

Mag. Milan SELAN

**Predsednik društva informatikov,
dokumentalistov in mikrofilmarnjcev - media.doc**

UPRAVLJANJE TAJNIH eDOKUMENTOV V OBLAKU Ó TUDIJA IZVEDLJIVOSTI¹

Izve ek:

Avtor je v članku predstavil reševanje problema upravljanja tajnih dokumentov po principu računalništva v oblaku in predstavil možnosti, kako se ta kupljena tehnologija tudi za reševanje drugih informacijskih problemov.

Ključne besede:

Računalništvo v oblaku, sistemi za upravljanje dokumentov, tajni dokumenti

Abstract:

The author presented in this article solving the problem of managing classified documents with so-called cloud computing way and presented the possibilities of how technology has been purchased could be used to solve other computer problems.

Keywords:

Cloud Computing, Document Management Systems, Classified Documents

UVOD

Pojem informatika (oziroma računalništvo) v oblaku (Cloud Computing) ni zgolj popularna modna skovanka zadnjih nekaj let, ampak je priljubljen za mala in novonastala podjetja za uporabo in cenovno uporabno informacijske komunikacijske tehnologije in informacijskih storitev. Pojem je ime dobil po oblaku, ki ga imamo za ponazoritev medmrežja, ponazarja pa nekakšen nedefiniran prostor, kjer uporabnik lahko dobi fiksno IKT, storitve in programe.

Računalništvo v oblaku je že drugo leto zapored s strani Gartner Group uvrščeno kot najpomembnejša strategija tehnologija za leto 2011. To, skupaj s podporo vseh največjih svetovnih IT podjetij, nedvomno dokazuje, da računalništvo v oblaku ni muha enodnevnica, ampak pomembno področje informatike, ki se mu v prihodnosti ne bomo mogli izogniti.

Fujitsu (1) je definirala pet različnih tipov računalniškega oblaka:

- Javni oblak (Public Cloud) je informacijsko okolje, ki ga lahko uporablja kdorkoli. IKT, informacijske storitve in programe si deli večje število uporabnikov. Omrežja niso ločena, zato uporabniki običajno ne vedo kje se hranijo njihovi podatki. Javni oblaki so v strokovnem smislu najučinkovitejši z osnovno zbiranjem podatkov in razpoložljivostjo na vseh nivojih.

¹ Tudija izraža osebno videnje reševanja problema in nikakor ne izraža uradnega ali neuradnega stališča organa, v katerem sem zaposlen

- Verodostojni oblak (Trusted Cloud) označuje okolje v katerem si omejeno število uporabnikov deli en oblak. Z ločenjem mrež lahko ta oblak nudi visoke nivoje varnosti. Vsako podjetje ima svoje virtualne strežnike in sisteme za shranjevanje podatkov do katerih dostopajo le preko virtualnega LAN-a.
- Zasebni oblak (Private Cloud) je IKT okolje namenjeno posameznim uporabnikom z zasebnim dostopom in deljenjem. Strogo določena pravila so lahko definirana in izvedena individualno. Zasebni oblak je lahko lociran v organizaciji ali gostuje pri zunanjih ponudnikih.
- Hibridni oblak (Hybrid Cloud) je kombinacija zasebnega, verodostojnega in/ali javnega oblaka. Podatki in aplikacije so segmentirani glede na določena vodila in podjetje ali IKT zahteve. Možno je, da bo hibridni oblak bolj razširjen v prihodnosti kot večinoma kot mešana oblika notranjih in zunanjih IKT storitev.
- Podjetniški oblak (Enterprise Cloud) je oblak, ki ga v celoti vzpostavi podjetje, namenjen pa je uporabnikom v lastni organizaciji kot primeren za podjetja s prostorsko razpršenimi poslovnimi enotami.

