečanih podatkovnih potreb, strežnike za podporo izobraževanju, itd. Rešitve za računalništvo v oblaku se običajno plačujejo po zakupljeni procesorski moči in količini prenesenih podatkov, prednost Arnesovih rešitev pa je tudi v tem, da so upravičenim uporabnikom na voljo brezplačno.

KLJUČNE BESEDE: RAČUNALNIŠTVO V OBLAKU,
STORITEV, VIRTUALIZACIJA

UVOD

Računalništvo v oblaku je zadnja moda IT sveta in temu se prilagaja tudi Arnes s svojimi storitvami. V letu 2011 nameravamo tako ponuditi našim uporabnikom storitev gostovanja strežnikov v oblaku, ki bo omogočila dodatne možnosti izobraževanja oziroma uporabe IKTja pri poučevanju oziroma raziskavah.

V letu 2011 bomo tako ponudili storitve, ki jih s tujko imenujemo Infrastructure as a Service – IaaS. Računalništvo v oblaku je namreč nadpomenka IaaS in je slog računalništva, pri katerem so dinamično razširljiva in pogosto virtualizirana računalniška sredstva na voljo kot storitev preko interneta (Vir 1). Uporabniki bodo tako imeli možnost gostovanja virtualnih strežnikov v Arnesovem oblaku in uporabljati strojne vire, ki se bodo fizično nahajali v Arnesovih sistemskih prostorih

IMPLEMENTACIJA

IaaS je v osnovi tehnologija, ki omogoča dostop do strojnih virov preko interneta. V preteklosti se je namreč pojavilo veliko zahtev po strojnih virih, ki bi gostovali na Arnesu, vendar ta možnost ni bila vedno izvedljiva. Z napredovanjem tehnologije in povečanje strojnih zmogljivosti posameznih strežnikov je tudi ta ovira umaknjena in v letu 2011 bodo tako uporabniki lahko uporabili storitev gostovanja strežnikov v Arnesovem oblaku. Storitve gostovanja v oblaku je zasnovana tako, da bodo lahko uporabniki pridobili vsaj en virtualni strežnik, ki bo pod popolno kontrolo samega uporabnika. Tako bodo lahko

ABSTRACT

More and more of ARNES' services are based on cloud computing. Apart from virtual servers – which we offer as part of web hosting – in 2011 more demanding users will also have access to server hosting in the cloud, known by the abbreviation IaaS – Infrastructure as a Service (a commercial example is Amazon Cloud). Such solutions allow independent monitoring of the operation of individual servers, independent design of new instances, independent selection of operating system and increased disk capacity. Users will be able to use these services to meet temporary increases in data requirements, servers, to support education etc. Cloud computing solutions are usually charged on a processor-power and data-traffic basis, but one of the advantages of ARNES' solutions is that they are available free of charge to eligible users.

KEYWORDS: CLOUD COMPUTING, SERVICE,
VIRTUALIZATION

uporabniki namestili svoj operacijski sistem, samostojno nastavljali vse detajle operacijskega sistema in obenem imeli možnost popolne prilagoditve. Arnes kot ponudnik storitve bo zagotavljal nemoteno delovanje strojne opreme, ki bo zagotavljala delovanje te storitve.

Storitev v osnovi bazira na uporabi virtualizacije, ki je ena od metod konsolidacije strojnih virov in uporabnikom omogoča boljše izkoristke same strojne opreme. Obenem virtualizacija omogoča tako imenovano »zeleno računalništvo«, kar bo v prihodnosti precej pomembna zadeva. Virtualizacija bo izvedena na gruči strežnikov, kar bo omogočalo nemoteno delovanje v primerih strojne okvare posameznih delov gruče. S takim pristopom bomo dosegli boljšo odzivnost in zanesljivost strežnikov, ki bodo gostovali v Arnesovem oblaku. Uporabniki tako ne bodo opazili razlike v delovanju strežnikov in se bodo lahko popolnoma posvetili upravljanju svojega strežnika in s tem bili razbremenjeni upravljanja s fizičnimi strežniki. Uporaba virtualizacije bo tudi omogočala enostavno razširitev Arnesovega oblaka, ko bo le ta dosegel svojo polno zmogljivost.

Uporabniki bodo z gostovanjem v Arnesovem oblaku pridobili predvsem s tem, ker ne bo več potrebno vzdrževati svoje strojne opreme. V oblaku namreč za strojno opremo skrbi ponudnik storitve, v tem primeru Arnesovi strokovnjaki. Glede na trenutno stanje je gostovanje v oblaku precej draga zadeva, Arnesov oblak bo ponujal gostovanje za upravičene stranke brezplačno.

Gostovanje v oblaku ima tudi svoje slabosti. Uporabniki namreč pri gostovanju v oblaku vse svoje strežnike preselijo v oblak in ne vedo, kje so dejansko podatki, ki so shranjeni na strežnikih. Obenem se pojavijo problemi z dostopom do teh podatkov v primeru nedosegljivosti Interneta, kar lahko povzroči dodatno škodo. Na Arnesu smo se tega lotili tako, da bomo vedno zagotavljali, da bodo podatki varno shranjeni v naših podatkovnih centrih, ki so fizično in požarno varovani, obenem zagotavljamo dežurnega systemskega administratorja, ki bo odpravil nepravilnosti v delovanju celotnega sistema v najkrajšem možnem času vse dni v tednu. Podobno kot za celoten oblak je poskrbljeno tudi za mrežni del infrastrukture, kjer Arnes zagotavlja redundanco za vse povezave med glavnimi vozlišči in podatkovnimi centri, kjer bodo nameščeni strojni viri. S tem bodo uporabniki imeli zagotovljeno zanesljivo delovanje strojne opreme in dostopa preko interneta.

ZAKLJUČEK

Arnes s svojo novo storitvijo spreminja pogled na sodobno računalništvo. Strojna oprema, ki je včasih zasedala prostor pri uporabnikih, se z vpeljavo nove storitve logično »seli« v Arnesove systemske prostore. Uporabniki se bodo lahko tako posvečali delu s samimi strežniki brez dodatnega napora okrog same strojne opreme.

Sam sistem Arnesovega oblaka je tudi zasnovan tako, da bo v prihodnosti omogočal enostavno razširitev in s tem lahko ponudil uporabnikom enostaven prehod iz sveta fizičnih strežnikov v območje računalništva v oblaku.

VIRI:

(2011) Wikipedia. [Online]. http://sl.wikipedia.org/wiki/Računalništvo_v_oblaku

ALI JE KAJ TRDEN VAŠ OBLAK? HOW STRONG IS YOUR CLOUD?!



GORAZD BOŽIČ,
ARNES

I/ The title is a paraphrase of a children's game "How strong is your bridge?" where a line of children (the train) passes under the hands of two players (the bridge).

POVZETEK

Storitve v oblaku pridobivajo na veljavi in omogočajo enostavno in cenovno ugodno implementacijo storitev za organizacijo. Izvoz podatkov in aplikacij v oblak pa ima nedvomno tudi varnostni vidik, ki ga običajno spregledamo. Smo še lastnik svojih podatkov in kaj narediti, če se oblak naenkrat razblini?

KLJUČNE BESEDE: OBLAK, VARNOST, ZANESLJIVOST, ZASEBNOST

ABSTRACT

Cloud computing is gaining in popularity due to the ease of use, scalability and economics. Outsourcing our data and applications undoubtedly has a clear security component, which is often overlooked. Are we still true owners of our data and what can we do if the cloud suddenly dissipates?

KEY WORDS: CLOUD, SECURITY, RELIABILITY, PRIVACY

UVOD

Enostavnost in dostopnost storitev v oblaku je dober razlog, da organizacije pričenjajo z uporabo teh storitev za različne namene. Kot ponavadi pa se kot zakasnela ali odri-njena misel pojavi vprašanje nadzora nad podatki in njihovo varnostjo. Z najemom oblaknih storitev podatke izrinemo iz našega (bolj ali manj) varnega okolja, kjer lahko z različnimi postopki in metodami poskrbimo za večnivojsko varovanje podatkov. Nujno je, da ponudnik storitev v oblaku prevzame del odgovornosti, ki se nanaša na zaščito podatkov in varen dostop do njih. Del njegove odgovornosti pa je odvisen od nivoja na oblaku, najmanj pri IaaS storitvah in največ pri SaaS.

POMISLEKI IN MOREBITNE PASTI

Poleg tega problema, da lahko zgradimo pravo trdnjavo na svojem lokalnem omrežju, nato pa vse podatke izvozimo v oblak, se trenutno kot morda največji problem kaže preveč enostavna avtentikacija. Z ukradenim geslom (ali drugim avtentikacijskim sred-stvom) lahko napadalec naenkrat pride do širokega nabora storitev v oblaku. Oblačne storitve zaenkrat še ne ponujajo bolj strukturiranega nadzora dostopa, preko katerega bi lahko opredelili več nivojev storitev in jih zaščitili z dodatnimi mehanizmi.

Oblaki delujejo vsak zase in ne obstajajo še standardi za oblačne storitve, kar je razumljivo, saj vsak ponudnik ponuja svojo različico in tudi privablja s prednostmi svoje rešitve. Po drugi strani pa za organizacijo to pomeni "lock-in" na enega ponudnika oziroma velike probleme pri migraciji z enega ponudnika na drugega. Ta neprožnost pa je še hujša, kadar ponudnik preneha s svojo dejavnostjo. Ali so sedanji preveliki, da bi propadli? Če pa bodo, ali bo kdo drug prevzel njihovo ponudbo, ali pa se bo naš oblak razpršil?

S premikom naše storitve v oblak bomo običajno zamenjali tudi pravno jurisdikcijo, pod katero sodijo naši podatki. Tudi ponudniki se tega zavedajo in Microsoft recimo navaja situacijo, kjer je njihov podatkovni center lociran na Irskem, njegove kapacitete pa uporabljajo stranke iz Nemčije. Oboje v EU boste rekli in torej ni problema? Ne čisto: Irska ima 24-mesečni rok hrambe prometnih podatkov, Nemčija pa 6-mesečnega.

PREDNOSTI RAČUNALNIŠTVA V OBLAKU

Oblak pa ponuja tudi nekaj prednosti, tudi varnostnih. Enotno upravljanje z nadgraj-dnjami in filtriranjem prometa in enostavno jačanje virtualnih strojev. Virtualizacija

običajno pomeni tudi možnost izdelave posnetkov stanja, kar lahko izkoristimo ob incidentih kot kopijo za forenzični pregled.

ZAKLJUČEK

Očitno je, da oblak ponuja udoben način nudenja storitev. Nekaj varnostnih pomislekov obstaja, a si jih lahko z ustrezno opredelitvijo v pogodbi olajšamo. Direktor evropske agencije za informacijsko varnost ENISA, Udo Helmbrecht, je v priporočilih o uporabi oblachnega računalništva zato svetoval: "Javne oblachne storitve ponujajo visok nivo dostopnosti in cenovne učinkovitosti. Vendar pa bi se uporaba morala trenutno omejiti na neobčutljive in nekritične aplikacije v kontekstu dobro definirane strategije vpeljave in z jasno izhodno strategijo." Predvsem ta izhodna strategija je nekaj, kar si ne smemo odmisлити ali odriniti v nedefinirano prihodnost.

VIRI

1. Daniele Catteddu: Security and Resilience in Governmental Clouds, ENISA Report
<http://www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds/>
2. Cloud Computing Risk Assessment, ENISA Report
<http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment>

VARNI NA INTERNETU SAFE ON THE INTERNET



JASMINA MEŠIČ,
ARNES

POVZETEK

V okviru Arnesa deluje tudi Slovenski center za posredovanje pri omrežnih incidentih SI-CERT, ki koordinira obveščanje in reševanje varnostnih problemov v računalniških omrežjih v Sloveniji. V letu 2011 SI-CERT prevzema tudi koordinacijo nacionalnega projekta ozaveščanja javnosti o informacijski varnosti. Projekt ozaveščanja je v sodelovanju z Ministrstvom za visoko šolstvo, znanost in tehnologijo zastavljen dolgoročno in bo naslavljal precej široko področje problematike informacijske varnosti, zato v začetni fazi kampanja izpostavlja tri najbolj kritična področja – spletne prevare, krajo identitete in spletno bančništvo. Projekt Varni na internetu naslavlja najširšo slovensko javnost, poseben sklop vsebin pa namenjamo manjšim podjetjem, ki pri svojem poslovanju prav tako uporabljajo spletno bančništvo in spletne trgovine.

KLJUČNE BESEDE: INFORMACIJSKA VARNOST, PROGRAM OZAVEŠČANJA, SPLETNE PREVARE, SPLETNO BANČNIŠTVO, DRUŽABNA OMREŽJA

UVOD

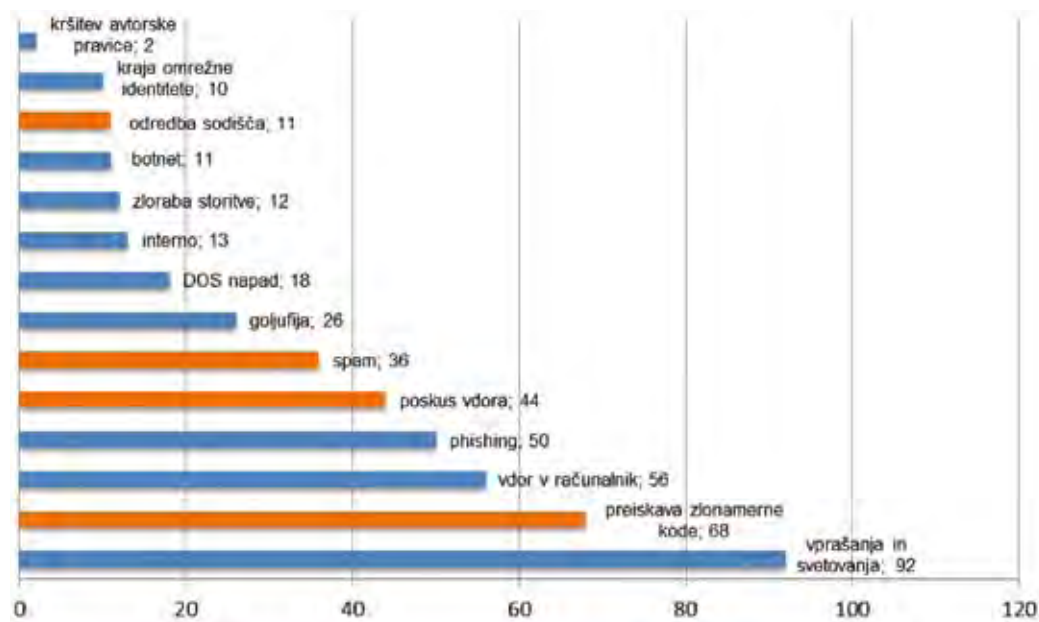
Uporaba interneta nam olajša komunikacijo in zabriše zemljepisne omejitve. Ravno zato smo na omrežju tudi bolj izpostavljeni različnim tveganjem. Z izkoriščanjem varnostnih lukenj, ranljivosti v programski opremi ali v naših vedenjskih vzorcih, lahko tujci pridobijo nadzor nad našo opremo, podatki in denarjem. V SI-CERT smo v letu 2010 prejeli 1.959 prijav (466 več kot leta 2009), na podlagi katerih smo obravnavali 478 incidentov, kar predstavlja kar 43 % porast v primerjavi z letom 2009 (Arnes 2011). Podatki o različnih tipih incidentov kažejo, da je prvič v delovanju SI-CERT do sedaj na vrhu svetovanje, kjer ne gre nujno za konkreten incident, ampak za splošna vprašanja o zaščiti in prepoznavanju vdorov ali spletnih goljufij (glej graf 1). To je pokazatelj, da uporabniki spleta potrebujejo jasna, natančna in razumljiva navodila kako zavarovati sebe in računalniško opremo.

ABSTRACT

SI-CERT is the Slovenian national CERT (Computer Emergency Response Team). SI-CERT is the main contact point for reporting network security incidents involving systems and networks located in Slovenia. SI-CERT is a service of ARNES (Academic and Research Network of Slovenia). In year 2011, SI-CERT has also taken over the coordination of the national project of raising public awareness on information security. Awareness raising project is being conducted in collaboration with Slovenian Ministry of Higher Education, Science and Technology and it is set as a long term activity. Awareness raising project will be addressing the rather broad scope of information security issues, so in the initial stage the campaign highlights the three most critical areas - online frauds, identity theft and online banking. Project Safe on the Internet is addressing the widest Slovenian public; a particular set of content is addressing SME (Small and Medium Enterprises), which also use online banking and online shops.

KEY WORDS: INFORMATION SECURITY, AWARENESS RAISING PROGRAM, ONLINE FRAUDS, ONLINE BANKING, SOCIAL NETWORKS

Graf 1:
VRSTE
OBRAVNAVANIH
INCIDENTOV V
LETU 2010 (ARNES
2011)



Zato tudi program ozaveščanja, ki je v sodelovanju z Ministrstvom za visoko šolstvo, znanost in tehnologijo zastavljen dolgoročno in bo naslavljal precej široko področje problematike informacijske varnosti. Vendar v začetni fazi projekta izpostavljam tri najbolj kritična področja - spletne prevare, krajo identitete ter spletno bančništvo, saj naša statistika kaže, da je predvsem naraslo število spletnih goljufig - phishing napadov ter prevar z lažnimi prodajami in nakupi preko omrežja. Projekt Varni na internetu bo izvajal javni zavod Arnes s strokovno podporo SI-CERT in pa v sodelovanju z MVZT, ki tudi v celoti financira projekt.

PROGRAM OZAVEŠČANJA O INFORMACIJSKI VARNOSTI

Dolgoročno je pglavitni cilj projekta Varni na internetu »vzgojiti« informacijsko pismenega spletnega uporabnika, ki bo znal varno in odgovorno uporabljati informacijsko-komunikacijske tehnologije. Kot prioriteto smo si zastavili dvig stopnje informiranosti o varni rabi interneta, ob tem pa pozornost namenjamo tudi bolj specifičnim sporočilom, ki jih želimo prenesti.

Ključni cilji projekta ozaveščanja so:

- dvigniti stopnjo zavedanja o različnih nevarnostih, katerim so uporabniki izpostavljeni na spletu;
- informirati o varni uporabi spletnega bančništva;
- informirati o različnih oblikah spletnih prevar in ponuditi praktične rešitve, kako se zavarovati;
- informirati o varstvu osebne identitete v socialnih omrežjih.

Zasnovali smo zgodbo, ki temelji na dualnosti, saj smo v resničnem življenju veliko bolj previdni in nezaupljivi, zakaj smo potem on-line drugačni? Tudi na spletu smo izpostavljeni različnim nevarnostim, zato moramo znati zaščititi sebe in svoj računalnik. Pglavitno sporočilo, ki ga želimo prenesti spletnim uporabnikom, smo strnili v slogan »Od mene je odvisno vse.«, saj sami lahko storimo največ, da zmanjšamo tveganja,

katerim smo izpostavljeni in v polni meri izkoristimo vse prednosti, ki jih internet prinaša. Kot zaščitni znak projekta Varni na internetu, nastopa prečrtan osliček, saj želimo na simpatičen, malo humoren način pristopiti k problemu, nikakor ne želimo moralizirati, strašiti, ali celo odvracati od uporabe določenih spletnih storitev.



VARNI NA INTERNETU

Od mene je odvisno vse.

www.varninainternetu.si

Skozi aktivnosti programa Varni na internetu naslavljamo najširšo slovensko javnost, saj je internet že skoraj nepogrešljiv del našega vsakdana. Ključna vodila varnega spletnega komuniciranja smo oblikovali z mislijo na povprečne slovenske uporabnike interneta - so informacijsko pismeni, se znajdejo v digitalnem okolju, uporabljajo IKT pri svojem izobraževanju, delu, e-upravi. So uporabniki spletnih bančnih rešitev. Na spletu iščejo dnevno-informativne novice, novice o glasbi, filmu, potovanjih, športu, uporabljajo socialna omrežja ter storitve elektronske pošte, do spleta pa dostopajo tudi v tujini. Poslužujejo se storitev spletnih trgovin in tudi sami prodajajo preko spleta (Bolha.com, eBay, Amazon ...). Imajo tudi določeno tehnično znanje (posodobitev določene aplikacije, namestitev protivirusnega programa ...). Projekt Varni na internetu neposredno ne naslavlja otrok in mladostnikov, vendar ima Arnes aktivno vlogo tudi kot partner projektov SAFE-SI in Spletno oko, ki potekata v okviru evropskega akcijskega načrta Varnejši internet.

