*Tomislav ROZMAN**

* LANCom d.o.o., Tržaška cesta 63, SI-2000 Maribor
tomi.rozman@gmail.com

Varna shramba digitalnega dokumentarnega gradiva v skupnem varnem prostoru: celovit pogled

ROZMAN Tomislav, A Safe Storage of Digital Documents in a Shared Safe Location: a Holistic Perspective. Atlanti, Vol. 19, Trieste 2009, pp. 137-150.

Original in Slovenian, abastract in English, Italian and Slovenian, summary in English

KEY WORD: *Digital documents, safe storage, research, consortium, computer infrastructure, standards*

Organizations are nowadays producing more digital documents than ever. Organizations must store their digital documents to ensure their business continuity and to comply with the national and international laws. The studies show that only 8% of organizations can survive data-loss disaster. Documentation managers must optimize the cost of digital documents storage and also they must ensure that no digital document is lost.
The purpose of the article is to present the results of the study, which goal was to create a comprehensive view on digital documentation storage factors and needs. The factors to ensure safe storage of digital documents encompass requirements for physical building, information and telecommunication infrastructure, software, business processes, organization and standards (ZVDAGA-national law). Results of the study include factors that influence the decision to the question: "Should we lease or build our own safe storage?". Therefore, the results of the study can be directly used by organizations, which do not already have an archive for their digital documents. The study is a result of cooperation between nine Slovenian companies and it is based on real-world needs.

ROZMAN Tomislav, Una conservazione sicura dei documenti digitali in ambiente sicuro: una prospettiva olistica. Atlanti, Vol. 19, Trieste 2009, pp. 137-150.

Le organizzazioni producono al giorno d'oggi più documenti digitali che mai. Esse debbono conservare i propri documenti digitali per as-

1. UVOD

V današnjem času je poslovanje večine podjetij informacijsko podprto. Večina podjetij ima elektronsko podprte poslovne procese, kot so prodaja, nabava, skladiščenje, proizvodnja. Rezultati informacijske podpore poslovanja so raznovrstni elektronski dokumenti in zapisi, ki se nahajajo v različnih oblikah, formatih, medijih. Elektronski dokumenti torej predstavljajo srce poslovanja podjetja, brez njih podjetja ne morejo delovati. Rezultati študij kažejo, da le 6% podjetij, ki so doživela izgubo podatkov, uspe preživeti več kot 1 leto po katastrofi [11]. Vsaj večja podjetja se zavedajo, da morajo celovito pristopiti k varovanju svojih elektronskih dokumentov. Dokumentarno gradivo nenazadnje postane arhivsko, katerega varovanje ni novost in zahteva premišljene ukrepe, kar ugotavlja že dr. Klasinc v [2]. Večina se jih zaveda, da le tehnološka podpora ni dovolj, prilagoditi morajo tudi organiziranost in svoje poslovne procese. Tudi država Slovenija se zaveda pomembnosti varovanja digitalnega gradiva, kar dokazuje s sprejetjem zakonov ZVDAGA (Zakon o varstvu dokumentarnega in arhivskega gradiva in arhivih [4]) in ZEPEP (Zakon o elektronskem poslovanju in elektronskem podpisu [5]). Zaradi kompleksnega področja ni naključje, da eno samo podjetje težko pristopi k projektu izgradnje varnega prostora za shranjevanje digitalne dokumentacije. Iz tega razloga je več slovenskih podjetij oblikovalo konzorcij in izvedlo projekt, katerega namen je bil izdelati študijo za izgradnjo ali najem varnega skupnega prostora.

2. ŠTUDIJA IN PROJEKTNA SKUPINA

V projektu je sodelovalo devet organizacij (štirje naročniki, pet izvajalcev) [1]. Naloga naročnikov je bila podati zahteve za shranjevanje digitalnega gradiva v skupnem varnem prostoru in zahteve za druge skupne storitve. Ta podjetja so velika v slovenskem merilu in letno proizvedejo skupaj več kot milijon digitalnih dokumentov. Zaradi omejevanja stroškov in naložb v informacijsko infrastrukturo so prisiljena razmišljati v smeri postavitve skupnega informacijskega centra, kamor bi shranjevala digitalno gradivo. Motivacija za študijo je bilo vprašanje: ali najeti obstoječe storitve varne shrambe ali izgra-

diti svojo shrambo digitalnega gradiva?