Po vsebini pa lahko v grobem razdelimo v tri sklope (3):

- informacijska infrastruktura kot storitev (Infrastructure as a Service o IaaS): omogoča uporabo navideznih virov, kot so procesorski zasloni, pomnilnik in diskovni prostor. Operacijski sistem, aplikacije in strežnike sicer na daljavo uporabljamo, kot bi jih imeli v podjetju, pri tem pa nam ni treba vzdrževati strojne opreme;
- platforma kot storitev (Platform as a Service o PaaS): posreduje določeno platformo, ki omogoča delovanje programov. Podjetje lahko na tej osnovi razvija svoje programe;
- programi kot storitev (Software as a Service o SaaS): programov ni treba namestiti na uporabnikovem računalniku. V tem primeru uporabnik ne more uporabljati lastnih programov, saj dostopa do razvitih programov prek spletnega vmesnika..

Pri odločitvi o lastni IKT ali o računalništvu v oblaku in o storitvah, ki jih nudi oblak, se je treba odločiti ne le na podlagi stroškov, ampak tudi na podlagi analize in ocene tveganj, ki jih prinaša lasten podatkovni center ali računalništvu v oblaku. Od rezultatov celovite analize so odvisne tako vrsta oblaka, kot vrste storitev, ki jih v oblaku lahko razmejujemo. Pri sklicevanju na dobro prakso uporabe računalništva v oblaku v tujini moram opozoriti, da je v tujini razmerje med stroški IKT in stroški strokovnjakov s področja IKT drugačen, kot pri nas, kjer dela, če posebej na tem področju, ne vrednotimo prav posebno dobro.

Če sodimo, da je računalništvu v oblaku priljubljenost za mala in novonastala podjetja za uinkovito in cenejšo uporabo informacijske komunikacijske tehnologije in informacijskih storitev, lahko v kategorijo novih in malih podjetij dodamo tudi segment ravnanja s tajnimi dokumenti organov državne uprave (TD DU). Z informacijsko podporo ravnanju s TD se soočamo šele v zadnjih nekaj letih, ko nas je v to prisilil konec prehodnega obdobja Uredbe o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih (InfoSec) kot vzpostavljanjem ustrezne infrastrukture in storitev so problemi podobni, kot pri novih podjetjih kot da pa področje sodi v sklop »malih« podjetij, pa menimo, da zaradi tega, ker so TD le zelo majhen segment celovitega sistema vsakega organa DU posebej.

INFORMACIJSKI SISTEM VLADE ZA RAVNANJE S TAJNIMI DOKUMENTI

V preteklem desetletju so na Generalnem sekretariatu Vlade RS (GVS) zgradili u inkovit informacijski sistem za podporo delu vlade in delovnih teles vlade (ISV), do konca prehodnega obdobja uredbe InfoSec, pa so se v tem IS pretakali in hranili tudi dokumenti ozna eni s stopnjo tajnosti interno (do 2011) in zaupno (do 2010).

ISV omogo a popolnoma brezpapirno poslovanje vlade od leta 2001, elektronsko poslovanje pa je omogo ilo, da GSV ukine tiskarno (4 delovna mesta) in zmanj-a -tevilu kurirjev-voznikov za razpo-iljanje vladnih gradiv (4 delovna mesta).

Glede na to, da uredba InfoSec v obi ajnem omreflju (HKOM, DSL) prepoveduje elektronsko razpo-iljanje (ne-ifriranih) tajnih dokumentov vseh stopenj tajnosti ó nekaj »odpustkov« je le za stopnjo tajnosti interno ó je za GSV pomenilo, da mora razmisliti o na inu sprejemanja, hrambe, razmnofovanja in distribucije tajnih dokumentov. e odmislimo enostavno re-itev v pove anju -tevila zaposlenih (kar pa je v sedanjih razmerah zmanj-evanja zaposlenih v DU »misija nemogo e«) in, e pri oceni moflnih re-itev upo-tevamo tudi u inkovitost obstoje ega sistema pri odlo anju o vladnih dokumentih (elektronske, oziroma dopisne seje, odlo anje na daljavo, takoj-en dostop do informacij, itd.), je GSV pri-el do edine moflne re-itve, in sicer, da se za segment TD vzpostavi »mini« kopija obstoje ega ISV.

Zaradi zahtev uredbe InfoSec (in Komisije za informacijsko varnost), da lahko promet s tajnim dokumenti med organi poteka le v -ifrirani obliki, uporaba elektronskih tajnih dokumentov (branje, pisanje, tiskanje) pa je dopustno le z napravami ali v prostorih, ki onemogo ajo nefeljeno elektromagnetno sevanje (TEMPEST), je bilo treba pri izgradnji celovitega sistema za ravnanje s tajnimi dokumenti vlade (ISV-TD) upo-tevati ne le dograditev obstoje ih programov, ampak tudi dograditev IKT GSV in organov, vklju enih v ISV-TD.