Poseben sklop vsebin namenjamo manjšim podjetjem, ki prav tako pri svojem poslovanju uporabljajo spletno bančništvo in spletne trgovine. Predvsem samostojni podjetniki, obrtniki, manjša podjetja z 1-5 zaposlenimi, zaradi omejenih kadrovskih ali finančnih virov, pogosto kar sami skrbijo za svoj "IT-oddelek". Pri tem so izpostavljeni različnim tveganjem in potrebujejo specifične informacije, kako varno poslovati na spletu. Za manjša podjetja smo pripravili informativne brošure, ki smo jih razposlali na 150 VEM točk (omogočajo registracijo samostojnega podjetnika, izvajajo izobraževanja in svetovanja za podjetja op. p.) po Sloveniji. V brošurah smo izpostavili ključna tveganja, katerim so izpostavljeni, in podali preproste in razumljive napotke, kako se lahko zavarujejo. Prav tako v sodelovanju z Obrtno-podjetniško zbornico Slovenije pripravljamo specifičen sklop predavanj za obrtnike, z namenom izobraževanja in svetovanja o zagotavljanju omrežne varnosti pri poslovanju.

V projektu ozaveščanja postavljamo v središče nov izobraževalni portal www.varninainternetu.si, na katerem gradimo bazo znanja, tako da podajamo opise različnih spletnih nevarnosti, podajamo praktične napotke, kako se pred le-temi zavarujemo, posredujemo hitre »recepte«, torej zgoščene informacije o ključnih problematikah, obveščamo o aktualnih spletnih prevarah ter tudi pišemo spletni blog Fokus, v katerem bolj poglobljeno obravnavamo določeno varnostno vprašanje.

ZAKLJUČEK

Besede dr. Radovana Pajntarja, predstavnika Ministrstva za visoko šolstvo, znanost in tehnologijo, povzemajo ključno vodilo programa Varni na internetu: »Z vidika uporabnikov so sprejemljive le tiste tehnologije, ki jim je mogoče zaupati in zagotavljajo zadostno varnost ter zasebnost. Uporabniki, ki uporabljajo splet, imajo pravico, da se imajo možnost zaščititi, da so varni in da se tako tudi počutijo.«

VIRI

Arnes. 2011. Arnes – pregled aktivnosti 2010. Interno gradivo, Arnes.

ZASEBNOST V OBLAKU PRIVACY IN THE CLOUD



MAG. ANDREJ TOMŠIČ,
INFORMACIJSKI
POOBlašČENEC RS

POVZETEK

Javne oblike računalništva v oblaku vzbujajo pomisleke glede varstva osebnih podatkov, ki se kažejo predvsem na področju pogodbene obdelave osebnih podatkov, zavarovanja osebnih podatkov ter izvoza podatkov v tretje države. V prispevku so ti pomisleki podrobneje obravnavani, predstavljeni pa so tudi možni mehanizmi, s katerimi bi lahko okrepili zaupanje v storitve računalništva v oblaku. Zaupanje v te storitve je namreč bistveno za pravno nespornost in praktično sprejemljivost računalništva v oblaku pri izvajalcih, ki jih nimamo pod neposrednim nadzorom.

KLJUČNE BESEDE: ZASEBNOST, OSEBNI PODATKI, RAČUNALNIŠTVO V OBLAKU, ZAVAROVANJE OSEBNIH PODATKOV, IZVOZ OSEBNIH PODATKOV, POGODBENA OBDELAVA OSEBNIH PODATKOV

ABSTRACT

Public cloud computing services raise concerns in terms of personal data and privacy protection, which generally touch upon the questions of contractual processing of personal data, data security issues and transfer of personal data to third countries. The article examines these concerns and puts forward some mechanisms that could foster trust in public cloud computing services. Trust in public cloud services that are out of our direct control is fundamental for legal acceptability of such services and a key enabler for deployment in practice.

KEY WORDS: PRIVACY, PERSONAL DATA, CLOUD COMPUTING, DATA SECURITY, EXPORT OF PERSONAL DATA, OUTSOURCING

UVOD

Zadnjih nekaj letih je vedno več govora o računalništvu v oblaku (angl. cloud computing), ki s seboj prinaša veliko tehničnih, pravnih in drugih vprašanj. V oblak se pospešeno seli čedalje več obdelave osebnih podatkov, kar neizogibno poraja dvome glede skladnosti z zakonodajo na področju varstva osebnih podatkov in zasebnosti. V prispevku bom obravnaval računalništvo v oblaku s stališča varstva osebnih podatkov, pojasnil, zakaj ob tem prihaja do pomislekov s strani nadzornih institucij in varuhov zasebnosti ter podal razmišljanje o mehanizmih, ki bi lahko te pomisleke minimizirali.

KAJ JE RAČUNALNIŠTVO V OBLAKU?

Uvodoma moramo pojasniti, kaj sploh obravnavamo s pojmom računalništvo v oblaku. Gre za storitve računalniške obdelave, programske opreme, hrambe in dostopa do podatkov, ki s strani končnega uporabnika ne zahtevajo fizične lokacije, in konfiguracije sistema, ki zagotavlja storitve. Bistvena značilnost računalništva v oblaku je, da obdelava podatkov ne poteka na vnaprej določenem statičnem mestu, ločimo pa med javnimi, skupnostnimi, zasebnimi in hibridnimi oblaki.

V bistvu ne gre za nek popolnoma nov koncept, saj gre po mnenju nekaterih le za sodobno verzijo modela računalništva iz 60-ih, kjer je bil dostop do računalniških zmogljivosti časovno razporejen. Spletna e-pošta, spletna družbena omrežja ali storitve oddaljene hrambe (varnostnih kopij) podatkov so vse oblike računalništva v oblaku. Gre torej za zunanje izvajanje storitev (angl. outsourcing), pri čemer lahko pri zunanjem izvajalcu dobimo tako gostovanje mrežne infrastrukture, programske in strojne opreme, zmogljivosti za hrambo podatkov in tako dalje (Schneier, 2009). Namen in cilji računalništva v oblaku so predvsem omogočiti dostopnost do računalniških zmogljivosti iz katerekoli lokacije na ekonomičen, prilagodljiv in nadgradljiv način.

POMISLEKI NADZORNIH ORGANOV ZA VARSTVO OSEBNIH PODATKOV IN VARUHOV ZASEBNOSTI

V evropskem prostoru je skrb za zasebnost, natančneje za informacijsko zasebnost (varstvo osebnih podatkov) izdatno urejena v nekaterih pravnih aktivih, med katerimi je treba izpostaviti zlasti *Konvencijo Sveta Evrope* o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov Strasbourg iz leta 1981, *Direktivo 95/46/ES* o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter *Zakon o varstvu osebnih podatkov* (Uradni list RS, št. 94/07 – uradno prečiščeno besedilo ZVOP-1). Vidiki varstva osebnih podatkov, ki se ob uporabi računalništva v oblaku najbolj izpostavljajo, so:

- pogodbeno obdelava osebnih podatkov,
- zavarovanje osebnih podatkov in
- izvoz osebnih podatkov v tretje države.

POGODBENA OBDELAVA OSEBNIH PODATKOV

Zakonodaja na področju varstva osebnih podatkov (tako Direktiva kot ZVOP-1) seveda dopušča možnost, da upravljavec osebnih podatkov, torej tisti, ki je opredelil namen in sredstva obdelave, določena ravnanja z osebnimi podatki zaupa drugi osebi – pogodbenemu obdelovalcu. Med ta ravnanja lahko sodijo kakršnakoli dejanja, ki vključujejo osebne podatke – obdelava osebnih podatkov namreč pomeni kakršnokoli delovanje ali niz delovanj, ki se izvaja v zvezi z osebnimi podatki, ki so avtomatizirano obdelani ali ki so pri ročni obdelavi del zbirke osebnih podatkov ali so namenjeni vključitvi v zbirko osebnih podatkov, zlasti zbiranje, pridobivanje, vpis, urejanje, shranjevanje, prilagajanje ali spreminjanje, priklic, vpogled, uporaba, razkritje s prenosom, sporočanje, širjenje ali drugo dajanje na razpolago, razvrstitev ali povezovanje, blokiranje. Tu je treba poudariti, da gre tudi v situacijah, ko pogodbeni obdelovalec sploh ne ve, na koga se podatki nanašajo (npr. nudi zgolj storitev gostovanja prostora za hrambo podatkov), za obdelavo osebnih podatkov. Še več – tudi če upravljavec osebnih podatkov svoje podatke hrani pri zunanemu ponudniku hrambe in na njegovih diskovnih zmogljivostih hrani svoje podatke v kriptirani, zunanjemu ponudniku hrambe neberljivi obliki, tudi takrat gre za hrambo osebnih podatkov, s tem pa za obdelavo osebnih podatkov in zakonske dolžnosti tako naročnika kot ponudnika storitve. Navedeno poudarjam zato, ker marsikje preberemo, da je za varstvo osebnih podatkov poskrbljeno s šifriranjem podatkov. Šifriranje podatkov je le eden od mehanizmov zaščite osebnih podatkov – v izrazoslovju ZVOP-1 gre za zavarovanje osebnih podatkov (angl. data security), skratka za enega od ukrepov s katerim ščitimo celovitost, zaupnost in razpoložljivost podatkov, varstvo osebnih podatkov (angl. data protection) pa je precej širši pojem. Drugače povedano, podatke imamo lahko odlično »zaklenjene«, pa lahko vseeno pride do kršitve varstva osebnih podatkov – morda nimamo pravne podlage za obdelavo osebnih podatkov, morda jih uporabljamo za nezakonite namene, morda jih predolgo hranimo. Pri računalništvu v oblaku nam zanašanje zgolj na tehnične metode lahko izboljša varnost podatkov, ne moremo pa se s tem izogniti zakonodaji na področju varstva osebnih podatkov.

Če se vrnemo na pogodbeno obdelavo podatkov, gre torej za dopustno prakso, pod pogojem, da so vzpostavljene določene varovalke, med njimi pa je bistveno to, da upravljavec osebnih podatkov lahko računa na določen nivo zavarovanja osebnih podatkov. ZVOP-1

I/ Poleg ustreznosti zavarovanja je danski nadzorni organ izpostavil tudi vprašanja zagotovil pogodbenega obdelovalca, razmerja moči med upravljavcem in pogodbenim obdelovalcem ter zakonske pogoje za izvoz osebnih podatkov v oblak.

tako v 11. členu določa, da sme zunanji izvajalec opravljati posamezna opravila v zvezi z obdelavo osebnih podatkov v okviru naročnikovih pooblastil in osebnih podatkov ne sme obdelovati za noben drug namen. Medsebojne pravice in obveznosti morata urediti s pogodbo, ki mora biti sklenjena v pisni obliki in mora vsebovati tudi dogovor o postopkih in ukrepih, s katerimi bodo podatki zavarovani pred slučajnim ali nameranim nepooblaščenim uničevanjem podatkov, njihovo sprememba ali izguba ter nepooblaščen obdelava teh podatkov (24. člen. ZVOP-1). Na tej točki pa pridemo tudi do glavnega pomisleka varuhov zasebnosti – ali in kdaj lahko zaupamo (zunanjemu) ponudniku računalništva v oblaku?

ZAVAROVANJE OSEBNIH PODATKOV

Informacijska varnost je bistveni del in eno temeljnih načel vseh regulativnih aktov na področju varstva osebnih podatkov. Kot je že bilo pojasnjeno, gre za varovanje celovitosti, zaupnosti in razpoložljivosti osebnih podatkov in s tem zelo pomemben del širšega koncepta varstva osebnih podatkov. Na pomen zavarovanja osebnih podatkov je zelo podrobno opozoril danski nadzorni organ za varstvo osebnih podatkov, ki predvsem zaradi teh pomislekov¹ eni od danskih občin ni dovolil uporabe Google Apps (Datatilsynet, 2011). Ali so naši podatki v oblaku bolje varovani ali ne, ni enostavno vprašanje in nanj ni dopustno pavšalno odgovoriti v smislu, da je nekaj, kar imamo sami pod nadzorom, tudi bolj varno (ENISA, 2009). Kot poudarjajo nekateri avtorji gre predvsem za vprašanje zaupanja (Schneier, 2009). Tako kot moramo zaupati operacijskemu sistemu, strojni opremljeni, programski opremljeni, moramo zaupati tudi ponudniku računalništva v oblaku – gre pravzaprav za podobno stvar in le za dodatnega ponudnika, ki ga moramo presojeti z vidika zaupanja. Pri zunanjem izvajanju pa je vseeno ena pomembna razlika – če imaš računalniške zmogljivosti pod svojim nadzorom, lahko sam ali s pomočjo drugih poskrbiš za varnost s pomočjo drugih varnostnih mehanizmov (dokumente na svojem računalniku lahko npr. varuješ z varnostnimi kopijami, protivirusnimi programi, če recimo popolnoma na zaupaš posamezni rešitvi, npr. brskalniku ali operacijskem sistemu). Pri zunanjem izvajalcu pa gre za zaupanje v celoti, kar ne vključuje le zaupanja v varnostne postopke in ukrepe, temveč gre tudi za zanesljivost, dostopnost in stanovitnost obratovanja. Pri lastnem izvajanju se namreč ne bojiš, da bo tvoja diskovna polja kupil neposredni tekmeč, da bi moral čez noč plačati (več) za dostop do svojih podatkov in da boš podatke čez noč izgubil, če imaš ustrezne postopke varnostnega kopiranja. Ali – oziroma kdaj – smo pri oblaku lahko v to prepričani? Nikakor ne gre pozabiti tudi na človeški faktor, saj se ljudje kljub jasnim politikam pogosto poslužujemo različnih bližnjic. Če je bilo včasih potrebno vdreti v računalnik zaposlenega za pridobitev zaupnih podatkov, je danes morda dovolj dobiti njegovo gmail geslo, če si je zaupne dokumente posredoval na takšen račun, da bo lahko »delal od doma« (Zittrain, 2009).

Posebne težave pri zagotavljanju pričakovane ravni zavarovanja osebnih podatkov porajajo tudi povezana vprašanja izvoza osebnih podatkov v tretje države, ki (ne) zagotavljajo enake ravni varstva osebnih podatkov kot domača jurisdikcija.

IZVOZ OSEBNIH PODATKOV

Kljub nekaterim konvencijam in premikom k mednarodnim standardom (The Madrid Privacy Declaration, 2009) in enotnemu regulativnemu okviru varstva osebnih podatkov

smo trenutno še vedno soočeni z različnimi režimi in ravnmi varstva osebnih podatkov. Izvoz osebnih podatkov iz držav EU (in držav, ki zagotavljajo podobno raven varstva osebnih podatkov²) v tretje države je tako možen le pod določenimi pogoji (ZVOP-1 tako izvoz osebnih podatkov ureja v 2. poglavju, členu 63.-71.) Evropski režim varstva osebnih podatkov se precej razlike od ZDA, od koder prihaja nekaj največjih ponudnikov zunanjega računalništva v oblaku, nekateri medsebojni dogovori, kot je t.i. *dogovor o varnem pristanu* (angl. Safe Harbor) pa naj bi omogočili lažjo izmenjavo podatkov med tema različnima režimoma. Varni pristan omogoča upravljavcem osebnih podatkov, da svoje podatke posredujejo upravljavcem ali pogodbenim obdelovalcem iz ZDA (kot so npr. Google, Amazon ipd.), če so se ta podjetja zavezala k spoštovanju načel varnega pristana (Evropska komisija, 2000). Težava je v tem, da gre v bistvu za princip samo-regulacije in nekateri nadzorni organi za varstvo osebnih podatkov so mnenja, da pri računalništvu v oblaku to ne zadostuje (ULD, 2010) in da bi ponudniki računalništva v oblaku – zaradi prej navedenih pomislekov z vidika zavarovanja podatkov – morali biti dolžni ponuditi močnejša zagotovila (Cavoukian, 2008). Podobno stališče zagovarjajo tudi glede certifikacije SAS 70 Type II, ki so jo npr. opravili Amazon, Salesforce.com, Google in Microsoft, saj se izbor kontrol s strani naročnika in revizorja pogosto štiti in redko objavlja ter se obenem lahko znatno razlikuje od primera do primera (ULD, 2010).

Kakšna naj bi bila potem ustrezna zagotovila? Nadzorni organ za varstvo osebnih podatkov v nemški zvezni deželi Schleswig-Holstein (ULD) navaja dve možnosti. Prva je uporaba t.i. *zavezujočih poslovnih pravil* (angl. Binding Corporate Rules-BCR), gre pa za formalizirane politike oziroma dogovore s strani določene korporacije glede spoštovanja EU načel varstva osebnih podatkov, te dogovore pa mora potrditi nadzorni organ za varstvo osebnih podatkov iz ene ali več držav EU. EU je pri tem razvila tudi postopek t.i. vzajemnega potrjevanja BCR, pri katerem samo potrjevanje prevzame ena od držav članic, njeno presojo pa potem ostale članice zgolj sprejmejo oziroma potrdijo. BCR so postale precej pogost mehanizem za izvoz osebnih podatkov (npr. kadrovskih podatkov, podatkov o naročnikih) iz EU v tretje države.

Druga možnost pa je *neodvisno zunanje certificiranje* s strani ustrezno usposobljenih organizacij ali združenj. Določene aktivnosti v tej smeri vodi združenje Cloud Security Alliance (CSA), katerega cilj je oblikovati smernice za varno računalništvo v oblaku. Med možne posamezne ukrepe sodi tudi certificiranje rešitev v smislu pridobitve potrdila oziroma certifikata.

Pri preučevanju varstva zasebnosti ob izvozu podatkov v tretje države ne gre pozabiti na vprašanja dostopa do podatkov s strani tretjih oseb, ki lahko zakonito ali nezakonito prestrezajo podatke med uporabnikom in ponudnikom računalništva v oblaku. Pri tem gre lahko tako za državne organe (znani so primeri tajnih programov ameriške NSA), kakor tudi za subjekte zasebnega prava, zato so ustrezna zagotovila toliko pomembnejša.

Enotnega mnenja varuhov zasebnosti trenutno še ni, kljub temu pa je možno zaključiti, da je brez ustrezno zagotovljene ravni varnosti računalništva v oblaku uporaba predvsem javnih oblik računalništva v oblaku tvegana in da bo lahko le z ustreznimi varovalkami mogoče pričakovati pravno nespornost in praktično sprejemljivost tovrstnih rešitev.

ZAKLJUČEK

V prispevku sem obravnaval bistvene pomisleke varuhov zasebnosti, ki se nanašajo predvsem na zagotavljanje zaupanja v storitve (javnega) računalništva v oblaku. Zavarovanje podatkov pri zunanjih izvajalcih, tako na ravni posameznega ponudnika kot na ravni državnega režima varstva osebnih podatkov, v katerega se podatki prenašajo, je pri varuhih zasebnosti najbolj izpostavljeno vprašanje, zavezujoča poslovna pravila in neodvisno zunanje certificiranje pa se kažejo kot možni mehanizmi za vzpostavitev zaupanja tako pri naročnikih kot pri nadzornih organih za varstvo osebnih podatkov.

VIRI

Cavoukian, A. (2008): Privacy in the Clouds. A White Paper on Privacy and Digital Identity: Implications for the Internet. Information and privacy commissioner of Ontario. Dostopno na: <http://www.ipc.on.ca/images/Resources/privacyintheclouds.pdf>

Cloud Computing und Datenschutz: Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD). Dostopno na: <https://www.datenschutzzentrum.de/cloud-computing/> (objavljeno 18.6.2010).

Datatilysynet, The Danish Data Protection Agency: Processing of sensitive personal data in a cloud solution. Dostopno na: <http://www.datatilysynet.dk/english/processing-of-sensitive-personal-data-in-a-cloud-solution/> (objavljeno 3.2.2011).

Direktiva 95/46/ES z dne Evropskega parlamenta in Sveta o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov. OJ L 281, 23/11/1995.

ENISA: Cloud Computing Risk Assessment. Dostopno na: <http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment> (objavljeno 20.9.2009).

Evropska komisija: 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, OJ L 215, 25/08/2000 P.0007 – 0047.

Konvencija Sveta Evrope o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov (Uradni list RS(28. 2. 1994)-MP št. 3-18/1994 (RS 11/1994)).

Schneider, B.(2009): Cloud Computing. Dostopno na: http://www.schneider.com/blog/archives/2009/06/cloud_computing.html (objavljeno 4.6.2009).

The Madrid Privacy Declaration - Global Privacy Standards for a Global World, 3.11.2009. Dostopno na: <http://thepublicvoice.org/madrid-declaration/>.

Zakon o varstvu osebnih podatkov (Uradni list RS, št. 94/07 – uradno prečiščeno besedilo; v nadaljevanju: ZVOP-1).