ISV-TD KOT HIBRIDNI, OZIROMA PODJETNITMKI OBLAK

ISV-TD smo oblikovali po principu podjetni-kega oblaka, oziroma, kot kombinacijo zasebnega in verodostojnega oblaka, pri tem pa upo-tevali vse sklope (3):

- ministrstva uporabljajo IKT GSV ó navidezni streflniki, navidezni uporabniki ó uporaba tankih klientov (uporabnik lahko dela, ko se uspe-no povefle s streflnikom in si na delovno postajo nalofi operacijski sistem in uporabni-ke programe), diskovni prostor;
- uporablja se enotna platforma, za katero ministrstva ne pla ujejo pristopnine ali licenc (ESX, LINUX, VDI (razen nekaterih licenc, ki se veflejo direktno na uporabnika kot fizi no osebo, ne kot organ), LN Domino, ISV-TD v ofjem smislu besede (programi za delo vlade in delovnih teles vlade), protivirusni programi, po-tni predali organov, itd);
- enotna programska oprema (npr. AdLib za pretvorbo v obliko zapisa PDF-A, komponente za elektronsko podpisovanje dokumentov PorXSign, OpenSource (odprto-kodne re-itve za urejanje besedila in preglednic), MS Office (v tem trenutku je -e v uporabi in je pla ljev ó licence za vsakega uporabnika, njegovo uporabo pa se na rtuje odpraviti v skladu z projektom uporabe odprto-kodnih re-itev Ministrstva za javno upravo).

Naveden pristop (terminal/streflnik oziroma tanki klient/streflnik) omogo a organom, da pri ravnanju s TD v vladnem postopku ne rabijo lastne IKT, ki jo v ra unalni-kem oblaku nudi GSV, ampak le:

- IKT, ki jo za potrebe de-ifriranja -ifriranega prometa zahteva InfoSec ó -ifrirna naprava, pofarna pregrada in delilniki prometa oziroma opti na stikala;

- z optimi kabli povezani optično stikalo in delovne postaje, in
- tanke kliente (delovne postaje brez trdega diska, operacijskega sistema in uporabniških programov), ki pa vsak ni vezan le na enega uporabnika.

1. faza ISV-TD

GSV je testno okolje za prvo fazo vzpostavil sredi junija, produkcijsko okolje pa prve dni septembra 2011. Prva faza ISV-TD omogoča uporabniku:

- seznanjanje z vsemi TD v ISV-TD v obsegu pomena besede (postopkovna zbirka, tekoča in stalna zbirka, zbirka elektronskih sej vlade, redne in dopisne, in delovnih teles vlade);
- seznanjanje s sklici sej in z novimi objavljenimi dokumenti na oglasni deski, in
- dajanje pripomb na oglasni deski ali preko uradnega poštne predala organa za TD (medresorsko usklajevanje, ko je gradivo fle v vladni proceduri), ki ga vsak organ dobi v svoji lastni oblaku ISV-TD (sistem ne predvideva osebnih poštnih predalov javnih uslužbencev, saj je posredovanje TD dopustno le preko uradnih poštnih predalov za ravnanje s TD).

Seveda morajo uporabniki, preden se jim odobri dostop do ISV-TD, izpolniti celo vrsto zahtev, večinoma pa se nanašajo na uredbo InfoSec, delo Komisije za informacijsko varnost, kombinacija obeh pa na zahteve skrbnika ISV-TD. Nekaj (res) osnovnih zahtev:

- ministrstvo ali vladna služba (organ) razpolagata z ustrezno IKT (TEMPEST lahki odjemalci, optična povezava, ...);
- organ postavi ključno oziroma kritično IKT (šifrirna in poštna naprava, tiskalnik) v varnostno območje (sklep predstojnika organa o vzpostavitvi VO, izjava o primernosti Urada za varovanje tajnih podatkov) in v ustrezno TEMPEST omaro ali TEMPEST sobo;
- organ ima vzpostavljeno primerno informacijsko varnostno politiko, in
- uporabniki imajo dovoljenje (clearance) za dostop do TD, ob tem pa izpolnjujejo vse kriterije potrebe po vedenju;

S prvo fazo je GSV dosegel, da je, v skladu s Polovnikom Vlade Republike Slovenije (PV), z objavo v ISV-TD izpolnil zahtevo PV po seznanitvi organov z vladnimi dokumenti, omogočil takojšnjo odzivnost organov (dajanje pripomb v samem ISV-TD) in odpravil potrebo po zaposlovanju tiskarjev ali kurirjev-voznikov. Seveda se je obremenjenost informatikov skoraj podvojila (ob ISV-TD je bilo treba zagotoviti tudi celovito informacijsko podporo pripravi in izvedbi sej vlade in delovnih teles vlade), o zaposlovanju pa kdaj drugi ...

2. faza ISV-TD

Z rezervacijo spomina na diskih GSV in nastavitvijo uradnih poštnih predalov organov za delo s TD, je GSV v drugi fazi omogočil organom,

- da oblikujejo in hranijo lastne dokumente in pregledne na trdem disku v svoji lastni oblaku GSV (GSV skrbi, skladno z lastno informacijsko varnostno politiko za ustrezen način in zahteve (RAID 5+, dnevno varnostno kopiranje, ...), in

- elektronsko izmenjavo dokumentov med organi v ISV-TD (običajno izmenjevanje tajnih podatkov, medresorsko usklajevanje, í).

Tudi druga faza je operativna od začetka septembra 2011.

3. faza ISV-TD

GSV je v lastni ISV-TD vključil celovito ravnanje s TD, od oblikovanja lastnih dokumentov, evidentiranja, razvrščanja in dodeljevanja v reševanje lastnih in vhodnih dokumentov, do elektronskega razdeljevanja, reševanja zadev in predaje rešenih zadev v elektronski arhiv. Se pravi, tudi v »tajnem« svetu je, tako kot v navadnem, informacijsko podprt celoten življenjski cikel dokumenta ó upoštewane so tako zahteve Uredbe upravnem poslovanju (UUP), kot Zakona o varstvu dokumentarnega in arhivskega gradiva in arhivih (ZVDAGA).

S tretjo fazo razvoja ISV-TD pa imamo v mislih celovito rešitev upravljanja elektronskih dokumentov tudi v organih vključeni v prvo in drugo fazo ISV-TD. Sistem namreč organom omogoča dostop do dokumentov v vladni proceduri, omogoča oblikovanje lastnih dokumentov, pošiljanje dokumentov v vladno proceduro ali drugim organom, ne omogoča pa tistega klasičnega (lastnega) upravljanja dokumentov ó evidentiranje, razvrščanje, dodeljevanje v reševanje, í , pravzaprav vse, kar razumemo pod pojmom SEUD ó sistemi za elektronsko upravljanje (elektronskih) dokumentov, oziroma »po domače«, program SPIS4, ki je pretežno v uporabi v vseh organih DU.

Za zakonsko (UUP, ZVDAGA) skladno ravnanje s TD bi organi morali vzpostaviti celovito IKT ó strefnike (poštni, podatkovni), lastno omrežje, sistemske in uporabniške programe, torej vse, kar je sicer že pri vzpostavitvi ISV-TD. Brez veliko dodatnih stroškov (morda le participacija pri stroških skupne IKT), lahko v tem delu na pomoč priskoči GSV in na obstoječi IKT oblikuje »enoten zasebni oblak« storitev za vsak organ posebej (SUED-ZO).