Zittrain, J. (2009): Lost in the Cloud New York Times. Dostopno na http://www.nytimes.com/2009/07/20/opinion/20zittrain.html?_r=1; (objavljeno 19.6.2009).

SLOVENSKO OMREŽJE GRID: DOSTOP DO VISOKIH RAČUNSKIH ZMOGLJIVOSTI V SLOVENIJI NATIONAL GRID INITIATIVE



PROF. DR. BORUT PAUL
KERŠEVAN,
JAN JONA JAVORŠEK,
ODSEK ZA
EKSPERIMENTALNO
FIZIKO DELCEV,
INSTITUT JOŽEF
STEFAN

POVZETEK

Napredek pri razvoju komercialnih procesorjev je s področja visokozmogljivih računalniških sistemov za raziskovalno izrinil superračunalnike, z razvojem omrežja pa so se gruče strežnikov povezale v večje sisteme, iz česar je v evropskem prostoru zrasla evropska infrastruktura mrežnega računalništva grid, s katero upravlja Evropska iniciativa za grid EGI. V prispevku bo predstavljeno delovanje infrastrukture grid in različnih tipov gruč v njej ter prednosti enotnega dostopa preko vmesne programske opreme grid v okviru Slovenske nacionalna iniciativa za grid pod vodstvom Arnesa, ki v Sloveniji posameznikom in organizacijam omogoča dostop do moči evropskega omrežja grid.

KLJUČNE BESEDE: GRID, NGI

ABSTRACT

Progress in commercial processor development is edging supercomputers out of the field of high-performance computing systems and the constant development of networks means that clusters of servers are being linked into larger systems, out of which has developed the European infrastructure of the network computing grid, operated by the European Grid Initiative (EGI). The paper will present the operation of grid infrastructure and various types of clusters, and the benefits of uniform access via intermediate grid software within the Slovenian National Grid Initiative led by ARNES, which enables individuals and organisations in Slovenia to access the power of the European grid network.

KEY WORDS: GRID, NGI

V zadnjem desetletju je napredek pri razvoju komercialnih procesorjev in omrežne infrastrukture bistveno spremenil področje visokozmogljivih računalniških sistemov za raziskovalno rabo. Nekdanje superračunalnike, ki so bili zgrajeni kot veliki večprocesorski sistemi s posebnimi procesorji in posebnimi pomnilniškimi enotami ter hitro notranjo povezavo med procesorji in pomnilniki, so nadomestile velike gruče strežnikov s komercialnimi procesorji in običajnim pomnilnikom, ki so med seboj povezani s komercialnimi omrežnimi komponentami (ethernet s prepustnostjo 1 Gb/s ali infiniband s prepustnostjo 40 Gb/s za naloge, ki potrebujejo medsebojno komunikacijo med procesi v različnih strežnikih). Ta premik se je zgodil zaradi dveh razvojnih trendov: komercialni procesorji so postali ne le cenovno, temveč tudi po zmogljivosti, primerljivi s superračunalniškimi sistemi, razvoj omrežne tehnologije pa je z dostopnostjo lokalnih omrežij 1 Gb/s ethernet in 40 Gb/s infiniband omogočil gradnjo gruč, ki so dovolj odzivne za različne tipe nalog, tudi naloge, kjer morajo posamezni procesi komunicirati med sabo. Nova tehnologija pa omogoča raziskovalnim centrom, da izbirajo opremo, ki je najprimernejša za njihove naloge. Tako imajo lahko posamezna računska vozlišča različno število procesorskih jeder, različno količino pomnilnika na jedro, različne povezave in različne diskovne kapacitete glede na pričakovane tipe naloge. Ta način gradnje računskih gruč omogoča optimalno konfiguracijo za naloge posamezne discipline ali raziskovalnega projekta in zmanjša nepotrebne stroške. Nastala sta zlasti dva tipa centrov – centri z velikim številom procesnih jeder, namenjenih za naloge, ki jih je mogoče paralelizirati, in centri, ki opravljajo naloge, kakršne so nekdanje zahtevale superračunalnike, in imajo zato na svojih računskih vozliščih nameščene povezave infiniband. Te imenujemo visokozmogljivi sistemi (HPC – high performance computing).

V istem obdobju je razvoj hitrega akademskega omrežja med raziskovalnimi in univerzitetnimi centri omogočil vse učinkovitejše povezovanje računskih gruč v večje siste-

me. Tako je postopoma v evropskem prostoru zrasla evropska infrastruktura mrežnega računalništva grid. Evropsko omrežje grid se je razvijalo z vrsto projektov (EGEE-I do III, NorduGrid, Unicore), danes pa z njim upravlja Evropska iniciativa za grid EGI, ki jo sestavljajo nacionalne iniciative držav članic, med njimi tudi Slovenska nacionalna iniciativa za grid, ki jo vodi Arnes.

V okviru razvoja visoko zmogljivega omrežja grid je s sodelovanjem številnih raziskovalnih skupin, zlasti skupin, ki delajo na projektih Velikega hadronskega trkalnika v Cernu, tako nastala vrsta implementacij vmesne programske opreme grid, ki je ne le omogočila povezovanje posameznih računskih gruč v večji sistem, temveč je s standardnimi vmesniki omogočila tudi dostop do izjemnih podatkovnih zmogljivosti in z uporabo akademskega omrežja in podatkovnih skladišč omogočila obdelavo izjemnih količin podatkov. Tako je nastal nov pojem, visoko pretočno računalništvo (HTC, High Throughput Computing). Pod tem pojmom razumemo omrežje računskih centrov, ki jih povezuje zmogljiva omrežna povezava in kompatibilna vmesna programska oprema ter s svojo strojno in programsko opremo omogočajo obdelavo in prenos zelo velikih količin podatkov. Raziskovalna skupina ATLAS tako s pomočjo različnih omrežij grid na dan obdela 3 PB podatkov (280 Gb/s oz. 35 GB/s).

ANATOMIJA RAČUNSKEGA GRIDA

Računski grid si lahko predstavljamo kot gručo gruč. Vsak računski center ima lastno računsko gručo, ki ima nadzorno vozlišče za upravljanje gruč, podatkovno shrambo (strežnik z množico diskovnih polij) ter računsko vozlišča za opravljanje nalog. Slednja so danes običajno namenski strežniki, lahko pa so tudi v souporabi kot delovne postaje. Na vseh strežnikih tipično teče operacijski sistem GNU/Linux. Programskih oprem za upravljanje gruč je na voljo zelo veliko in imajo različne značilnosti, med njimi pa so tako prostokodne kot komercialne.

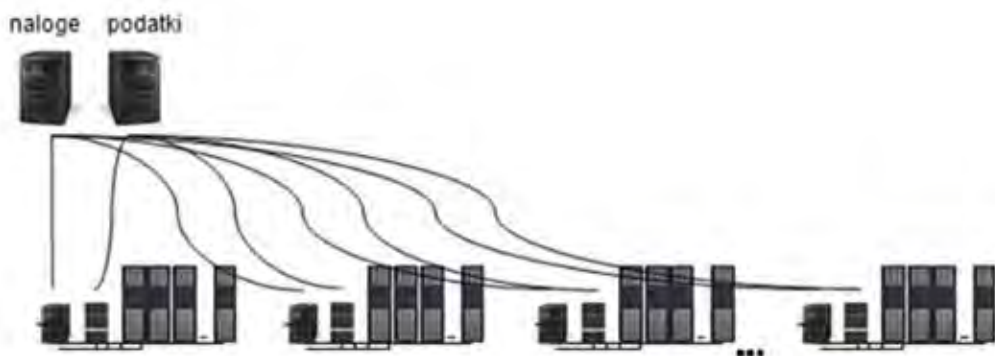
Značilnosti posamezne gruč so lahko zelo različne in lahko podpirajo različna okolja za izvajanje nalog, različne knjižnice za visokoprepustno računanje (MPI ali OpenMP) ipd.

Povsem neodvisno od programske opreme za upravljanje z gručo je nameščena vmesna programska oprema grid. Njena naloga je zagotavljanje standardiziranega vmesnika za upravljanje z nalogami na gruč. Obstaja več implementacij, v slovenskem omrežju grid npr. podpiramo NorduGrid ARC in gLite. Vmesna programska oprema grid lahko preko upravljalnika gruč preverja stanje gruč ter upravlja z nalogami, ima pa tudi vrsto servisov, ki v omrežje sporočajo podatke o razpoložljivih zmogljivostih in delovanju gruč. Ti servisi vključujejo informacijske servise (razpoložljive zmogljivosti), nadzor (testi in javljanje napak), statistiko (koliko in kakšne naloge so se izvajale na gruč) ter podatkovne prenose do upravljalnika gruč ali podatkovne shrambe.

V evropskem omrežju EGI se vsako središče grid vključuje v nacionalno omrežje, ki ga vodi nacionalna iniciativa za grid. To zagotavlja osrednje servise za nadzor, obveščanje in statistiko, običajno pa skrbi tudi za informiranje administratorjev, izobraževanje, varnost in razvoj omrežja. Preko nacionalnih omrežij pa je vsako središče grid vključeno v evropsko omrežje EGI, kjer je središče zavedeno v vseh osrednjih informacijskih sistemih.

Na ta način posamezno središče grid z vključitvijo v omrežje postane dostopno vsem uporabnikom grida. Pri tem ostane ves nadzor nad gručo v rokah lokalnih administratorjev, ki odločajo, katere skupine in kateri projekti bodo imeli dostop do zmogljivosti gruče. To poteka preko sistema virtualnih organizacij, s katerimi projekti in raziskovalne skupine organizirajo pravice za dostop do razpoložljivih sredstev, pri čemer je za overjanje in varnost poskrbljeno z infrastrukturo javnih ključev organizacije International Grid Trust Federation (IGTF). Tako lahko upravljavec vsakega centra določi, kakšne naloge in kateri uporabniki bodo uporabljali sredstva centra, ne da bi se moral zato ukvarjati z upravljanjem posameznih uporabniških imen in pravic za veliko množico uporabnikov, za varnost in overjanje pa skrbi robusten sistem z razvejano mednarodno varnostno mrežo.

Slika 1:
SHEMA OMREŽJA
GRID KOT GRUČE
GRUČ



SLOVENSKO OMREŽJE GRID

Slovensko omrežje grid se razvija od leta 2003, ko je na Institutu »Jožef Stefan« nastala prva slovenska gruča grid. Namenjena je bila delu v okviru omrežja grid za projekt Velikega hadronskega trkalnika v Cernu. IJS je sodeloval tudi v projektih EGEE, EGEE-II in EGEE-III, pri čemer se je vse bolj poglobljalo sodelovanje z akademskim omrežjem Arnes, saj bi brez podpore akademskega omrežja takšno delo ne bilo mogoče. Končno je Arnes prevzel vodilno vlogo pri ustanavljanju Slovenske iniciative za grid (SLING) in slovenskega omrežja grid (SiGNET, Slovenian Grid Network) ter postal eden od ustanovnih članov Evropske iniciative za grid EGI.

Tako imamo v Sloveniji danes najsodobnejše omrežje grid, ki je namenjeno zlasti akademskemu in visokoškolskemu raziskovalnemu delovanju, odprto pa je tudi za sodelovanje z industrijo. Omrežje trenutno sestavljata centra na Arnesu in na Institutu »Jožef Stefan«, v fazi vključevanja pa je še vrsta drugih centrov fakultet in državnih agencij. Omrežje šteje približno 1500 procesnih jeder in ima 220 TB diskovnih zmogljivosti. Arnes zagotavlja osrednje servise, podporo in izobraževanje, pri vzdrževanju gruč pa sodelujejo strokovnjaki z drugih centrov, ki so vključeni v iniciativo.

Večina kapacitet slovenskega omrežja je namenjena zlasti za delo na področjih, na katerih delajo lastniki opreme, vendar se uporabo omogoča tudi drugim raziskovalcem. Tako poleg virtualnih organizacij ATLAS, Pierre Auger in BELLE (eksperimentalna fizika delcev in astrofizika) na teh zmogljivostih tečejo tudi naloge s področja aplikativnega jezikoslovja, statistike, informatike, gradbeništva in statistike itd.

Slovensko omrežje je trenutno v fazi hitre širitve. Obstoječe zmogljivosti centrov se vsako leto nadgrajuje, prehajamo v namestitev notranjih omrežij infiniband, vključujejo pa se tudi organizacije, ki imajo obstoječe ali nove gruče in jim bo omrežje grid olajšalo upravljanje z njimi in s souporabo vseh zmogljivosti omogočilo boljši izkoristek in dostop do večjih zmogljivosti.

Slovenska nacionalna iniciativa za grid zagotavlja nacionalne servise in povezljivost za vse centre, ki bi želeli svoje gruče vključiti v omrežje. Ima pa tudi lastne kapacitete, ki omogočajo posameznim raziskovalcem ali organizacijam preizkusiti tehnologijo ali uporabljati neznansko moč grida za lastne raziskovalne naloge. Te naloge pa so lahko zelo različnih tipov glede na potrebno programsko infrastrukturo, zahteve po V/I kapacitetah gruče in računskih vozlišč, zmožnosti medsebojne povezljivosti vozlišč za delo s knjižnicami OpenMP in MPI, diskovne kapacitete vozlišč in gruče ter zahtevano zunanjo omrežno povezavo do omrežja GÉANT. Vmesna programska oprema za grid omogoča enovit dostop do različnih virov, ki lahko izpolnijo še tako specifične zahteve.

S stališča raziskovalca so sodobni računski gridi omrežja visoko zmogljivih računskih gruč, ki se vedejo kot en sam sistem in v uporabniku v okviru mednarodnih kooperacij omogočajo dostop do izjemnih računskih in podatkovnih kapacitet, ki so za velikostni red večje kot karkoli je mogoče doseči znotraj ene same organizacije. Za dostop so na voljo orodja ukazne vrstice, na osnovi katerih si področja in raziskovalne skupine večinoma vzpostavijo spletne portale in aplikacije za avtomatizacijo večjih skupin nalog.

Grid je tako postal eno od sodobnih orodij, ki omogoča uporabo novih raziskovalnih pristopov ter sodelovanje v velikih mednarodnih projektih, kjer so raziskovalne skupine in centri združeni v virtualne organizacije, ki imajo dostop do skupnih sredstev.

UPRAVLJANJE Z IDENTITETAMI NA NORVEŠKEM IDENTITY MANAGEMENT IN NORWAY



LARS KVITENG,
UNINETT

POVZETEK

Feide je norveška infrastruktura za overjanje istovetnosti in avtorizacijo na področju izobraževanja. Uporabnikom omogoča dostop do aplikacij z enotnim uporabniškim imenom in geslom. Federacija Feide deluje že deseto leto, njeni člani pa so vse univerze ter skoraj vse visoke šole na Norveškem. Feide sodeluje tudi z osnovnimi in srednjimi šolami. Predstavitev se osredotoča na postopke, ki so se v Feide izkazali za uspešne, in prednosti, ki jih ponujajo – za domače organizacije, ponudnike storitev in končne uporabnike. Pojasnili bomo tudi, kako se tega trenutno lotevamo in predstavili naše načrte v prihodnosti.

KLJUČNE BESEDE: FEIDE, IDM

ABSTRACT

Feide is the Norwegian authentication and authorisation infrastructure for the education sector. Feide gives end users access to webservices with single username and password. The Feide Federation has been in operation for ten years, and today all universities and most university colleges in Norway are members of the Federation. Feide also covers primary and lower secondary schools. My presentation will focus on what the successful policies have been for Feide, and what the benefits have been – for home organisations, service providers and end users. I will also focus on how we are currently going about this, and then mention a few words about the road ahead.

KEY WORDS: FEIDE, IDM

OKROGLA MIZA: FEDERATIVNE STORITVE V SLOVENSKEM IZOBRAŽEVALNEM PROSTORU

ROUND TABLE: FEDERATED SERVICES IN SLOVENIAN EDUCATION

VODI:
DAVOR ŠOŠTARIČ,
MVZT

POVZETEK

Najprej smo si morali zapomniti množico telefonskih števil; danes nam telefonska »pamet« to breme odvzema. Potem so prišli PIN-i. Tu si pomaga vsak sam z bolj ali manj uspešno »mnemonično trikologijo«. In zdaj je tu še nepregledna množica gesel za dostop do številnih spletnih in računalniških aplikacij ter storitev. Vsaj takrat, ko je dovoljenje za uporabo takih aplikacij in storitev povezano z določenim statusom posameznika (študent, učitelj, raziskovalec, zaposleni ...), nam iz zadrege pomagajo posebni sistemi, namenjeni prav temu – da se namreč iz enega mesta taki aplikaciji ali storitvi da vedeti, da sta dostop in uporaba v okvirih dovoljenega. Ampak – ali se to resnično uporablja in ali imajo naši uporabniki iz izobraževalnega in raziskovalnega sveta dejansko kaj od tega? O tem se bomo pogovarjali in pogledali, katere svetovne vrhunske storitve so na te načine dostopne pa tudi kaj in kako bi naj naše organizacije (npr. univerze, šole in raziskovalni inštituti) naredile pri svojih internih aplikacijah in storitvah.

KLJUČNE BESEDE: STORITVE

ABSTRACT

First we had to remember many telephone numbers; today, our telephone's memory removes this burden. Then came PIN numbers, remembered through more or less successful mnemonic tricks. Now there are masses of passwords for access to numerous web and computer applications and services. At least where permission to use such applications and services is linked to a particular status (student, teacher, researcher, employee), there are special systems designed to help with this problem – to enable such applications or services to recognise from a single place that access and use are permissible. But are they actually used, and what do our education and research users actually gain from this? We will discuss this and investigate which world-class services are available, and what and how our organisations (e.g. universities, schools and research institutes) should do in their internal applications and services.

KEY WORDS: SERVICES

SPLETNI DNEVNIK IN IZMENJAVA DATOTEK PREK SPLETA BLOGS AND WEB-BASED FILE EXCHANGE

MITJA MIHELIC,
ARNES

POVZETEK

Spletni dnevnik oz. blog vam omogoča čim enostavnejšo objavo vsebin na spletu. Svoj blog lahko na enostaven način prilagodite in ga uporabite celo za spletno stran organizacije ali projekta. Pri tem boste uporabniki pripravljali vsebine, na Arnesu bomo poskrbeli za nemoteno delovanje strežnika. Po elektronski pošti v zadnjem času pošiljamo vedno več multimedijских vsebin in tudi dokumenti so vedno večji. Na težavo naletimo takrat, ko tako velikih datotek prek poštних strežnikov ne moremo odposlati ali sprejeti. Za premostitev te težave smo na Arnesu pripravili rešitev, ki vam bo prek spletnega vmesnika omogočila enostavno izmenjavo večjih datotek z vašimi kolegi in sodelavci, ne glede na to, kako imajo nastavljene poštne strežnike.

KLJUČNE BESEDE: BLOG, DINAMIČNE SPLETNE VSEBINE, DATOTEKE, E-POŠTA

UVOD

Spletni dnevnik ali blog se je pojavil kot osebna spletna stran, namenjena pisanju dnevnika, komentiranja, opisa dogodkov ali prikaza slik in videa. Vnosi so ponavadi prikazani v obratnem kronološkem zaporedju. Večina blogov je interaktivnih in obiskovalcem omogoča na primer komentiranje prispevkov, ocenjevanje ter nalaganje slik. S časom je uporaba bloga postala čedalje bolj enostavna, številni dodatki in preobleke pa blogu omogočajo uporabo za kakršenkoli namen. Tudi v poslovnem svetu je spletna predstavitev podjetja ali njihovega projekta izdelana na neki različici programske opreme za blog, saj omogoča hitro obveščanje z objavljanjem kratkih novic.

Izmenjava datotek prek spleta ponavadi pomeni pošiljanje priložnosti po e-pošti, kar je lahko neuspešno zaradi različnih razlogov. Najpogostejši razlog je prav gotovo poskus pošiljanja priložnosti, katere velikost presega omejitve največjega dovoljenega sporočila na mail strežnikih. Rešitev za to težavo je spletna aplikacija Filesender, preko katere datoteko enostavno odložite na Arnesov strežnik, nato sistem vašim sodelavcem samodejno pošlje povezavo do datoteke. Storitve ponuja začasno shranjevanje datotek, ki se po določenem času izbrišejo, zato ni namenjena izmenjavi datotek, ki morajo biti dostopne trajno.

SPLETNI DNEVNIK – BLOG

Arnes je kot rešitev za storitev spletnega dnevnika izbral orodje Wordpress, ki stremi k temu, da uporabnikom ponuja čim bolj prijazno in enostavno platformo za delo z blogom. Uporabnik le obišče stran za prijavo v Arnesov blog ter se prijavi s svojim uporabniškim imenom in geslom. Po uspešni prijavi lahko takoj začne z objavljanjem svojih prispevkov ali postov. Klikne na gumb „New Post“, vpiše naslov, doda spremni tekst, morda vključi še kakšno sliko in vse skupaj objavi s klikom na gumb „Publish“.