SUED-ZO se lahko že v tem trenutku vzpostavi za vsak organ, ki to želijo izraziti in je pripravljen storitev tudi finančno in/ali kadrovske podpreti. SUED-ZO sestavljajo zbirke (oziroma podpira procese):

- SPIS4 (tipi na postavitve, pripravljena za GSV za ravnanje s TD) ó podpira procese, predpisane z UUP in ZVDAGA, pretvorbo dokumentov v obliko za dolgoročno hrambo (PDF-A), elektronsko podpisovanje s spletno komponento ProXSign, omogoča reševanje zadev s prenosom v tekočo zbirko in ponovno aktivacijo zadev;
- eArhivi ó podpira procese priprave in pretvorbe dokumentarnega in arhivskega gradiva (DAG) v obliko za dolgoročno hrambo (PDF-A), prenosa v stalno zbirko, odbiranja in predaje arhivskega gradiva v Arhiv RS. Celovito rešitev je GSV pripravil za ravnanje z običajnimi dokumenti in zadevami, v celoti pa je uporabna (in jo uporablja) tudi za TD.
- Varnostno arhiviranje in hramba DAG na različnih lokacijah.

SUED-ZO ne podpira priprave predlogov predpisov (IPP), saj se centralni modul (CM) in Register predpisov Slovenije (SPS) nahajata v nezdruffljivem »oblaku«.

Do SUED-ZO lahko ministri dostopajo tudi na seji vlade v času, ko se obravnavajo točke s TD, oziroma celo sejo, če se bo za »tajni« na in obravnave vseh točk odločil predsednik vlade. V drugem primeru pomeni, da ministri nimajo do osebne pošete, zbirk na strefnikih organa in interneta, saj je ta del v nezdruffljivem (ne-tajnem) delu.

Sofinanciranje 3. faze ISV-TD

Z vzpostavitvijo ISV-TD (1. in 2. faza) je GSV izpolnil zahteve, ki jih GSV nalaga Poslovnik vlade o seznanjanje in omogoanje dela ministru ali direktorju vladne službe, drflavnemu sekretarju in –e nekaterim poimenovanim posameznikom, za morebitno –iritev uporabe sistema, pa se zahteva sovlaganje v skupno IKT ali zdrufljevanje namenskih sredstev vseh organov o za »nadstandard«, se pravi, v primeru, da organ rabi ve navideznih uporabnikov, pa bo treba sovlagati v IKT GSV (vsak uporabnik zahteva kar precej navideznega spomina, stro-ki pa se dajo dovolj natan no tudi izra unati).

Glede na to, da je SPIS4 brezpla en, treba ga je znati le namestiti in prilagoditi za vsako organ posebej o vsak organ si lahko sam pripravi repliko rednega SPIS4 ter pobri-e postopkovno in teko o zbirko, dostavi zbirke GSV (tudi signirni na rt, pa –ifrante in na rt klasifikacijskih znakov), GSV pa zbirke naloffi v direktorij organa (vsak organ ima svojega) na novem navideznem DOMINO strefniku. Stro-ki v zvezi z aplikacijo se pojavijo –ele pri teko em vzdrfljevanju in dograjevanju. Glede na to, da zunanji izvajalec ne bo imel oddaljenega dostopa ampak bo moral vse posege na zbirkah opravljati na GSV, prav tako pa se bo za zagotavljanje delovanja celotnega sistema tro–ilo veliko asa sistemskih inflenirjev GSV, bo treba tudi ta del stro–kov kot storitev zara unati organu o ta stro–ek je seveda neodvisen od –tevila uporabnikov.

Edini omembe vreden stro–ek tretje faze je stro–ek »raz–irjene« uporabe. Z uvajanjem SUED-ZO se pojavi potreba po ve jem –tevilu uporabnikov, kot jih predpisuje sam Poslovnik vlade, edina omembe vredna stro–ka pa sta uporaba strefni–kega spomina, ki ob trenutnih cenah predstavlja kak–nih 1.000 EUR za celotno flivljenjsko dobo strefnika (4-5 let) in licenca za vsakega uporabnika za navidezno delovno postajo.

Prednosti dopolnjenega ISV-TD

S predlaganim pristopom:

- zagotovo zmanj–amo stro–ke organov (enostavno se da izra unati, koliko vsak organ stane vzpostavitve lastnega omreflja za ravnanje s tajnimi dokumenti (predvsem gre tu za strefnike, sistemske in uporabni–ke programe);
- GSV zagotavlja skladnost SUED-ZO z UPP in ZVDAGA, od nastanka e-dokumenta do dolgoro ne hrambe v stalni ali arhivski zbirki;
- tak pristop zagotavlja ve jo varnost tajnim e-dokumentom. Tajni dokumenti se nahajajo le na enem mestu, za vse tajne dokumente velja enotna za–itna shema in ista informacijska varnostna akreditacija;
- izvedljivost: do konca leta 2011 (oziroma pol leta po zaklju ku prvih dveh faz ISV-TD).