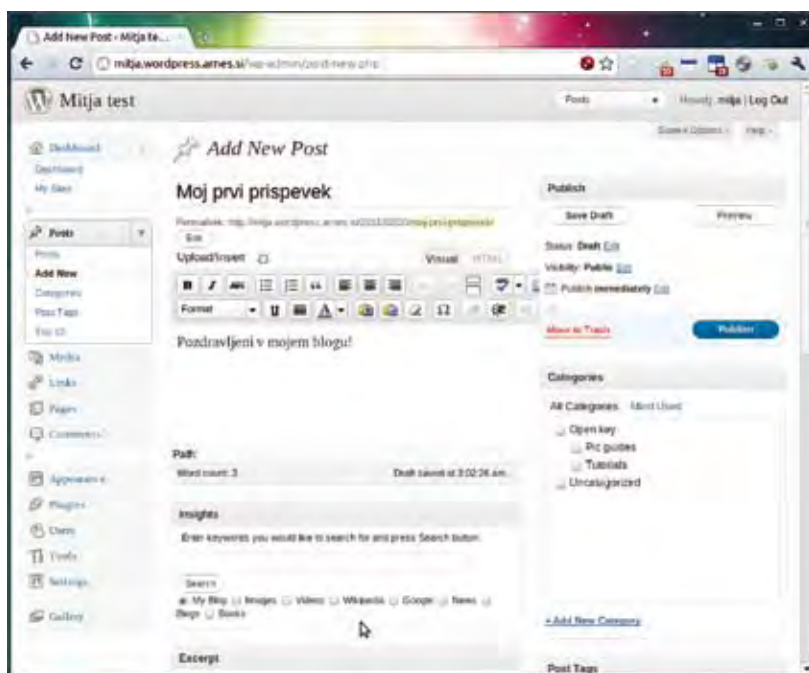
ABSTRACT

Weblogs or blogs allow you to effortlessly publish content online. You can easily adapt your blog and even use it as a website for an organisation or a project. Users create content, while ARNES ensures uninterrupted operation of the underlying infrastructure. More and more multimedia content is sent via email every day, and documents are also growing in size. Problems arise when such large files cannot be sent or received via email. To overcome these problems, ARNES has prepared a solution that will allow you to exchange large files with your colleagues and associates via a web interface, regardless of the configuration of their mail servers.

KEY WORDS: BLOG, DYNAMIC WEB CONTENT, FILES, E-MAIL

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 zelenih blogov.

Slika 1:
PRIPRAVA
PRISPEVKA



Nekateri uporabniki bodo najprej spremenili izgled bloga, da bo boljše 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 veliko število tem: od enostavnih ali minimalističnih, do osebnih ali poslovnih. Menjava tem je zelo enostavna, dovolj je klik na povezavo „Activate“ pri posamezni temi in rezultat je takoj viden na blogu.

Slika 2
IZBIRA TEME



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

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

Podobno, kot teme omogočajo spremembo izgleda, vtičniki ali plugini dopolnjujejo in razširjajo obstoječo funkcionalnost. 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. Namesto dodajanja posameznih slik v prispevek, jih uporabniki lahko združijo v galerije, katere združijo v albume. V galerijo s svojega računalnika naložijo slike in jih ustrezno opremijo s kratkimi imeni, daljšimi opisi in dodatnimi oznakami. Galerija omogoča osnovne operacije za prilagoditev slike in sicer: spremembo velikosti ter zasuk levo in desno. Galerijo enostavno dodajo v prispevek s klikom na gumb za vstavljanje galerije. Pri tem imajo na izbiro tri načine prikaza slik. Prvi je seznam slik oziroma pregled pomanjšanih slik v obliki tabele. Nad tabelo se prikaže povezava, ki omogoči preklon prikaza seznama slik v diaproyekcijo in nazaj. S klikom na pomanjšano sliko se odpre povečana slika, pod njo se prikažeta gumba za navigacijo naprej in nazaj po galeriji. Drugi način je diaproyekcija, ki ciklično zaporedoma prikazuje slike iz galerije. Klik na sliko sproži predčasen prehod na naslednjo sliko. Tretji način je brskalnik, ki v okviru prikazuje sliko, pod katero sta gumba za navigacijo naprej in nazaj po galeriji.

IZMENJAVA DATOTEK PREK SPLETA - FILESENDER

Filesender je spletna storitev, ki uporabnikom omogoča varno in enostavno pošiljanje velikih datotek prek svetovnega spleta. Uporabnik se v storitev prijavi s svojim uporabniškim imenom in geslom. Neregistrirani uporabniki lahko do storitve dostopajo preko voucherja, ki jim ga podeli registriran uporabnik.

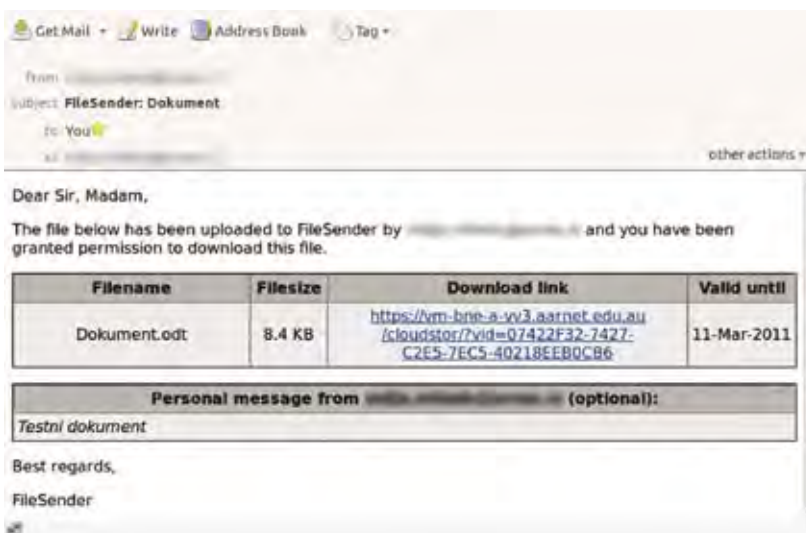
Vmesnik, ki se prikaže po uspešni prijavi, je soroden oknu za pošiljanje e-pošte in uporaba je enostavna. Uporabnik vpiše e-poštne naslove prejemnikov, kratek opis datoteke ter sporočilo prejemnikom, nastavi datum, po katerem se datoteka samodejno izbriše, in naloži datoteko.

Slika 3:
NALAGANJE
NOVE
DATOTEKE



Po uspešnem zaključku sistem samodejno pošlje e-pošto s spletno povezavo do naložene datoteke pošiljatelju in prejemnikom

Slika 4:
E-POŠTA S
SPLETNO
POVEZAVO DO
NALOŽENE
DATOTEKE



Klik na spletno povezavo v prejeti e-pošti uporabniku prikaže vmesnik, od koder si nato prenese datoteko na svoj računalnik.

Slika 5:
PRENAŠANJE
DATOTEKE
NA SVOJ
RAČUNALNIK



Po vsakem uspešnem prenosu datoteke pošiljatelj in prejemnik, ki je datoteko prenesel na svoj računalnik, prejmeta potrditev o uspešnem prenosu.

ZAKLJUČEK

Uporaba spletnega dnevnika uporabnikom prinese novo dimenzijo objavljanja svojih vsebin na internetu. Objavljanje novic je enostavno, besedilo pa je lahko dodatno popestrjeno s slikami ali video vsebino. Velika izbira preoblek oziroma tem omogoča, da blog spremeni svoj izgled in postane spletna stran organizacije, projekta ali osebna spletna stran. Z Wordpressom bodo naši uporabniki dobili sodobno in enostavno orodje za izdelavo svoje spletne predstavitve.

Rešitev izmenjave datotek prek spleta, Filesender, močno olajša delo, saj datotek samih ne bo več potrebno pošiljati po e-pošti. Uporabnik bo datoteko prek spletnega vmesnika naložil na Arnesov strežnik in določi naslovnike spletne povezave do datoteke. Sistem nato samodejno razpošlje spletno povezavo naslovnikom. Tako ne bo prihajalo do nepotrebnega polnjenja poštnega predala, kar bo še posebej dobrodošlo tistim uporabnikom, ki so na poštnem strežniku omejeni s prostorom.

VIRI

Spletna stran: www.wordpress.org (20.02.2011).

Spletna stran: www.filesender.org (20.02.2011).

NADGRADNJA GOSTOVANJA VIRTUALNIH STREŽNIKOV IN DINAMIČNIH SPLETNIH STRANI UPGRADING VIRTUAL SERVER AND DYNAMIC WEB SERVICE HOSTING

DOMEN ZALAR,
ARNES

POVZETEK

Spletno gostovanje virtualnih strežnikov in dinamičnih spletnih strani je ena izmed najbolj priljubljenih Arnesovih storitev, saj na njem svoje spletne strani gosti že preko 700 organizacij. Rešitev redno nadgrajujemo, v letu 2011 pa bo novosti kar veliko. Vsi strežniki bodo temeljili na operacijskem sistemu Centos 6 in PHP 5.3, kar bo omogočalo namestitve novjših aplikacij, kot je na primer Moodle 2 ali Joomla 1.6. Vaše spletne storitve že podpira tudi IPv6-protokol, dostop do vaših podatkov pa lahko omogočite tudi preko varnega HTTPS-protokola. Poleg tega boste lahko, predvidoma do konca leta 2011, svoje strežnike upravljali tudi preko intuitivnega grafičnega vmesnika.

KLJUČNE BESEDE: VIRTUALNI STREŽNIK, IPV6, HTTPS, PHP, GRAFIČNI VMESNIK

ABSTRACT

Web hosting of virtual servers and dynamic websites is one of the most popular of ARNES' services, with ARNES hosting the websites of more than 700 organisations. We regularly upgrade solutions, with many innovations scheduled for 2011. All servers are now based on the Centos 6 operating system and PHP 5.3, enabling installation of the latest applications, such as Moodle 2 or Joomla 1.6. Your web services can now support the IPv6 protocol, while access to your data can be enabled via the secure HTTPS protocol. We have significantly increased disk space and available internal memory. By the end of 2011, you should also be able to manage your server to some extent yourself via an intuitive graphical interface.

KEY WORDS: VIRTUAL SERVER, IPV6, HTTPS, PHP, GRAPHICAL INTERFACE

GOSTOVANJE DINAMIČNIH SPLETNIH STRANI

Leta 2007 je Arnes svojim uporabnikom ponudil novo storitev – dinamično gostovanje spletnih strani (Arnes 2011). Storitve se je v tem času precej razvila, prav tako pa se je povečalo število virtualnih strežnikov, ki gostujejo pri nas. Trenutno na Arnesovih strežnikih gostuje 700 organizacij. Vse več organizacij se za virtualne strežnike odloča zato, ker ti omogočajo dinamične spletne predstavitve in administratorjem ponujajo večjo svobodo pri oblikovanju spletnih strani. Izobraževalne ustanove pa se odločajo za virtualna učna okolja, v katerih lahko svojim učencem ponudijo dodatne izobraževalne izzive. Tako statične kot dinamične spletne strani imajo svoje prednosti in omejitve, katere je potrebno pri postavitvi upoštevati.

Pri statičnih spletnih straneh se sama vsebina strani ob obisku ne spreminja. Stran je na strežnik naložena v obliki datoteke, vsak obiskovalec vedno vidi enako vsebino in obliko. Za izdelavo take strani se uporablja html, pri naprednejših straneh, z boljšo oblikovno strukturo, lahko uporabimo html v povezavi s CSS. Ko je stran enkrat objavljena, je potrebno vse spremembe popravljati ročno in jih ponovno prenašati na spletni strežnik, kot da bi popravili dokument, ga shranili in ponovno prenesli v zeleno mapo. Urejanje takih strani zahteva od uporabnika določeno znanje in je časovno zamudno. Statične spletne strani so primerne za predstavitve, kjer ne prihaja do sprememb v zelo kratkem časovnem intervalu. Obiskovalci lahko pridobijo informacije, so le pasivni opazovalci, vsebine ni mogoče dopolnjevati ali komentirati.

Dinamične spletne strani nam ponujajo pri oblikovanju in urejanju spletnih strani veliko večjo svobodo, saj lahko statične spletne strani dopolnimo z blogi, forumi, klepetalnicami, videokonferencami idr. Na Arnesovih strežnikih se organizacije največkrat

odločijo za namestitve LMS- ali CMS-aplikacij, kot so Moodle, Joomla, Drupal ... Po postavitvi spletne strani je mogoče vse podatke dodajati in urejati preko uporabniškega vmesnika na spletni strani. Zaradi dokaj enostavnega dodajanja in urejanja novih vsebin, lahko k sodelovanju pritegnemo veliko število ljudi. Spletna stran je vsebinsko in oblikovno bogata, pogosto se spreminja in dopolnjuje in je zato bolj zanimiva, s čimer si zagotovimo stalne obiskovalce, kar je verjetno cilj vsakega urednika spletne strani.

Izobraževalne organizacije lahko na strežnik namestijo svoje virtualne učilnice in s tem svojim učencem ponudijo dodatna gradiva, atraktivnejše naloge in jim s tem lažje vzbudijo zanimanje za učenje. Tako lahko vsak uporabnik, ki ima pravice, aktivno sodeluje in vsebinsko dopolnjuje spletno stran.

Vsi podatki pri dinamičnih spletnih straneh so shranjeni v bazi in se generirajo vsakič, ko uporabnik zahteva določeno vsebino. Samo delovanje v ozadju je dosti bolj kompleksno, kot pri statičnih spletnih straneh, saj je delovanje spletne strani odvisno tudi od baze. Za delovanje dinamične spletne strani je zato potrebna zmogljivejša strojna oprema. Večje kot je število zahtevkov (obiskovalcev), zmogljivejši strežnik potrebujemo. Z večanjem priljubljenosti spletne strani lahko prihaja do težav, saj postane spletni strežnik počasen pri obdelovanju zahtev ali celo preneha delovati. V primeru nedelovanja dinamičnih spletnih strani, je ugotavljanje razloga za težavo bolj kompleksno. Težava se lahko pojavlja v sami aplikaciji, operacijskem sistemu, servisih, bazi ali strojni opremi. Za opravljanje takšnih težav pa je potrebno dobro tehnično znanje in poznavanje sistema. Na Arnesu sproti vpeljujemo različne mehanizme za optimizacijo delovanja strežnika in baze.

Pri storitvi gostovanja gre za skupek več strežnikov, ki gostujejo na nekaj močnejših fizičnih strežnikih. S tem dosežemo lažje upravljanje s strežniki in tudi boljši izkoristek strojne opreme. Vsakemu virtualnemu strežniku dodelimo del pomnilnika, procesorske moči in diskovnega prostora. V primeru, da pride v določenem trenutku na posameznem virtualnem strežniku do potrebe po večji procesorski moči, se le-ta samodejno prerazporedi iz ostalih virtualnih strežnikov, ki je v tem trenutku ne potrebujejo. Diskovnega prostora smo v začetku dodelili 2 GB vsakemu virtualnemu strežniku, kar se je izkazalo za premalo. Sedaj vsaka organizacija pridobi 10 GB prostora za spletne vsebine, po potrebi pa lahko prostor povečamo na 20 GB.

Gostovanje dinamičnih spletnih strani ponujamo na virtualnih strežnikih z arhitekturo LAMP (Linux, Apache, MySQL in Perl/Python/PHP). Za delovanje dinamičnih spletnih strani skrbijo različni servisi, ki tečejo na sistemu.

V letošnjem letu bomo opravili nadgradnjo operacijskega sistema na CentOS 6, s tem bo omogočeno delovanje novejših aplikacij, kot sta denimo Moodle 2 in Joomla 1.6.

PAKETI GOSTOVANJA

Vse upravičene organizacije lahko izbirajo med tremi paketi gostovanja. Najosnovnejši paket Polni, naprednejši Asistenca in paket Samostojni, kjer pridobite dostop do strežnika z vsemi uporabniškimi pravicami.

Polni paket je primeren za organizacije, ki nimajo časa ali znanja za postavitve dinamične spletne strani. Pridobijo dostop do strežnika, na katerem je že nameščena Joomla in Moodle, ki omogoča spletno učno okolje. Organizacije pridobijo administrativni dostop do aplikacij, vendar so pri tem nekoliko omejene. Lahko dodajajo vsebine in jih urejajo, lahko spreminjajo obliko, ne morejo pa dodajati različnih novih funkcionalnosti v aplikacije. Za vse nadgradnje aplikacij, operacijskega sistema in strojne opreme skrbi Arnes, podpora in izobraževanje pa sta zagotovljena v okviru projekta E-šolstvo.

Asistenca ponuja organizacijam že večjo svobodo pri postavitvi in upravljanju dinamičnih spletnih strani. Organizacije pridobijo dostop do strežnika, kjer aplikacije še niso nameščene, a jih morajo namestiti same. S pomočjo različnih odjemalcev (SCP, SSH, FTP) lahko na strežnik prenesejo spletne vsebine. Za to je potrebno nekoliko več tehničnega znanja, a hkrati je mogoča večja svoboda pri urejanju vsebin in dodajanju novih funkcionalnosti. Organizacija mora poskrbeti za vse varnostne popravke spletnih aplikacij. V primeru težav v spletni aplikaciji, mora za odpravo napake organizacija poskrbeti sama, lahko se za pomoč obrne tudi na svetovalce iz projekta E-šolstvo. Arnes pri tem paketu skrbi za posodabljanje in vzdrževanje operacijskega sistema in strojno opremo.

Pri paketu Samostojni organizacije pridobijo dostop do strežnika z vsemi uporabniškimi pravicami. Na strežnikih je nameščen operacijski sistem CentOS. Za upravljanje takega strežnika je potrebno dobro poznavanje Linux sistema, saj Arnes v tem primeru ne zagotavlja nobene podpore. Za vse posodobitve operacijskega sistema, nameščanje modulov in posodobitev ter varnostne popravke, mora organizacija poskrbeti sama.

NOVOSTI V LETU 2011

V letu 2011 bo Arnes poleg že omenjene nadgradnje operacijskega sistema na CentOS 6, poskrbel tudi za druge novosti.

IPv4 naslovov vztrajno zmanjkuje. Arnes se na prehod iz IPv4 na IPv6 že pospešeno pripravlja. Tako smo v začetku letošnjega leta na vseh virtualnih strežnikih omogočili IPv6 naslove. Vsi obiskovalci, ki do spleta dostopajo preko IPv6 naslova, bodo lahko s strežnikom komunicirali neposredno preko IPv6 protokola.

Pri obisku spletne strani preko protokola HTTP se podatki med obiskovalcem in spletno stranjo prenašajo nešifrirano. Posledično lahko nekdo podatke prestreže in s tem pridobi občutljive informacije, kot je uporabniško ime in geslo. To pomanjkljivost rešuje protokol HTTPS, ki je kombinacija HTTP protokola in šifriranja SSL/TLS. Pri dostopu do spletne strani preko tega protokola, pride do šifriranega prenosa podatkov. V primeru da nekdo prestreže podatke, iz njih ni možno pridobiti nobenih uporabnih informacij. Do letošnjega leta je bila uporaba protokola HTTPS možna na paketih Samostojni in Polni, letos pa je to možno tudi na paketu Asistenca.

Pri naraščanju števila virtualnih strežnikov, se povečujejo tudi administrativni zahtevki in posledično odzivni čas reševanja teh zahtevkov. V letošnjem letu bo na voljo spletni grafični vmesnik, preko katerega bodo uporabniki lahko preverjali, v kakšnem

stanju je njihov virtualni strežnik. Poleg osnovnih informacij o porabi prostora in pomnilnika, bodo uporabniki lahko izvajali določene nastavitve na strežniku: možno bo dodajati poddomene, ponovno zagnati določene servise ali samo prebrati dnevniške datoteke. S tem za določene operacije ne bo več potrebno pošiljati zahtevkov na Arnes, ampak bo lahko vsak skrbnik strežnika samostojno opravil zelene spremembe.

Zaradi same strukture virtualnih strežnikov vseh želja, ki jih imajo naši uporabniki, ne moremo uresničiti, vendar se ves čas trudimo da bi bila storitev boljša in uporabniki zadovoljni. Pri vsem tem bi si želeli večji odziv na vse spremembe, ki jih uvedemo. Tako pozitivna kot negativna kritika je vedno dobrodošla, saj nas usmerja k nadaljnji širitvi storitve.

VIRI

Arnes. 2011. Dinamično gostovanje (PHP/MySQL).

[Http://www.arnes.si/storitve/splet-posta-strezniki/gostovanje-spletnih-strani/dinamicno-gostovanje-phpmysql.html](http://www.arnes.si/storitve/splet-posta-strezniki/gostovanje-spletnih-strani/dinamicno-gostovanje-phpmysql.html) (16. 2. 2011).

NOVOSTI S PODROČJA VEČPREDSTAVNOSTI NA ARNESU MULTIMEDIA INNOVATIONS AT ARNES

MATJAŽ BATIČ
FINŽGAR, ARNES

POVZETEK

Večpredstavne vsebine postajajo glavna internetnega prometa. Za njihovo shranjevanje zato potrebujete hiter in zanesljiv strežnik, na katerem se po možnosti lahko nastavi tudi to, kdo si lahko posnetek ogleda. Spletni portal Arnes video vam omogoča shranjevanje in predvajanje vaših posnetkov na spletu, samodejno konverzijo v ustrežni format in vnos metapodatkov v obliki, prilagojeni svetovnim iskalnikom gradiv. Hkrati boste lahko na novi strežnik prenesli tudi posnetke svojih H.323-konferenc. In kar je najpomembnejše, za vsak posnetek boste lahko določili, kateri posameznik ali skupina si ga lahko ogleda. Spletne konference VOX so v preteklem letu doživele oblikovno in funkcionalno nadgradnjo. Poleg novih funkcionalnosti, kot je na primer uporaba konferenc na pametnih telefonih in prenovljeni spletni vmesnik, vam bomo predstavili tudi možnosti video urejanja vaših posnetkov prek spletnega vmesnika.

KLJUČNE BESEDE: VIDEO PORTAL, FLASH PRETOČNI VIDEO, H.323 VIDEOKONFERENCE, SPLETNE KONFERENCE VOX

UVOD

S pojavom pametnih telefonov se del življenja modernega človeka seli na internet. Na internetu pa je video nesporni vladar. Zato se tudi na Arnesu vsako leto trdimo uporabnikom ponuditi nove storitve s področja večpredstavnosti.

OSREDNJI DEL

Letos bomo uporabnikom ponudili nov video portal. Gre za spletno stran, ki združuje vse Arnesove multimedijske storitve, pretočni video na zahtevo, posnetke videokonferenc in spletnih konferenc, v prihodnosti pa bo portal omogočal tudi video prenose v živo. Na portalu bodo lahko profesorji in učitelji shranjevali posnetke, 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, pripravi se slika s povzetkom videa, uporabnik pa lahko vnese opis videa v obliki, ki je prilagojena svetovnim iskalnikom gradiv. Prijava v video portal bo mogoča preko federacije ArnesAAI, zato bodo lahko profesorji dostop do svojih posnetkov omejili na izbrane posameznike ali skupine.

Konec leta 2010 so korenito prenavo doživele tudi spletne konference VOX. Ogrodje spletnih videokonferenc po novem podpira Action script 3, zaradi česar je grafični vmesnik hitrejši in odzivnejši. Izboljšali smo tudi kvaliteto videa v orodju kamera ter omogočili

ABSTRACT

Multimedia content increasingly accounts for the bulk of Internet traffic. Storing it requires a fast and reliable server on which you can also control who can view the content. The ARNES video web portal enables you to store and play your recordings on the web, and enables automatic conversion to the appropriate format and the input of metadata in a form adapted to global search engines. You will also be able to transfer recordings of your H.323 conferences to the new server. Most importantly, for each recording you will be able to determine which individuals or groups can view the content. VOX web conferences have had design and functional upgrades last year. As well as new functionality, such as the use of conferences on smartphones and an updated web interface, we will also present the possibility of editing your videos via a web interface.

KEY WORDS: VIDEO PORTAL, FLASH VIDEO STREAMING, H.323 VIDEOCONFERENCES, VOX WEB CONFERENCES

enosmerno vključitev H.323 videokonferenc na Arnesovem strežniku MCU s spletnimi konferencami. S tem smo vsem uporabnikom H.323 videokonferenc omogočili kvaliteto prenašanje videokonferenc preko spleta v flash tehnologiji. Poleg naštetih posodobitev prenovljen spletni vmesnik omogoča tudi uporabo barv in stilov v orodjih za skupinsko delo in klepet.

ZAKLJUČEK

Video portal bo združil svet videokonferenc in video prenosov v živo s flash pretočnim videom, ki omogoča, da so video vsebine dostopne na osebnih računalnikih in pametnih telefonih. Prenovljene spletne konference VOX pa so zaenkrat enosmerno združile svet H.323 videokonferenc visoke ločljivosti s spletnimi videokonferencami VOX.

OKOLJE ZA KONSTRUKTIVISTIČNO SODELOVALNO UČENJE Z RABO INFRASTRUKTURE V OBLAKU ENVIRONMENT FOR CONSTRUCTIVIST COLLABORATIVE LEARNING USING INFRASTRUCTURE IN A CLOUD

ANDREJ BRODNIK,
MOJCA CIGLARIČ,
ANDREJ KREVI,
UNIVERZA
V LJUBLJANI,
FAKULTETA ZA
RAČUNALNIŠTVO
IN INFORMATIKO,

JOŽE RUGELJ,
UNIVERZA
V LJUBLJANI,
PEDAGOŠKA
FAKULTETA

POVZETEK

V prispevku je najprej predstavljen razvoj spletnega učnega okolja za konstruktivistično učenje v visokem šolstvu s poudarkom na poučevanju vsebin iz inženirstva in naravoslovja (engineering and science). Avtorji okolja so pri svojem delu upoštevali najnovejše ugotovitve pedagoškega raziskovanja in razpoložljivost novih tehnologij, da bi ustvarili uspešno in učinkovito okolje za učenje. Učna tehnologija oz. navidezni laboratorij je izvedena v obliki spletne storitve. Celo več, navidezni laboratorij postane infrastruktura uporabna v oblaku – IaaS. V nadaljevanju predstavimo svoje izkušnje pri uporabi okolja v prvem letu praktične uporabe s približno 700 študenti v študiju računalništva in informatike.

Predstavitev vključuje tehnične značilnosti (npr. kako obremenjen je bil sistem) kot tudi vsebinske značilnosti. V zaključku podajamo praktičen primer rabe navideznega laboratorija od priprave laboratorijske vaje, rezervacije laboratorija s strani študenta do izvedbe naloge v laboratoriju in njenega ocenjevanje.

KLJUČNE BESEDE: KONSTRUKTIVISTIČNO
UČENJE, VIRTUALNI LABORATORIJ, IAAS, UČENJE
RAČUNALNIŠTVA IN INFORMATIKE.

UVOD

V zadnjem desetletju se je tako v Sloveniji kot v številnih drugih evropskih državah prišlo do velikih sprememb v visokošolskem izobraževanju. Skoraj 80% mladostnikov starih od 18 do 23 let je vpisanih v visokošolske študijske programe. Po drugi strani pa količina denarja v državnem proračunu namenjenega visokemu šolstvu in posledično število pedagoških delavcev in vseh ostalih virov ni sledila tej rasti števila študentov, kar je ogrozilo tako učinkovitost kot tudi kakovost izobraževanja.

Odgovorni v večini visokošolskih ustanov so tako prišli do zaključka, da lahko s pomočjo uporabe informacijsko komunikacijske tehnologije (IKT) pri učenju in poučevanju, kar navadno imenujemo *e-učenje*, vsaj delno pripomore k rešitvi omenjenih problemov. E-učenje je za naš namen definirano kot uporaba vsakršnih novih tehnologij ali aplikacij za potrebe učenja ali podpore učencu. To je pomembno, ker lahko e-učenje bistveno vpliva na način učenja učencev, hitrost osvajanja veščin, preprostost učenja in na užitek pri učenju (Laurillard, 2005). Tako kompleksen sklop tehnologij bo imel kulturno, intelektualno, socialno in praktično vplival na izkušnjo učenja.

ABSTRACT

The paper presents a development of web-based learning environment for constructivist learning in higher education with an emphasis on learning process in science and engineering. In the development of successful and efficient learning environment were used novel ideas and paradigms of didactics and ICT. The learning environment includes a virtual laboratory, which is defined as a service. Indeed, the virtual laboratory becomes an infrastructure that can be used in a cloud – IaaS. The paper also presents our experience with the environment used in classes attended by over 700 students of Computer Science.

The presentation will include technical details of the environment (e.g. system load) as well as brief description of its use. The later will include complete development cycle of an assignment in the virtual laboratory.

KEY WORDS: CONSTRUCTIVISTIC LEARNING,
VIRTUAL LABORATORY, IAAS, LEARNING
OF COMPUTER SCIENCE.

K temu moramo prišteti še finančne posledice. Omrežja in dostop do spletnih virov ponuja alternativo prostorsko in časovno določenemu učenju, kar zmanjša potrebo po dragih prostorih in stroške dostopa do oddaljenih virov. Kljub vsemu pa učenci še vedno potrebujejo podporo ljudi, kar pomeni, da so pričakovane finančne koristi na račun stroškov naložb v nov sistem in stroškov učenja uporabe navadno precenjene. Iz teh razlogov Lauriard trdi, da znižanje stroškov ni zadosten argument za vpeljavo e-učenja. Tako se je bolje zavzemati za vlaganje v izboljšanje kakovosti kot pa za zmanjšanje stroškov.

Drugi razlog za povečanje zanimanja za e-učenje je usmerjen v skrb, da lokalni visokošolski zavodi ne morejo imeti monopola nad izvajanjem izobraževanja (Alexander, 2001). Konkurenca naj bi domnevno izvirala iz mednarodnih institucij visokega šolstva.

IKT in e-učenje sama ne moreta rešiti vseh omenjenih težav. Novi pristopi k učenju morajo vključevati prednosti osebnega stika in spletnega učenja na sinergijski način, in s tem ustvariti edinstveno učno izkušnjo skladno s kontekstom in namenom izobraževanja (Garrison, 2008). Ti pristopi se imenujejo mešano učenje (*blended learning*).

ZASNOVA

Znotraj učnega okolja, ki ga podpira LMS, smo uporabili pristop mešanega učenja, saj smo želeli ohraniti koristi osebnega stika in razredne interakcije pri poučevanju kot tudi koristi uporabe virtualnega učnega okolja (Lapuh Bele, 2007). Pri računalniških predmetih smo uporabili inovativne učne aktivnosti, ki temeljijo na konstruktivizmu (Nančovska Šerbec, 2009; Ben-Ari, 2001), in ki so bile oblikovane kot pilotni predmeti, saj večino udeležencev v projektu predstavljajo računalniški strokovnjaki.

Konstruktivizem je teorija učenja, ki trdi, da študenti sami konstruirajo svoje znanje in ne morejo zgolj prejeti in shranjevati znanja, ki jim ga posreduje učitelj. Po konstruktivistični učni teoriji morajo učenci znanje ponotranjiti (Learning Theories, 2009). V različnih fazah učnega procesa uporabljamo različne aktivne oblike pedagoškega dela, da bi spodbudili študente k personalizaciji znanja (Nančovska Šerbec, 2009). Ti lahko prilagodijo globino svojega učenja glede na svoje potrebe in zmožnosti zaradi odprte definicije nalog.

Pripravili smo tudi možnosti za vključitev študentov v aktivne oblike učenja preko novih oblik ocenjevanja, kot je na primer medsebojno ocenjevanje. Očitno je, da bodo aktivne oblike učenja in ocenjevanja vplivale na kakovost učenja v našem učnem okolju. Izobraževalno ocenjevanje je postopek ocenjevanja in dokumentiranja znanja, spretnosti, stališč in prepričanj. Spretnosti in sposobnosti za ocenjevanje so zelo zaželeno v visokem šolstvu (Assessment in Higher Education, 2009; Nančovska Šerbec, 2009).

Študent potrebuje priložnosti za formativno preverjanje in pridobivanje povratnih informacij za razvoj spretnosti in konceptov. Ker običajno ni dovolj priložnosti, da jih dobijo od zaposlenih, oblike sodelovalnega učenja zagotavljajo možnosti za dodatne povratne informacije. Medvrstniška ocena je proces, v katerem študenti izrazijo mnenje, in določijo stopnjo, vrednost ali kakovost izdelka ali nastopa drugih oseb v podobnem položaju, ki se navadno izvede med študenti v določenem razredu.

To predstavlja tudi pristop pri usposabljanju študentov, za zagotavljanje dragocenih povratnih informacij in predlogov za izboljšanje učinkovitosti. Sluijsmans (Sluijsmans, 1999) je opredelil številne prednosti pri medvrstniškem ocenjevanju. Nekaj najbolj pomembnih je, da lahko motivirajo študente, ter spodbujajo njihovo aktivno sodelovanje pri učenju, spodbujajo študente, da postanejo bolj samostojni pri učenju, signalizirajo študentom, da se njihove izkušnje vrednotijo in mnenja spoštujejo, in da študenti bolj poglobljeno razmišljajo o drugih rešitvah problemov, zbirajo točke in se naučijo konstruktivno kritizirati. Učitelji imajo pogosto težave pri vključevanju vrednotenja študentov v skupne dejavnosti. Težava ni le pri ocenjevanju ravni učenja, ki jih producira sam proces, temveč tudi pri določanju dejanske stopnje, do katere je posameznik dejavno sodeloval in prispeval k skupnemu delu.

Drug pomemben vidik učinkovitega učenja je socialna razsežnost učenja. Socialni konstruktivizem poudarja, kako pomen in razumevanje raste v medsebojnih interakcijah. Poudarek je na študentu kot aktivnem ustvarjalcu pomenov. Učitelj in vrstniki začnejo dialog s študentom, poskušajo razumeti pomen vsebine, ki se jo mora vsak posamezen študent naučiti, in pomagajo študentu, da izboljša svoje razumevanje.

Za tradicionalna izobraževalna okolja so pogosto značilni procesi, v katerih učitelj dodeli učne dejavnosti, ki jih običajno študent izvaja samostojno. Vendar s tem učni proces izgubi socialne razsežnosti. Tako ideja o spodbujanju sodelovalnega učenja kot situaciji, v kateri se dve ali več oseb skupaj uči ali poskuša nekaj skupaj naučiti, predstavlja sredstvo za krepitev te dimenzije z ustvarjanjem pogojev za posameznikov kognitivni razvoj, ki je posledica interakcije v skupini (Hansen, 1998).

V primeru sodelovalnega učenja, podprtega s storitvami računalniških omrežij, te strategije običajno izvajamo z dodeljevanjem nalog skupinam študentov, ki potem skupaj iščejo rešitev dane naloge (sodelovalno reševanje problemov) ali skupaj pišejo sestavek (skupinsko pisanje) na zastavljeno temo. Te strategije vključujejo različna orodja za komunikacije in sodelovanje, ki omogočajo učencem, da aktivno sodelujejo pri gradnji znanja ter izboljšujejo procese sodelovalnega pisanja in omogočajo njihovo spremljanje.

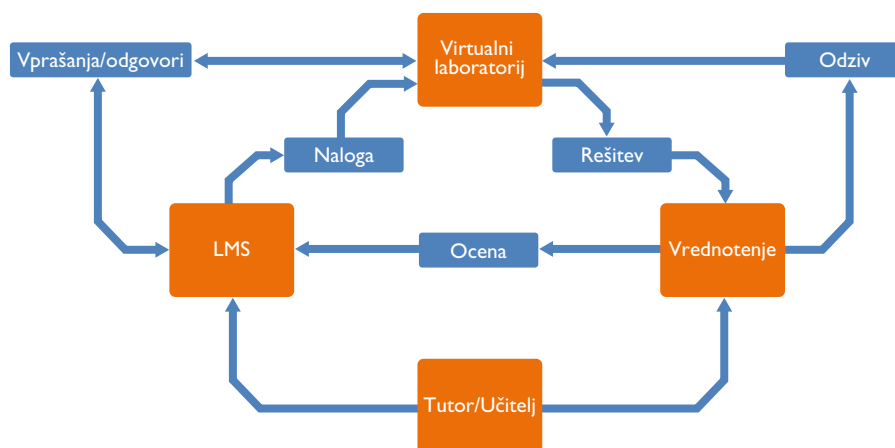
VIRTUALNI LABORATORIJ

Poseben izziv je implementacija zgoraj omenjenih konceptov v IKT podprtih učnih okoljih. Večina trenutno dostopnih z IKT podprtih učnih okolij je le zbirka bolj ali manj tradicionalnih učnih gradiv. Samo nekatera od njih so bila narejena na novo, večinoma pa so le digitalizirani učbeniki in druga učna gradiva. Študenti naj bi brali besedila, ki so v nekaterih primerih obogatena z ilustracijami ali z nekaj animacijami in video posnetki. Večina od njih pa temelji na tradicionalnem pristopu poučevanja z začetno razlago in z nekaj vajami v različnih oblikah po tem. Samo nekateri primeri vključujejo različne multimedijske motivacijske elemente.

Zato smo se odločili, da najprej opredelimo arhitekturo, ki bo omogočala souporabo različnih orodij in učnih okolij. To predstavlja inovativen pristop s konstruktivistično teorijo učenja v izhodišču.

Slika 1 prikazuje strukturo učnega okolja, ki je bil razvit v okviru projekta SAKE. Temelji na aktivnem učenju. Študenti so aktivni v problemsko naravnanih učenih aktivnostih. Zelo pomembno je, da opredelimo ustrezne probleme, ki niso preveč preprosti, da bi se študenti ob njih dolgočasili, in ne preveč zahtevni, da študenti ob njih ne bi obupali. Vygotsky ta koncept opredelil kot območje proksimalnega razvoja (zone of proximal development), ki je razlika med tem, kar lahko študent stori brez pomoči in tistim, kar lahko stori s pomočjo učitelja. Vygotsky je ugotovil, da študent sledi reševanju primerov in ob tem postopoma razvija sposobnost za izvajanje nekaterih nalog brez pomoči. Vloga izobraževanja je, da študentom ponudijo take »učne probleme«, ki so v coni proksimalnem razvoja in na ta način spodbuja in pospešuje njihovo individualno učenje.

Slika 1:
ARHITEKTURA
RABE
VIRTUALNEGA
LABORATORIJA.



V naši arhitekturi so problemi zastavljeni v standardnem učnem sistemu za upravljanje z učenjem - LMS (npr. Moodle). Po seznanitvi s problemom študente usmerimo v virtualni laboratorij, kjer lahko najdejo osnovno »raziskovalno infrastrukturo« z mnogimi orodji, potrebnimi za rešitev problema. Lahko se posvetuje tudi s *tutorjem*, ki nadzoruje dejavnosti v virtualni učilnici, in lahko da različne nasvete in priporočila.

Glavne naloge tutorja so: oblikovanje učnega načrta, ki določa časovni okvir, zahteve in aktivnosti pri učnem predmetu; oblikovanje kodeksa ravnanja pri predmetu; objavljane učnih ciljev in pričakovanj; spremljanje dela učencev in njihovega napredka; pomoč učencem, da skupaj napredujejo po pravi poti; spodbujanje komunikacije med udeleženci pri predmetu; aktivno sodelovanje, spodbujanje in vodenje interaktivnih razprav; priprava odgovorov na vprašanja, povratnih informacij in priporočil o poteku dejavnosti; ovrednotenje in analiza dela učencev.

Pomembna funkcija našega sistema je ocenjevanje. Izvedli smo funkcionalnosti, ki lahko podpirajo oba načina ocenjevanja, tako formativno ocenjevanje, ki daje študentu takojšnje povratne informacije in jih usmerja pri nadaljnjih učnih aktivnostih, kot tudi sumativno ocenjevanje ob koncu učne dejavnosti za merjenje doseganja učnih ciljev in za ugotavljanje končnih rezultatov učenja (Lapuh Bele, 2007).

Ker ni stalne prisotnosti tutorja in naj bi študenti številne dejavnosti izvajali sami, so povratne informacije v obliki formativne ocene njihovih dejavnosti ključnega pomena. Formativno in sumativno ocenjevanje je mogoče avtomatizirati in jih imple-

mentirati kot ekspertni sistem, ki je del posebne funkcionalnosti virtualnega laboratorija ali pa ga je mogoče zagotoviti s »človeškimi mentorji«. Očitno je, da rezultate formativnega ocenjevanja predstavimo študentov v virtualnem laboratoriju, medtem ko je rezultate sumativnega ocenjevanja treba poslati v LMS.