Pomanjkljivosti takega koncepta

V predlaganem sistemu ni prostora za posami ne »eksoti ne« programe ali platforme, ki ne delujejo na precej skr enem naboru sistemskih in uporabni–kih programov in orodij. Glede na to, da so uporabniki navajeni na MS Office, bo prehod (verjetno do konca leta 2012) na odprto-kodne re–itve zagotovo povzro al nekaj nejevolje.

DODATNE MOŽNOSTI, KI JIH NUDI IKT ISV-TD

V ISV-TD, oziroma na vzpostavljeno informacijsko infrastrukturo za ravnanje s TD (pri tem gre predvsem poudarek strežnikom, zbiranim povezavam, centralnemu nadzoru nad poštarnimi pregradami) je možno enostavno dodati tevilne storitve, ki se nanašajo na ravnanje s tajnimi dokumenti, ob predpostavki, da za delovanje uporabljajo programsko infrastrukturo (sistemski programi), predvidno za delovanje ISV-TD in SUEB-Z(O) s ESX, Linux, VMware, DOMINO, LotusNotes, OpenOrg. Od primernih se mi prvenstveno zdi Sporoilni sistem diplomatsko-konzularnih predstavnikov (DKP) in Ministrstva za zunanje zadeve, bolj poznan kot Depeni sistem (DS), seveda pa se da s kratko analizo procesov in potreb organov priti do nekega minimalnega nabora potreb, ki jih je smiselno reševati z opisanim rešitvovom v oblaku GSV.

LITERATURA IN VIRI:

- (1) Fujitsu Cloud Glossary:
http://ts.fujitsu.com/it_trends/dynamic_infrastructures/cloud/glossary.html
- (2) Robert Dukari, Matjaž B. Juri: Vloga in pomen rešitvov v oblaku
http://www.soa.si/wp-content/documents/certificates/FRISK_Dukaric_Juric.pdf
- (3) Cloud Tweaks: Cloud Computing s Demystifying SaaS, PaaS and IaaS
<http://www.cloudtweaks.com/2010/05/cloud-computing-demystifying-saas-paas-and-iaas/>

Povzetek:

Rešitvov v oblaku je koncept prostorske porazdelitve informacijske telekomunikacijske tehnologije, informacijskih storitev in programov, ki uporabniku omogoča učinkovito, enostavno in poceni reševanje problemov rešitvovke podpore procesom - na tak način je Generalni sekretariat vlade rešil tudi problem upravljanja tajnih dokumentov Vlade Republike Slovenije. V članku je avtor nakazal možnost uporabe kupljene IKT tudi za druge poslovne procese organov državne uprave.

O avtorju:

Milan Selan, magister informacijskih znanosti, se z informatiko ukvarja vse od leta 1972. Trenutno je zaposlen kot vodja Sektorja za informatiko v Generalnem sekretariatu vlade in odgovoren za informacijski sistem vlade, oblikovanje elektronskih arhivov v skladu z ZVDAGA in ETZ, informacijski sistem za podporo odločanja o zakonodajnih in drugih aktih Sveta EU in za vzpostavitev sistema za ravnanje z elektronskimi tajnimi dokumenti v skladu z uredbo InfoSec.

Summary:

Cloud computing is the concept of spatial distribution of information technology, telecommunications, information services and programs, which enables the effective, easy and inexpensive computer support problem-solving process - in this way, the General Secretariat of the Government solve the problem of managing classified documents of the Government of the Republic of Slovenia. In this paper the author indicated the possibility of using ICT, purchased for classified documents, for other business processes of state government.

About Author:

Selan Milan, m.sc of Information Science, deals with informatics since 1972. He is currently employed as a Head of the Informatics Department of the General Secretariat of the Government and responsible for the governmental information system, creation of electronic archives in accordance with ZVDAGA and UTR, for the information system to support

decisions on legislative and other acts of the EU and for establishing a system for handling classified electronic documents in accordance with the regulation of InfoSec.