Omenili smo pomen socialnega vidika učenja in njegov pomen v konstruktivističnem učnem pristopu. V naši arhitekturi je vsaj del dejavnosti opredeljenih na tak način, da spodbujajo vzajemno učenje (angl. peer learning). Vzajemno učenje je oblika sodelovalnega učenja, ki poveča vrednost interakcije študent-študent in daje kot rezultat na različnih ugodnih rezultatov učenja. Za uresničitev prednosti vzajemnega učenja mora učitelj zagotoviti ustrezno »podporo«. Učno okolje mora podpirati sodelovalne dejavnosti s podporo komunikaciji in s pomočjo skupne rabe učnih virov. Zaradi tega smo razširili običajne forume v LMSjih z vključitvijo sodobnih družabnih omrežij, kot so Twitter, Facebook, itd.

Samo vzdrževanje fizičnih laboratorijev oziroma računalniških učilnic za praktične vaje zahteva veliko časa za namestitve in vzdrževanje, ni fleksibilno, težko sledi zahtevam za nove namestitve in posodobitve programske opreme, varnost je problematična, pogoste so težave zaradi okvar na strojni opremi, dostop v prostor in čas uporabe pa sta omejena z urnikom. Dodatne težave nastopijo pri predmetih, kjer učna vsebina zahteva, da ima učeči upravljalne pravice na učnem računalniku, saj se rado zgodi, da po nesreči spremeni nastavitve tako, da računalnik ni več ustrezno konfiguriran za naslednje uporabnike. Virtualizacija ponuja možno rešitev vseh teh izzivov, saj omogoča oddaljen dostop do virov brez omejitev časa in fizične prisotnosti (premik v prostoru in času), poenoteno vzdrževanje je bistveno lažje, okolje pa je nadzorovano, dosegljiv je višji varnostni nivo, lažje pa je tudi upravljanje z licencami programske opreme.

Naša definicija virtualnega laboratorija predpostavlja, da imamo dovolj zmogljivo strežniško infrastrukturo, na kateri poganjamo navidezne računalnike, ki jih potrebujejo učeči. Takšno infrastrukturo imenujemo tudi centralizirana virtualizacija – virtualni laboratorij je dejansko infrastruktura, ki se jo uporablja kot storitev. Govorimo lahko tudi o infrastrukturi kot storitvi v oblaku (*IaaS cloud*).

Z vidika uporabnika je sistem preprost za uporabo. V spletni učilnici izbere ustrezno povezavo, ki ga pripelje v rezervacijski sistem virtualnega laboratorija. Tu si izbere željeno vajo iz seznama vseh možnih vaj in izbere termin opravljanja vaje – če infrastruktura še ni popolnoma zasedena, lahko tudi takoj vstopi v vajo.

Vstop v vajo pomeni oddaljeni dostop do navideznega računalnika (ali večih računalnikov), ki se je medtem zagnal na virtualni infrastrukturi. V zelo kratkem času se požene sveža slika operacijskega sistema, ki ga je učitelj določil za izbrano vajo, in v sistem je nameščena ustrezna programska oprema, ki je potrebna za izvajanje vaje. Učenec nato po navodilih izvaja laboratorijsko vajo na navideznem računalniku na popolnoma enak način, kot če bi sedel v računalniški učilnici pred fizičnim računalnikom.

IZKUŠNJE PRI UPORABI

V poletnem semestru 2010 je FRI-jev virtualni laboratorij v okviru predmeta Računalniške komunikacije uporabljalo več kot 300 študentov. Tehnično je sistem deloval brez kakih izrazitih težav. Študentom smo ob začetku semestra in po zadnjem poletnem izpitnem roku v izpolnjevanje ponudili dve anketi.

Prvo anketo je izpolnilo 349 študentov, 307 fantov in 42 deklet, vpisanih v univerzitetni (164) in strokovni (185) program računalništva in informatike. 72% študentov je kot študijsko literaturo uporabljalo zapiske, ki so jih študentje pisali v wiki strani na spletni učilnici. Večina študentov (85,7%) se učijo sami, le 17% se jih pogosto uči skupaj s prijatelji, 49% pa to počne le občasno. Vidimo, da študentom manjka sodelovalnih spretnosti in jih je k sodelovanju potrebno močno motivirati. Pragtako le redko poiščejo dodatne razlage na spletu: le 52% jih občasno poišče kako literaturo na spletu, medtem ko 3% sploh nikoli ne počnejo tega. Sklepamo lahko, da študenti niso vajeni prevzemati aktivne vloge pri učenju in da še nimajo izkušenj s konstruktivističnim učenjem. Zato bo potrebno pri nadaljnji izvedbi predmeta več pozornosti posvetiti privajanju na sodobne oblike učenja.

Študenti so lahko svoja vprašanja pošiljali učiteljem ali asistentom po elektronski pošti ali pa prek forumov na fakultetni spletni učilnici in večinoma so dobili odgovor v enem dnevu, pogosto že v uri ali dveh. Kljub temu se kar 21% študentov strinja ali močno strinja s trditvijo, da bi postavili več vprašanj, če bi jih lahko postavljali na Facebooku, 26% na Skypu in 9% na Twitterju. Za učitelja so ti odgovori močan opomin, da si ne more privoščiti ignoriranja sodobnih tehnologij in sredsev komuniciranja, temveč naj jih raje vključi v svoj način poučevanja.

V virtualnem laboratoriju bilo prijavljenih 317 študentov. Za izpolnitev svojih obveznosti so morali v virtualnem laboratoriju izvesti dve nalogi, eno z eno rezervacijo in eno s tremi rezervacijami. Ocena trajanja naloge je 60 minut, vendar pa so lahko študenti rezervacijo podaljšali na največ 2 uri. Dejansko trajanje rezervacij lahko vidimo v Tabeli 1. Rezervacije, krajše od 25 minut, lahko v veliki večini označimo kot poskus in preiskovanje terena pred zaresnim reševanjem naloge.

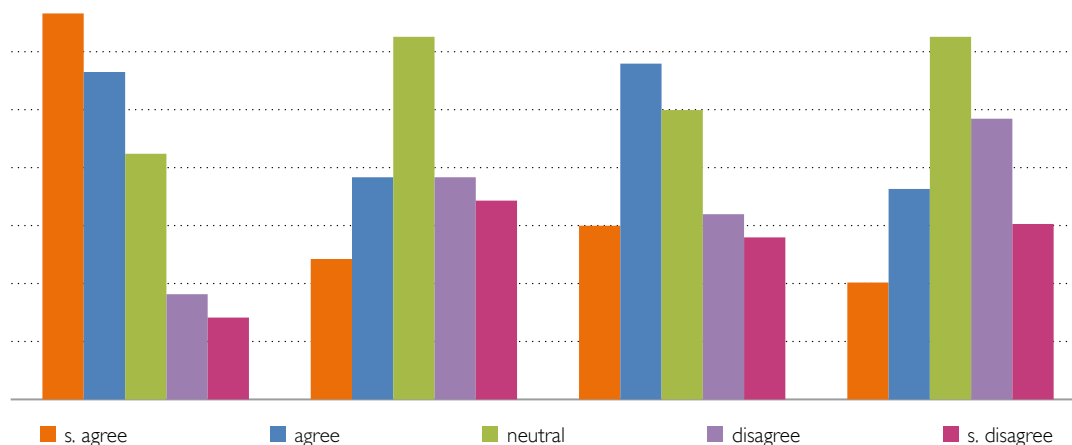
Ostale pa predstavljajo bolj ali manj spretno reševanje zadanih nalog. Glede na predstavljena števila je časovni okvir vaje primerno zasnovan.

Tabela 1:
PREGLED
TRAJANJA
REZERVACIJ.

Trajanje	Število rezervacij
0 minut	249
1-25 minut	627
26-50 minut	654
51-75 minut	1130
76-100 minut	131
101-125 minut	49

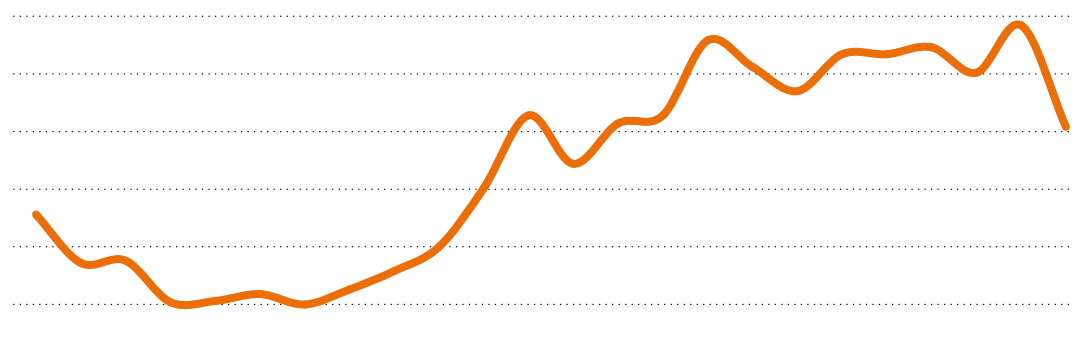
Slika 2 prikazuje mnenja študentov o sami izvedbi predmeta. Študenti so morali oceniti štiri trditve: da jim je bila izvedba predmeta všeč, da jim je klasična izvedba bolj všeč, da je novi način težji kot klasični in da so se po novem naučili več kot po klasičnem načinu. Možni odgovori so bili povsod enaki: lahko so se strinjali ali močno strinjali, lahko so bili nevtralni, lahko so izrazili nestrinjanje ali močno nestrinjanje.

Slika 2
PREGLED MNENJ
ŠTUDENTOV O
SAMI IZVEDBI
PREDMETA.



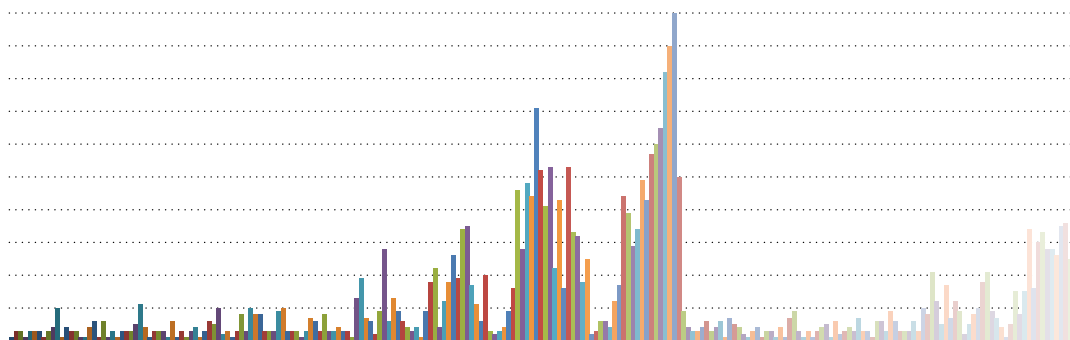
Slika 3 pa prikazuje ure v dnevu glede na to, kako so bile priljubljene pri študentih. Prikazano je skupno število rezervacij v vsem opazovanem obdobju v določeni uri dneva. Vidimo, da so daleč najboljši termini od 15. Ure pa nekje do polnoči, do 3 ure zjutraj aktivnost skoraj popolnoma upade, 6-7h je edina ura, ko v celotnem obdobju ni bilo niti ene rezervacije, dopoldan pa število počasi narašča do vročega termina 15. ure. Dopoldanske ure, ki so za pedagoški proces najbolj priljubljene pri učiteljih, študentom sploh ne ustrezajo in tudi na tem mestu smo z uvedbo virtualnega laboratorija izpolnili dve zahtevi. Učitelji namreč lahko odgovarjajo na študentska vprašanja dopoldan, študentje pa lahko virtualni laboratorij preizkušajo tudi sredi noči, če to želijo. Fizična prisotnost ob istem času in na istem kraju ni več potrebna.

Slika 3:
SKUPNO ŠTEVILO
REZERVACIJ V
VIRTUALNEM
LABORATORIJU
GLEDE NA URO
DNEVA: ŠTUDENTI
IMAJO RADI
VEČERE!



Slika 4 prikazuje časovno dinamiko uporabe virtualnega laboratorija po dnevih. Po dveh tednih je bil rok za večino študentov, manjša skupina pa je imela rok podaljšan še za en tede. Vidimo lahko, da je obakrat največja obremenitev sistema ravno tik pred rokom za oddajo.

Slika 4:
SKUPNO ŠTEVILO
REZERVACIJ
V VIRTUALNEM
LABORATORIJU
NA POSAMEZNI
DAN: ŠTUDENTI
DELAJO TIK PRED
ROKOM!



Kvalitativni odziv študentov na izvedbo predmeta je bil mešan. Prevladuje občutje, da so bile naloge težke in da jih novi pristopi k učenju zmedejo. Po končanem izpitnem obdobju je sicer odziv rahlo bolj pozitiven. 62% študentov se strinja (28%) ali močno strinja (34%) s trditvijo, da jim je bila izvedba predmeta všeč. Obenem jih 31% meni, da je klasični način izvajanja predmeta vendarle boljši, medtem ko se jih 37% s tem ne strinja (ostalih 31% je zavzelo nevtrarno stališče). 44% študentov meni, da je novi način težji in dolgotrajnejši, 30% pa se jih s tem ne strinja. Zanimivo je, da se večina študentov ni opredelila za klasični način poučevanja, kljub temu da v povprečju ne mislijo, da so se v virtualnem laboratoriju naučili več kot bi se v klasičnem. 29% študentov misli, da so se naučili več, 39% pa misli, da se niso naučili nič več kot na klasičen način. Čeprav so ti rezultati na prvi pogled videti protislovni, verjamemo da odpor do novih načinov deloma izvira iz privajanja na aktivno vlogo v življenju in učenju.

V prvih izpitnih rokih smo na vseh izpitih študentom zastavili eno nalogo iz ožjega področja vsebine, ki so jo študenti obravnavali na vajah v virtualnem laboratoriju. Pričakovali smo, da bo analiza pokazala, da imajo študenti, ki so opravljali virtualni laboratorij, več točk iz teh vsebin kot študentje, ki niso delali virtualnem laboratoriju. Na izpitih pa se je pokazalo, da so povprečne ocene obeh skupin popolnoma enake. Ob kasnejšem iskanju razlage tega dejstva smo prišli do ugotovitve, da se na drugačen način pridobljeno znanje tudi kaže na drugačen način. Vsebinske vtisne za dalj časa, ostane pa tudi v obliki iznajdljivosti in spretnosti pri reševanju problemov in ne toliko v obliki memoriranja nekih dejstev. Klasični izpiti za ocenjevanje deklarativnega znanja so tako manj primerni, zato bomo morali v prihodnosti več pozornosti posvetiti tudi novim načinom preverjanja in ocenjevanja znanja, saj je pridobljeno znanje drugače strukturirano in drugače zapomnjeno.

ZAKLJUČEK

V članku je predstavljena spletna arhitektura, ki podpira konstruktivistično sodelovalno učno okolje s posebnim poudarkom učenja naravoslovnih in inženirskih disciplin. Arhitektura sestoji iz osrednjega iz večih gradnikov kot so LMS, družabna omrežja in predvsem virtualni laboratorij. Slednjega uporabljamo kot infrastrukturo in je implementiran kot storitev – IaaS.

Laboratorij vključuje orodja za ocenjevanje učenčevega dela, ki je lahko formativno ali sumativno. Poleg tega je v laboratoriju predvidena neprestana prisotnost tutorja, ki ni nujno samo v človeški obliki.

Nadaljnje delo na arhitekturi gre v treh smereh. Najprej je potrebno v laboratorij še bolje vtakati vlogo tutorja ter vse skupaj tesneje povezati z LMS in drugimi gradniki sistema. Naslednja smer razvoja je dodelava laboratorija za druge učne vsebine. Na koncu a ne nazadnje je širša raba infrastrukture. Nekaj izkušenj je že tudi na tem področju, saj ga uporabljamo pri izvedbi krožkov računalništva in informatike po srednjih šolah.

VIRI

Alexander, S. (2001): E-learning developments and experiences, *Education + Training*, 43 (4/5), 240 - 248

Assessment in Higher Education, <http://ahe.cqu.edu.au/> (17. 5. 2009).

Ben-Ari, M. (2001): Constructivism in Computer Science Education. *Jl. of Computers in Mathematics and Science Teaching*, 20 (1), 45-73.

Garrison, D.R., Vaughan, N.D. (2008): *Blended Learning in Higher Education*, San Francisco, Jossey-Bass.

Hansen, T., Dirckinck-Holmfeld, L., Lewis, R. and Rugelj, J. (1998): Using telematics for collaborative knowledge construction, in Dillenbourg, P. (ed.): *Collaborative Learning: Cognitive and Computational Approaches*, Pergamon - Elsevier Science.

Lapuh Bele, J.; Rugelj, J. (2007): Blended learning - an opportunity to take the best of both worlds, *Int. j.: emerg. technol. learn.*, 2 (3), 71-75.

Lapuh Bele, J., Rugelj, J. (2007): Providing feedback in web-based learning. V: AUER, Michael E. (ur.). 10th International Conference, ICL 2007. ePortfolio and quality in e-learning. Wien: International Association of Online Engineering.

Laurillard, D. (2005): E-Learning in Higher Education, in *Changing Higher Education: The Development of Learning and Teaching*, Paul Ashwin (ed), RoutledgeFalmer.

Learning Theories. Wikibooks, http://en.wikibooks.org/wiki/Learning_Theories (14. 5. 2009)

Nančovska Šerbec, I., Strnad, M., Rugelj, J. (2009): Active learning in computer science courses in higher education. V: KINSHUK (ur.). *Proceedings of the IADIS international conference on Cognition and exploratory learning in digital age (CELDA 2009)*. Roma: International Association for Development of the Information Society, IADIS, 538-540.

Nančovska Šerbec, I., Strnad, M., Rugelj, J. (2009): Assessment of active forms of learning in the higher education. In: AUER, Michael E. (ed.). *ICL2009. The Challenges of Life Long Learning*. Wien: International Association of Online Engineering; Kassel: University Press, 489-496.

Nančovska Šerbec, I., Strnad, M., Rugelj, J. (2009): Students' attitude to active forms of e-learning, In: M. Činčin-Šain, (ed.). *Proceedings Rijeka: MIPRO*, 100-103.

Sluijsmans, D., Dochy, F., & Moerkerke, G. (1999): Creating a learning environment by using self-, peer- and co-assessment. *Learning Environments Research* 1, 293-319.

SHRANJEVANJE PODATKOV IN OZNAČEVANJE "SPAMA" STORAGE AND MARKING SPAM

JERNEJ PORENTA,
ARNES

I / IaaS – Infrastructure
as a Service / Infrastruktura
kot storitev

POVZETEK

V letu 2011 bo Arnes organizacijam ponudil tudi nekatere storitve, ki jih danes radi imenujemo storitve v oblaku. Poleg osnovnega Arnesovega oblaka bomo v letu 2011 ponudili tudi diskovni prostor, ki ga bodo lahko uporabljale organizacije, priklopljene v Arnesovo omrežje. Tak diskovni prostor bodo lahko uporabniki uporabljali predvsem za shranjevanje varnostnih kopij in deljenje datotek preko spleta. Poleg tega bodo naši uporabniki začeli uporabljati storitev označevanja nezaželenih elektronske pošte, ki smo jo razvili v sodelovanju s strokovnjaki Instituta Jožef Stefan. Storitev je namenjena organizacijam, ki že imajo svoje poštne strežnike in želijo izkoristiti znanje, ki ga ima Arnes s področja nezaželene elektronske pošte.

KLJUČNE BESEDE: RAČUNALNIŠTVO V OBLAKU,
STORITEV, NEŽELENA SPOROČILA, SHRANJEVANJE
PODATKOV

UVOD

V sklopu Arnesovih storitev v oblaku bomo v letu 2011 ponudili tudi storitev shranjevanja večjih količin podatkov za naše uporabnike preko znanih protokolov in označevanje neželene elektronske pošte za organizacije, ki imajo svoje poštne strežnike.

SHRANJEVANJE PODATKOV V ARNESOVEM OBLAKU

Shranjevanje podatkov v oblaku je ena izmed storitev IaaS¹. Uporabniki storitve dobijo na voljo nekaj prostora v oblaku, ki ga lahko porabijo poljubno za svoje potrebe. Tak prostor v oblaku je namenjen predvsem temu, da bodo lahko uporabniki odlagali svoje podatke na ločeno lokacijo za namene varnostnih kopij oziroma začasne hrambe podatkov.

Storitev shranjevanja podatkov v Arnesovem oblaku bo bazirala na javno dostopni programski opremi in bo omogočala dostop do podatkov preko znanih protokolov (iSCSI, SCP, FTP ...), ki bodo poenostavili uporabo storitve končnim uporabnikom. Ti protokoli so namreč dandanes vgrajeni v vse sodobne operacijske sisteme in ne potrebujejo dodatne programske opreme.

Sam sistem bo zasnovan tako, da bo omogočal razširitev prostora za končne uporabnike in tudi enostavno razširitev celotnega sistema za Arnes. Sama arhitektura bo zasnovana tako, da bo v prihodnosti omogočala porazdelitev strojnih virov po celotni Sloveniji, kar bo omogočilo tudi boljše zmogljivosti celotnega sistema.

ABSTRACT

In 2011, ARNES will offer organisations certain services today known as cloud services. The presentation will first outline the possibility of storing larger amounts of data on ARNES servers. Organisations will thus obtain disk space for their own purposes, including backup storage, distribution of large files on the Internet etc. ARNES has also long since offered its users a service to mark unwanted email, or spam. This year we will also offer this service to organisations that receive email on their own mail server and that have problems in the operation of mail servers due to spam, as well as end-user dissatisfaction due to electronic messages incorrectly marked as spam.

KEY WORDS: CLOUD COMPUTING, SERVICE, SPAM,
STORAGE

Prednosti, ki jih bodo deležni uporabniki te storitve, so predvsem v tem, da bodo lahko na enostaven način shranjevali podatke na oddaljeno lokacijo, ki bo povezana z zmogljivo mrežno povezavo v internet. Nezanemarljiv podatek je tudi to, da bo storitev na voljo Arnesovim uporabnikom brezplačno.

OZNAČEVANJE NEŽELENE ELEKTRONSKE POŠTE

Arnes je že dolga leta znan po svojem filtru za označevanje neželene elektronske pošte. Pri internem testiranju smo ugotovili, da pravilno označi 99,98% elektronske pošte, kar pomeni, da dosega izvrstne rezultate.

V letu 2011 nameravamo tako pridobljeno znanje deliti tudi z drugimi organizacijami, ki so upravičene do Arnesovih storitev. Organizacije, ki imajo svoje pošte strežnike, bodo lahko svojo elektronsko pošto preverile na Arnesovih sistemih in tako enostavno omogočile svojim uporabnikom pravilno označeno elektronsko pošto.

Neželena elektronska pošta ali »spam« je namreč velik problem, obenem sistemi, ki omogočajo označevanje le-te, potrebujejo veliko vzdrževanja in prilagajanja tehnikam, ki jih uporabljajo pošiljatelji neželene pošte. Ker to na Arnesu počnemo znotraj dnevnih aktivnosti, hočemo to storitev ponuditi tudi zunanjim uporabnikom.

Slabosti te storitve so povezane z varstvom osebnih podatkov, čemur na Arnesu posvečamo veliko pozornosti. Zato bodo vse organizacije, ki bodo hotele to storitev, podpisale poseben dogovor o varstvu osebnih podatkov. Na tak način bo organizacija dobila zagotovilo, da je elektronska pošta na Arnesu samo označena glede na vsebino, ne pa tudi shranjena za kasnejšo obdelavo.

ZAKLJUČEK

Nove storitve, ki jih razvijamo na Arnesu v okviru Arnesovega oblaka, bodo uporabnikom omogočile enostavno uporabo le-teh v svojih strežniških sistemih. S tem bodo znižali stroške svoje informacijske infrastrukture, saj so vse storitve, ki jih ponujamo na Arnesu, brezplačne.

I, 2, 3, 4 – NA IPV6!

I, 2, 3, 4 – GO IPV6!

MATJAŽ STRAUS
ISTENIČ, ARNES

POVZETEK

Regionalnim internetnim registrom je bil v začetku februarja 2011 dodeljen ves razpoložljiv naslovni prostor IPv4. Nove IPv4-naslove bomo lahko pridobili le iz zaloga. Z izčrpanjem le-teh se bo širitev IPv4-omrežij dokončno ustavila. Soočeni bomo z dejstvom, da bo za nove omrežne sisteme in storitve možen le novi protokol – IPv6. V prispevku je predstavljenih nekaj bistvenih razlik med protokoloma IPv4 in IPv6 ter ključnih točk za uspešno posodobitev omrežij in storitev: pridobitev dostopa do interneta preko IPv6; izbor in izobraževanje lastnih strokovnjakov za IPv6; pregled svojega omrežja in storitev ter raziskava vpliva uvajanja IPv6; postopno uvajanje IPv6 v omrežje in posodabljanje storitev; varnost novega omrežja in storitev na IPv6; sobivanje novega protokola z IPv4.

KLJUČNE BESEDE: IPV6, PROTOKOL IP, UVAJANJE, VARNOST IP.

UVOD

Internetni protokol (IP) omogoča učinkovito komunikacijo preko obsežnih omrežij, v katera je povezanih izjemo veliko število naprav – pravimo, da komuniciramo preko »interneta«. Ključno je, da IP-protokol omogoča neposredno (angl. *end-to-end*) komunikacijo. Vsaka komunikacijska naprava v ta namen uporabi svoj lasten IP-naslov, brez katerega ne more neposredno komunicirati z drugimi napravami. Število različnih IP-naslovov in s tem število neposredno dosegljivih naprav v internetu je omejeno.

V začetku februarja 2011 so po svetovnih regijah razdelili zadnje IP-naslove, ki so definirani po IP-protokolu različice 4 (IPv4). Posamezne regije (Evropa, Amerika, Latinska Amerika, Afrika, Azija in Pacifik) imajo v času priprave prispevka na zalogi dovolj IPv4-naslovov za nekaj 100.000 srednje velikih lokalnih omrežij (vir 1). Z izčrpanjem le-teh bo širitev IPv4-interneta dokončno ustavljena.

Nove naprave torej potrebujejo nove naslove, ki pa jih IPv4 več ne more zagotoviti. Uporabiti bo potrebno posodobljeno različico internetnega protokola – različico 6 (IPv6). Na IPv6 lahko poenostavljeno gledamo kot na nov način oštevilčenja interneta (vir 2). Najpomembnejša lastnost IPv6 je spremenjen zapis IP-naslova, ki omogoča dovolj različnih IPv6-naslovov za vsako praktično uporabo, ki si jo danes lahko zamislimo.

ABSTRACT

The last available IPv4 address space has been allocated to regional Internet registries beginning of February 2011. New IPv4 addresses will only be available from back stock. As these are exhausted, the expansion of IPv4 networks will finally stop. We will be facing the fact that only a new protocol – IPv6 – will be possible for new network systems and services.

The paper will first examine certain fundamental differences between the IPv4 and IPv6 protocols and discuss certain key points for successful modernisation of network services: Gaining an access to IPv6 service, recruitment and training of IPv6 experts, reviewing networks and services, and research into the impact of the introduction of IPv6, gradual introduction of IPv6 to the network and modernisation of services, revision of security of IPv6 networks and services, and coexistence between the new protocol and IPv4.

KEY WORDS: IPV6, IP PROTOCOL, DEPLOYMENT, IP SECURITY.

I/ IPv4-naslov je 32-bitna številka, ki jo zapišemo s štirimi decimalnimi števili med 0 in 255 ločenimi s pikami, npr. 193.2.1.66.

V nadaljevanju si bomo ogledali nekaj bistvenih razlik med protokoloma IPv4 in IPv6. Tako bomo lažje razumeli pomembnost posameznih korakov, ki jih bomo morali opraviti med posodabljanjem omrežja in storitev na IPv6 (vir 3). IPv6 namreč ni samo spremenjen IP-naslov v praktično neomejenem naslovnem prostoru – IPv6 je drugačen in z IPv4 nezdržljiv protokol. Za uspešno uvedbo IPv6 bodo morali naši strokovnjaki za informacijsko tehnologijo pridobiti nova znanja, temeljito pregledati obstoječa omrežja in storitve ter prepoznati in obvladovati morebitne spremembe ob prehodu na nov protokol. Spoznati bodo morali nove in spremenjene lastnosti IP-protokola ter njihov vpliv na varnost omrežja.

Ne pozabimo, da IPv4 ne bo čez noč izginil iz naših omrežij. Pripraviti se bomo morali na dolgoletno sobivanje obeh različic IP-protokola in postopno ukinitve IPv4.

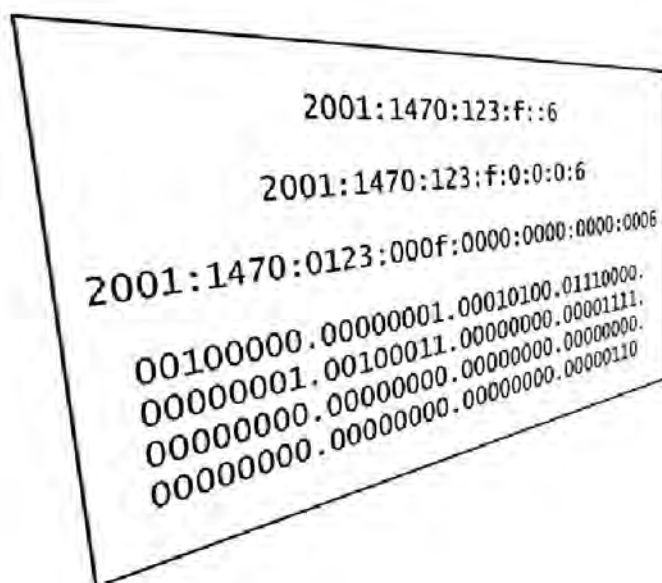
○ 4 IN 6 OGROMEN NASLOVNI PROSTOR

- 128-biten IPv6-naslov zapišemo s šestnajstiškiimi števili, ločenimi z dvopičji, npr. 2001:1470:1:fee1::600d.
- Sisteme v lokalnem omrežju oštevilčimo s 64 biti.
- IPv6-naslovov je ogromno, dovolj za nekaj 10 milijonov lokalnih omrežij na kvadratni meter zemlje.
- Naslovni prostor IPv6 hierarhično delimo na manjše dele.

Najpomembnejša razlika med IPv4 in IPv6 je v dolžini IP-naslova, najvidnejša pa v zapisu IP-naslova. IPv6-naslov je sestavljen iz 128 bitov, združenih v osem 16-bitnih skupin¹. Te skupine zapišemo s šestnajstiškiimi števili med 0 in ffff ter jih ločimo z dvopičji. K preglednosti zapisa pripomore, če opustimo strjeno zaporedje samih ničel in ga nadomestimo z dvema dvopičjema. Prav tako lahko opustimo vodilne ničle v posameznih skupinah. Primer IPv6-naslova prikazuje Slika 1 .

Slika 1:

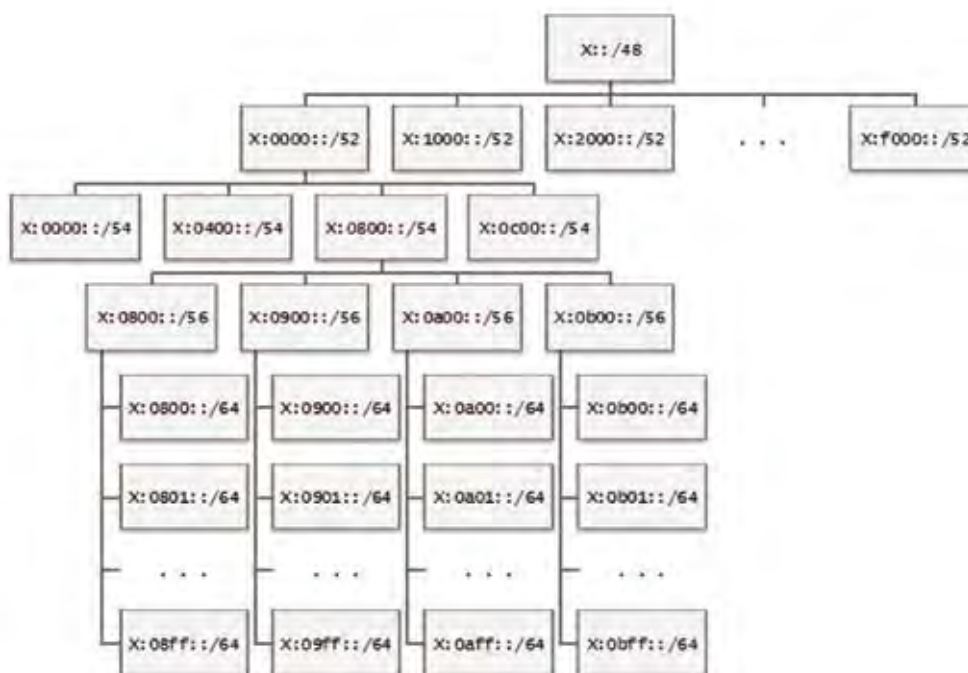
RAZLIČNE
PREDSTAVITVE
IPV6-NASLOVA.
OD ZGORAJ NAVZDOL:
SKRAJŠAN – KOMPAKTEN
IN PRIPOROČLJIV ZAPIS,
RAZŠIRJEN ZAPIS, POLN
ZAPIS BREZ OPUŠČANJA
NIČEL (8 SKUPIN PO 16
BITOV), BINAREN ZAPIS
(128 BITOV).



O številu vseh IPv6-naslovov pogosto govorimo v presežkih. Primerjajmo obseg 128-bitnega naslovnega prostora IPv6 z 32-bitnim naslovnim prostorom IPv4. V lokalnih omrežjih je običajno, da za številčenje posameznih IPv6-sistemov v nekem skupnem segmentu omrežja uporabimo 64 bitov. 128 bitov nam omogoča, da naslovimo sisteme v 2^{64} lokalnih omrežjih. To je ogromno število, ki si ga težko predstavljamo, zato ga raje slikovito primerjamo s številom vseh možnih IPv4-omrežij, v katerih je pribl. 250 sistemov. Teh je 2^{24} , saj od 32 bitov IPv4-naslova uporabimo 8 bitov za številčenjem posameznih sistemov. Razmerje med številoma tovrstnih IPv6- in IPv4-omrežij je ogromno, vendar bolj predstavljivo – $2^{40} \approx 10^{12} \approx 1.000.000.000.000$ (milijon milijonov). Predstavljajmo si, da bi vsa IPv4-omrežja stlačili v eno samo pšenično zrno z maso 40 mg. Za IPv6-omrežja bi potrebovali vsebnik za 40.000 ton pšenice. Ne pozabimo, da lahko v vsako od teh IPv6-omrežij »v zrnih« – zgolj teoretično, seveda – povežemo vse IP-sisteme na Zemlji, v eno od IPv4-omrežij iz naše primerjave pa le približno 250 sistemov.

Ogromen naslovni prostor nam omogoča učinkovite hierarhične načine delitve naslovov znotraj omrežij ponudnikov in uporabnikov internetnih storitev. Organizaciji z več internimi omrežji ponudnik internetnih storitev dodeli naslovni blok /48. Tak blok je dovolj velik za več kot 65.000 omrežij, zato ga v organizaciji z nekaj deset omrežji lahko brez težav razdelimo na več manjših delov enake velikosti. V IPv4-omrežjih smo bili omejeni z velikostjo posameznih delov omrežja, zato smo nekaterim namenili manj, drugim pa več IPv4-naslovov. Z IPv6 je drugače. Blok /48 razdelimo v drevesni strukturi na manjše dele, bodisi /52, /56 ali /60. Strogih pravil za tako delitev ni, priporočamo pa, da se v delitvi omejujemo na velikosti, ki so mnogokratnik števila 4. Slika 2 prikazuje primer take delitve.

Slika 2:
 HIERARHIČNA
 DELITEV
 NASLOVNEGA
 PROSTORA /48.
 PROSTOR ORGANIZACIJE
 JE NAJPREJ RAZDELJEN NA
 16 LOKACIJ /52, POTEM
 PA PODROBNEJE ZA
 PRVO LOKACIJO, KJER SE –
 GLEDE NA VARNOSTNO
 POLITIKO – DELI V ŠTIRI
 DELE /54 S SKUPNO 16
 PODROČJI /56. V VSAKEM
 OD TEH PODROČJI
 JE LAHKO DO 256
 PODOMREŽIJ /64.



2/ Običajno ima vmesnik IPv6-naprave vsaj dva IPv6-naslova – lokalnega in globalnega. Nekateri operacijski sistemi že v privzeti konfiguraciji dodelijo vmesniku več globalnih naslovov.

3/ To ne pomeni, da sistem za komunikacijo preko interneta lahko uporabi lokalni naslov – ne, vedno uporabi globalnega, vendar lahko posreduje promet tudi preko lokalnega naslova privzetega prehoda.

4/ NAT ni varnostni mehanizem – za varnost skrbimo na drugačen način kot s skrivanjem za nekim javnim naslovom (filtri, požarne pregrade, zaščita na računalnikih samih).

5/ V IPv4 so zelo pomembna ICMP sporočila, ki se nanašajo na delitev paketov, npr: »destination unreachable/fragmentation needed and Don't Fragment bit set«. Blokiranje takih sporočil lahko onemogoči uporabo nekaterih internetnih storitev.

NASLOV ZA DOLOČEN NAMEN

- Na vsakem od vmesnikov IPv6-naprave je lahko več naslovov, ki so lahko lokalni ali javni (globalni) in različnega tipa.
- IPv6-naslovi določenega tipa se uporabljajo glede na namembnost.
- Za komunikacijo v internetu uporabljamo javne naslove.
- Naslov znotraj nekega IPv6-podomrežja si naprava lahko določi sama.

Vmesnik na neki IPv6-napravi ima lahko več IPv6-naslovov². Glede na način komuniciranja in namembnosti jih delimo v naslednje skupine:

eden z enim: *unicast*,

- lokalna komunikacija na skupnem segmentu: *link-local unicast*,
- lokalna komunikacija v organizaciji: *unique local unicast (ULA)*,
- globalna komunikacija na internetu (javni naslov): *global unicast*,
- komunikacija z IPv4-sistemi (v IPv6 preslikan IPv4-naslov): *IPv4-mapped*,
- eden z mnogimi: *multicast*,
- eden z najbližjim: *anycast*.

Naslove za komunikacijo enega sistema z mnogimi (*multicast*) poznamo že iz protokola IPv4, vendar so v IPv6 mnogo bolj sistematično definirani (vir 4, poglavja »IPv6 Addressing«, »IPv6 Multicast«). Novost v IPv6 so naslovi, ki omogočajo komunikacijo enega sistema z drugim, ki je glede na topologijo omrežja najbližje (*anycast*) in naslovi, ki so namenjeni komunikaciji na skupnem lokalnem segmentu omrežja (*link-local*). To velja tudi za naslov privzetega prehoda do interneta (angl. *default gateway*) – tudi ta naslov je lokalnega tipa, kar je na prvi pogled nenavadno, posebno, ker v IPv4-omrežjih ni tako³.

Za komunikacijo v IPv6-internetu uporabljamo javne naslove (*global unicast*). Teh je za vse naprave dovolj, zato translacijski mehanizmi NAT niso potrebni⁴.

V IPv6 je definiran mehanizem, ki napravam omogoča, da si same samodejno nastavijo unikatni globalni naslov. Pogosto je, da se ta naslov določi iz razširjenega naslova omrežnega vmesnika (*MAC – Media Access Control Address*) ali pa ga sistem izbere naključno.

KONTROLNA SPOROČILA ICMP

- ICMPv6 je izjemno pomemben protokol, predvsem v lokalnem omrežju.
- Previdno pri filtriranju ICMPv6-sporočil!

S sporočili ICMP kontroliramo povezljivost omrežnih naprav (npr. *ping*, *traceroute*), preverjamo stanje in lastnosti omrežja (npr. največjo velikost paketa, ki se lahko posreduje brez delitve – *MTU*), dosegljivost končnih sistemov ipd. Pravilno delovanje IPv4-storitev ni kritično odvisno od kontrolnih sporočil ICMP⁵, kar pa nikakor ne velja za IPv6. ICMP za IPv6 (ICMPv6) je zelo pomemben – ključen protokol in veliko osnovnih mehanizmov IPv6 sloni prav na njem, npr.:

- identifikacija sosedov v omrežju,
- odkrivanje podvojenih/že uporabljenih IPv6-naslovov,
- razglašanje in iskanje usmerjevalnika,
- pridobivanje informacij za samodejno nastavitve IPv6-naslova,
- ugotavljanje največje velikosti paketa (*MTU*) na poti do nekega ciljnega sistema.

6/ To je novost v NDP, na katero smo dolgo čakali. Opisuje jo RFC 6106 (IPv6 Router Advertisement Options for DNS Configuration), nov. 2010.

Nepravilno filtriranje sporočil ICMP zato lahko povzroči nepravilno delovanje ali celo prepreči uporabo omrežnih storitev po protokolu IPv6.

NA OMREŽJU ETHERNET

- Namesto ARP-a so v IPv6 vgrajeni mehanizmi ND, ki slonijo na ICMPv6.
- IPv6 omogoča samodejno določitev IP-naslova in privzetega prihoda.

Naprave si v omrežju ethernet izmenjujejo podatke v t.i. »ethernet okvirjih«. Vsak okvir je opremljen z MAC-naslovoma pošiljatelja in prejemnika. IP-sistemi morajo poznati MAC-naslov prejemnika, ki mu predajajo v ethernet okvirjen IP-paket. V IPv4 je za identifikacijo MAC-naslova, ki pripada nekemu IPv4-sistemu, skrbel poseben protokol z imenom ARP (*Address Resolution Protocol*). V IPv6 je naloge ARP-a prevzel protokol NDP (*Neighbor Discovery Protocol*), ki za transport podatkov uporablja ICMPv6.

NDP deluje znotraj lokalnega omrežja. Končnim sistemom omogoča, da:

- poiščejo usmerjevalnike in privzete prehode,
- izvejo IPv6-naslove podomrežij, znotraj katerih si lahko sami nastavijo naslov,
- preverijo, ali je določen naslov že v uporabi (*DAD – duplicate address detection*),
- preverijo, ali je nek drug sistem v omrežju dosegljiv,
- ugotovijo MAC-naslov nekega drugega sistema v omrežju, vključno z MAC-naslovom privzetega prehoda.

Usmerjevalniki lahko končnim sistemom s pomočjo NDP sporočijo tudi naslov imenskega strežnika DNS in privzeto ime internetne domene⁶.

KAKO NA 6?

- Pridobite dostop do internetnih storitev preko IPv6. Obrnite se na svojega internega ponudnika (Arnes).
- Določite lastnega strokovnjaka za IPv6 in poskrbite za njegovo izobraževanje.
- Preglejte svoje omrežje in storitve ter raziščite vpliv uvajanja IPv6.
- Omrežje in storitve posodablajte postopoma, začnite pri najmanj kritičnih storitvah in si pridobite izkušnje.
- Ne pozabite na varnost novega omrežja in storitev na IPv6.
- Pripravite se na sobivanje novega protokola z IPv4.

Uvajanje IPv6 je zaradi sorodnosti z IPv4 enostavnejše, kot je bilo uvajanje IP v začetkih IPv4-interneta. Otežuje ga le »kronično« pomanjkanje časa – za IPv4 smo se postopoma izobraževali vrsto let, IPv6 pa bomo morali osvojiti v letu ali dveh. Zato je toliko bolj pomembno, da se tega lotimo premišljeno. Raziskovalnim in izobraževalnim organizacijam bo pri tem v veliki meri pomagal Arnes.

KJE POMAGA ARNES?

- Registracija in delitev IPv6-naslovnega prostora.
- Svetovanje pri izboru dostopovne opreme.
- Vzpostavitev povezave z IPv6-omrežjem ARNES in nastavitve dostopovne opreme.
- Svetovanje pri posodabljanju storitev.
- Izobraževanje za IPv6.

Prehod na IPv6 se začne pri ponudniku internetnih storitev. Arnes omogoča omrežne storitve po protokolu IPv6 na vseh povezavah, kjer ima organizacija/članica ustrezno dostopovno opremo (usmerjevalnik IP-prometa) in povezavo do Arnesovega hrbteničnega omrežja. Največja ovira je prav zastarela in neprimerna dostopovna oprema, ki ne omogoča IPv6, drug problem pa so dostopovne povezave preko omrežij ponudnikov, ki na IPv6 še niso pripravljeni.

Začeli bomo s pridobitvijo IPv6-naslovnega prostora (vir 7) in razporeditvijo le-tega po lokalnih omrežjih. Arnes predlaga primerno dostopovno opremo, jo nastavi in omogoči povezavo s hrbteničnim omrežjem. Arnesovi strokovnjaki svetujejo tudi pri posodobljanju osnovnih omrežnih storitev.

KAJ NAREDI ORGANIZACIJA/ČLANICA SAMA?

Prvo in najbolj pomembno je, da organizacija izbere in čimprej izobrazila lastnega strokovnjaka, ki bo vodil prehod na IPv6. Začel bo s pregledom omrežja in omrežnih storitev in ugotovil, kaj vse je potrebno posobiti in kje lahko nastopijo potencialni problemi pri posodobitvi na IPv6. Na podlagi tega lahko v organizaciji ocenijo stroške prehoda in planirajo prehod na IPv6. Izbrati bo potrebno ustrezne dobavitelje opreme, serviserje in svetovalce oziroma preveriti, ali so obstoječi že primerno usposobljeni za IPv6.

Zavedati se moramo, da en sam strokovnjak za IPv6 v organizaciji ne bo dovolj. Izobraževanje za IPv6 bo v primernem obsegu zajelo vse osebe za informacijsko tehnologijo. Žal to ne bo poceni (vir 8).

ZA KONEC ŠE NEKAJ NASVETOV:

- Ne vklaplajte IPv6 v omrežjih, ki nimajo zanesljive IPv6-povezave. Le-ta naj bo po kvaliteti in zmogljivostih primerljiva z IPv4-povezavo.
- Povsod uporabljajte globalni (javni) IPv6-naslovni prostor.
- Naslovni prostor razdelite hierarhično.
- V lokalnih omrežjih uporabljajte naslovne bloke /64, kar omogoča nemoteno samodejno konfiguracijo sistemov (angl. *Stateless Autoconfiguration*).
- Kontrolni protokol (ICMPv6) je zelo pomemben za delovanje IPv6-omrežja in storitev! Nepravilno filtriranje prometa ICMPv6 je pogost vzrok za napake v delovanju.
- Bodite previdni pri izbiri omrežne opreme. Izberite le tako opremo, kjer se IPv4 in IPv6 promet obravnavata enako ali vsaj primerljivo (vir 5).
- Skrbite za varnost omrežja! Pri IPv4 ste bili morda navajeni skrivanja za mehanizmi NAT, sedaj pa boste na lepem uporabljali globalno dosegljive javne IPv6-naslove. Izberite primerno požarno pregrado in poskrbite za varnost omrežja neposredno na računalnikih samih.

Prepoznavajte in odpravite napravnosti, vendar ne tako, da bi na svojem računalniku preprosto izklopili IPv6 in s tem »rešili problem«.

- Poskrbite za pravočasno prenovo internetnih storitev, ki jih nudite. Novi uporabniki interneta morda ne bodo imeli več IPv4-naslovov – naj bo vaša storitev dosegljiva tudi njim.

Sodelujte in izmenjujte mnenja in izkušnje! Slovenska inicijativa za IPv6 je močna (vir 6), na Arnesu je splošen »debatni krožek« razprava@ipv6.si, IPv6 lahko preizkusite

v laboratorijih Arnesa, zavoda Go6, LTFE Univerze v Ljubljani in projekta *6deploy*, organiziramo IPv6-srečanja z delavnicami (peto bo predvidoma maja 2011) itd. Vzpodbujajte sodelavce, ki pokažejo zanimanje in zagnanost za uvajanje IPv6 v vašem okolju: izobrazite jih, dajte jim možnost dela na področju IPv6, nagradite jih – obrestovalo se vam bo!

ZAKLJUČEK

IPv6 je sprememba na bolje, korak naprej. Kot vsaka sprememba pa zahteva, da se nanjo pripravimo in se prilagodimo novemu. Zato je izobraževanje ključnega pomena za uspešno uvedbo IPv6 v naša omrežja. Pri tem vam lahko pomagajo tudi Arnesovi strokovnjaki, ki so dosegljivi na ipv6-podpora@arnes.si.

Prvi kratkoročni cilj, ki si ga lahko z Arnesom zastavimo, je, da bo spletna stran vaše organizacije dostopna po IPv6 na svetovni IPv6-dan 8.6.2011 (vir 9). Se »vidimo« na IPv6!

VIRI

(vse našete spletne strani so bile obiskane februarja 2011)

http://en.wikipedia.org/wiki/Regional_Internet_registry, <http://www.iana.org/numbers/>, <http://www.potaroo.net/tools/ipv4/>, <http://ipv6.he.net/statistics/>

<http://www.arnes.si/storitve/omrezne-storitve/ip-povezljivost/ipv6.html>

<http://www.ipv6actnow.org/info/how-to/>

<http://www.6deploy.eu/index.php?page=tutorials>, http://en.wikipedia.org/wiki/IPv6_address

<http://www.ripe.net/ripe/docs/ripe-501>

<http://go6.si/>

<http://www.arnes.si/storitve/dostop/registracija-ip.html>

<http://www.erion.co.uk/IPv6Training/>

<http://dan.ipv6.si/>

IPV6 – KAJ PA STORITVE?

IPV6 – WHAT ABOUT SERVICES?

KLEMEN ANDREUZI,
ARNES

POVZETEK

Uporabniki, ki v medmrežje ne bodo povezani preko IPv4 protokola – bodisi zaradi izčrpanosti IPv4 naslovnega prostora, ali katerega drugega razloga – ne bodo imeli dostopa do storitev, ki podpirajo samo IPv4 protokol. Zato je zelo pomembno, da poleg prilagoditve omrežne opreme IPv6 protokolu, prilagodimo tudi storitve, ki jih ponujamo na višjih plasteh, kot so na primer spletni strežniki, poštni strežniki, domenski strežniki ipd. V članku bom na podlagi lastnih izkušenj opisal, na kaj je potrebno biti pozoren, ko svoje storitve prilagajamo IPv6 protokolu.

KLJUČNE BESEDE: IPV6, STORITVE

ABSTRACT

Users who will not connect to the Internet via the IPv4 protocol (either due to the exhaustion of the IPv4 address space or for some other reason) will not be able to access services that only support the IPv4 protocol. It is therefore very important that – in addition to adjusting network equipment to the IPv6 protocol – we also adjust services offered on higher layers, such as web servers, mail servers, domain name servers etc. The paper will show, based on our own experience, things to be aware of when adapting services to the IPv6 protocol.

KEY WORDS: IPV6, SERVICES

UVOD

Storitve, ki jih nudimo uporabnikom preko IPv4, je potrebno prilagoditi, da delujejo tudi na IPv6. Nadgradnja storitve z delovanjem po Ipv6 se deli na več sklopov, ki jih je potrebno za delovanje opraviti. Potrebno je namreč zagotoviti IPv6 povezljivost – podpora operacijskega sistema IPv6 protokolu ter same omrežne nastavitve. Poskrbeti je potrebno za podporo oziroma nastavitve programske opreme na kateri teče naša storitev. Nazadnje pa je potrebno pravilno urediti zapise na domenskih strežnikih. Naš cilj bo torej zagotoviti delovanje storitev, ki jih ponujamo tudi preko IPv6.

STORITVE NA IPV6 NASTAVITVE OMREŽJA IN OPERACIJSKEGA SISTEMA

Pri nadgradnji storitve na Ipv6 in v smislu zagotovitve čim kvalitetnejše storitve, ki jo nudimo uporabnikom, je najprej potrebno zagotoviti dve stvari:

- brezhibno delovanje IPv6 omrežja na katerem bo delovala naša storitev;
- podpora in nastavitve operacijskega sistema za IPv6.

Načeloma je IPv6 podoben IPv4. IPv6 prinaša več naslovov, nekaj izboljšav in dodatkov. Razlik na nižjih plasteh omrežja ni. Torej je dobro postavljeno omrežje, na katerem dobro deluje IPv4 povsem primerno tudi za delovanje IPv6. Tako so razlike le v internetni plasti internetnega sklada. Tam je konfiguracija IPv4 ločena od IPv6. Pri tem je potrebno zagotoviti, da je propustnost omrežja in povezljivost enaka ali boljša od IPv4. Kot propustnosti se smatra hitrost in kvaliteta prenosa paketov čez omrežje. Pri povezljivosti omrežja pa je potrebno biti pozoren na več stvari. Ena iz med stvari, na katere je potrebno biti pozoren je to, da bo dostop odjemalca do storitve enak, ne glede na to, ali bo dostopal preko IPv4 ali Ipv6. Zato je potrebno, da so filtri na omrežju za servise na IPv6 enaki tistim na IPv4.

Primer: predpostavimo, da se ime spletne strani razreši v IPv4 in IPv6. Filtre na IPv6 je potrebno prilagoditi tako, da bo dostop do vrat 80 enak tistim na IPv4. V nasprotnem

primeru se odjemalcem z IPv6 naslovom ne bo uspelo povezati. Odjemalci z obema protokoloma (IPv4 in IPv6) pa bodo vzpostavljali povezavo le preko IPv6. Tako onemogočimo dostop do storitve tudi tistim odjemalcem, ki imajo poleg IPv6 še IPv4.

Pri nadgradnji servisov na IPv6 je torej, s stališča omrežja, potrebno paziti, da bodo filtri omrežja kar se da podobni IPv4 filtrom. Potrebno je zagotoviti tudi enako propustnost in kvaliteto, ki pa nam jo običajno zagotovijo že dobro postavljene nižje plasti omrežja.

Podpora današnjih operacijskih sistemov IPv6 je relativno dobra. Tako operacijski sistemi, kot so Windows, Linux, *BSD, Solaris ... že precej časa podpirajo IPv6 mreženje. Zagotoviti je le potrebno, da so moduli oziroma gonilniki vključeni v jedro operacijskega sistema. Sistemski administrator mora poskrbeti le še za pravilne nastavitve IPv6 naslovov, mask in usmeritvenih tabel.

Pri sami postavitvi IPv6 storitev imamo na izbiro več različic postavitve. Servis z IPv4 in IPv6 lahko ponudimo na istem strežniku, lahko jih ločimo na različne strežnike, ali pa na istemu strežniku z različnimi instancami iste programske opreme nudimo storitev preko IPv4 in IPv6. Več v naslednjem poglavju.

PROGRAMSKA OPREMA

Ločenost aplikacijske plasti od internetne plasti, še ne pomeni, da bo programska oprema podpirala IPv6. Programska oprema mora poznati IPv6, da lahko poda jedru zahteve za ustrezno IPv6 inicializacijo.

Podpora programske opreme za IPv6 počasi narašča. Vsaka nova (resnejša) programska oprema, ki je namenjena ponujanju storitve na internetu, podpira IPv6. Vprašanje pa se postavi, kako je s starimi. Z nadgradnjo na novejša različica programske opreme, običajno dobimo tudi IPv6 podporo. Seveda za vse storitve ni moč dobiti IPv6 podpore, zato se moramo odločiti za menjavo programske opreme, oziroma storitve sploh ne nadgradimo.

Postavitev IPv6 programske opreme je odvisna od več dejavnikov. Sprejeti je potrebno nekaj odločitev:

- storitvi lahko ločimo po strežnikih/gručah;
- storitvi lahko ločimo po različni programski opremi;
- storitvi lahko ločimo po isti programski opremi z različno instanco programske opreme;
- storitvi imamo na isti programski opremi z isto instanco.

Ponavadi je zadnja možnost najboljša. Potreben je le pogoj, da programska oprema podpira IPv6. Tako je potrebna le ustrezna konfiguracija programske opreme.

Na Arnesu smo vse storitve, ki smo jih nadgradili z IPv6 pustili na isti programski opremi z isto instanco. V veliki večini so različice, ki so distribuirane z našo distribucijo operacijskega sistema, že podpirale IPv6. Tako nadgradnja programske opreme ni bila potrebna. Nekaj programske opreme smo morali nadgraditi z drugih virov, nekatere pa je bilo potrebno ročno prevesti. Z distribucijo operacijskega sistema pridejo tudi varnostni popravki programske opreme. Tako nam ni potrebno posebej skrbeti za nadgradnjo.

V primeru, da dobimo pakete iz drugih virov, oziroma, da jih prevedemo sami, je potrebno tudi spremljati morebitne varnostne grožnje. Na primer, CentOS distribucija operacijskega sistema, ki ga uporabljamo na Arnesu, ne prinaša paketa squid z IPv6 podporo. Paket smo morali narediti sami, zanj pa moramo sami spremljati varnostne postavke.

Na Arnesu smo uspešno postavili kar precej programske opreme z IPv6 podporo. Med njimi so Apache, Mysql, Vsftpd, Squid, Bind, Unbound ... Dokumentacija odprtokodne programske opreme za ipv6 je presenetljivo dobra. Tako je konfiguracija relativno enostavna.

Tipično na istem strežniku lahko ponujamo več storitev. Prehod na IPv6 za vse storitve hkrati je lahko težaven, ali pa celo nemogoč. Tako je najboljše storitve nadgraditi postopoma. Pomagamo si lahko z zapisi na domenskih strežnikih.

ZAPISI NA DOMENSKIH STREŽNIKIH

Domenski strežniki skrbijo za ustrezne preslikave imen strežnikov v IP (verzije 4 in/ali 6), in obratno. Zapisi za IPv4 se imenujejo A zapisi, za IPv6 pa AAAA zapisi. CNAME zapisi pa so tako imenovani kazalci na druga imena strežnikov, za katere obstaja A ali AAAA zapis.

Ob nadgradnji storitve na IPv6 je torej potrebno urediti še ustrezne zapise na domenskih strežnikih. Pri dodajanju AAAA zapisov je potrebno nekaj previdnosti. Tipično je najboljše, da imenu strežnika ne damo AAAA zapisa kar takoj. Najboljše je, da AAAA zapis dodamo za kakšno drugo ime. V primeru selitve Arnesove spletne strani nismo dodali AAAA zapisa za www.arnes.si, ampak smo dodali AAAA zapis www.ipv6.arnes.si in nato testirali delovanje. Po določenem času smo dodali AAAA zapis za www.arnes.si z majhno TTL (*time to live*) vrednostjo. TTL vrednost nam pove kako dolgo je zapis veljaven. Tako bi lahko ob morebitnih težavah hitro odstranili zapis.

V primeru, da imamo strežnik z več storitvami, je potrebna dodatna pozornost. Tipično ima tak strežnik A zapis, storitve, ki jih ponujamo, pa CNAME zapise. V primeru Arnesa je tak strežnik poprovec.arnes.si, ki ponuja več storitev; ftp.arnes.si, proxy.arnes.si, cache.arnes.si, news.arnes.si ...

Vseh storitev na tem strežniku nismo selili na IPv6. Tako poprovec.arnes.si ni dobil AAAA zapisa, servisi z IPv6 podporo pa so zamenjali CNAME zapis z A in AAAA. V nasprotnem primeru bi servisi brez ipv6 podpore lahko imeli IPv6 naslov.

Verjetno najbolj zapleten primer dodajanja storitve na IPv6 predstavlja dodajanje poštne strežnikov. Že sama konfiguracija IPv6 poštnega strežnika je zaradi več razlogov težavna. Posebej pozoren velja biti pri dodajanju zapisov na domenske strežnike. Zapisi za poštna strežnika se imenujejo MX zapisi. MX zapisi so kazalci na strežnike z A in/ali AAAA zapisi. V primeru več MX zapisov za določeno domeno, je v zapisu določena tudi prioriteta zapisa. Tako lahko poštnemu strežniku z A in AAAA zapisom dodelimo večjo prioriteto, kot tistemu samo z A zapisom. IPv6/IPv4 odjemalci se bodo tako najprej poskušali povezati preko IPv6, v primeru težav pa bodo poskušali še z IPv4-strežnikom z manjšo prioriteto.

Zapisi na domenskih strežnikih so tako še ena iz med stvari, ki jih je potrebno opraviti pri nadgradnji storitev na IPv6. S pravilno ureditvijo zapisov si lahko prehod še poenostavimo.

ZAKLJUČEK

Nadgradnja storitev z IPv6 je lahko enostavna, če se nanjo dobro pripravimo in se zavedamo pasti, ki nas pri tem čakajo. IPv6 je tukaj, vsekakor ni stvar, ki se bi je morali bati in z njo odlašati. S hitro in kvalitetno nadgradnjo bomo dvignili nivo storitev, razveselili uporabnike in prispevali k hitrejši vpeljavi IPv6.




KONFERENCA ARNES 2011
KAJ NAM PRINAŠA RAČUNALNIŠTVO V OBLAKU
ZBORNİK ČLANKOV
IZDAL IN ZALOŽIL: Arnes
UREDIL: Domen Božeglav
LEKTORIRALA: Tjaša Žorž
PREVOD: Amidas
OBLIKOVANJE: www.zadruga.si
TISK: tiskarna Kalipso
NAKLADA: 1000 izvodov

CIP - Kataložni zapis o publikaciji
Narodna in univerzitetna knjižnica, Ljubljana

004.77(082)

AKADEMSKA in raziskovalna mreža Slovenije. Konferenca (2011 ;
Kranjska Gora)
Kaj nam prinaša računalništvo v oblaku? : zbornik člankov /
Konferenca Arnes 2011, 13. april 2011, Kranjska Gora, Slovenija ;
[uredil Domen Božeglav]. - Ljubljana : Arnes, 2011

ISBN 978-961-6321-06-8
1. Gl. stv. nasl. 2. Božeglav, Domen
255435008



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