Člani projektne skupine so večji ponudniki informacijskih in telekomunikacijskih storitev v Sloveniji. Ta podjetja so na podlagi svojih izkušenj prispevala k nastanku študije iz tehnološkega in organizacijskega vidika. Avtor članka je tudi sodeloval pri izdelavi študije v okviru izvajalca - podjetja LANCom d.o.o.. Izdelava študije je trajala osem mesecev. Končni rezultat je dokument [1], na podlagi katerega se lahko uprave podjetij sprejmejo strateške odločitve glede varne shrambe digitalnega gradiva.

2.1 Cilji študije

Cilji študije varnega sistemskega prostora s stališča podjetja izvajalcev so:

1. Pokazati, da je skupni varni prostor za e-dokumente ekonomsko ugodnejši za naročnika v konzorciju v primerjavi s samostojno izgradnjo takšnega prostora.
2. Pokazati, za katere komponente varnega prostora je smiselno da jih naročniki uporabljajo v deljenem načinu.
3. Pripraviti dobro osnovo za izvedbeni projekt in EU sofinanciranje.

2.2 Pričakovani rezultati študije

Rezultat študije s stališča podjetij - izvajalcev je idejna zasnova varnega prostora z vključenimi načrti za posamezne sklope. Načrti so na nivoju konceptualnih shem in opisane so karakteristike takšnega sistema, upoštevaje vhodne podatke o vrsti in količini podatkov, ki jih priskrbi naročnik. Rezultat študije tudi zajema seznam storitev, ki ji bi takšen prostor lahko nudil. V primeru začetnega predimenzioniranja se lahko neuporabljen del varnega prostora ponudi tudi kot center za gostovanje IT storitev ali ASP (Application Service Provider) center za zunanje stranke.

Študija vsebuje pod-sklope:

- skupne dolgoročne razvojne vizije konzorcija za varni prostor,
- opredelitev arhitekturnih nivojev,
- opredelitev razpoložljivih sistemov in možnih rešitev po arhitekturnih nivojih (komunikacijski podsistem v prostoru, strežniški nivo, pomnilniški podsistem, sistem za arhiviranje/backup, nadzorni sistem, nivo navideznih strežnikov, nivo OS, nivo namenske programske opreme, nivo vzdrževanja in nadzora),
- ekonomski, varnostni in ekološki vidiki skupnega varnega sistemskega prostora (ekonomski: ocenitev cene strojne in programske opreme, ekološki: varčevanje z energijo na strežniškem nivoju s pomočjo virtualizacije in kako to sovpada s strategijo Green-IT)
- nabor in opis predvidenih storitev (varnostne kopije, rezervni center, arhiviranje,…)
- procesni model izvajanja in upravljanja storitev (osnova je Service Desk oz. Operations management po ITIL),
- opis in analiza politik licenciranje programske opreme (operacijski sistem, virtualizacijske tehnologije, oprema za arhivi-

sicurare una continuità nelle loro attività e per conformarsi alle leggi nazionali ed internazionali. Gli studi dimostrano che solo l'8% delle organizzazioni possono far fronte ad una perdita dei dati. Coloro che gestiscono la documentazione debbono ottimizzare i costi della conservazione dei documenti digitali ed anche assicurare che nessun documento venga perduto. Scopo dell'articolo è di presentare i risultati di uno studio il cui obiettivo era di creare un sguardo d'insieme onnicomprensivo sui fattori ed i bisogni della conservazione della documentazione digitale. I fattori per assicurare una conservazione sicura dei documenti digitali comprendono esigenze relative agli edifici, infrastrutture informatiche e di telecomunicazione, software, processi commerciali, organizzazione e standard (ZVDAGA – legge nazionale). I risultati di tale studio includono i fattori che influiscono sulla decisione relativa alla domanda: "Dobbiamo prendere in affitto il nostro deposito o costruirlo ex novo?". Così, i risultati dello studio possono venir direttamente utilizzati dalle organizzazioni che non possiedono un archivio per i documenti digitali. Questo studio è il risultato di una cooperazione tra nove compagnie slovene ed è basato sui bisogni effettivi.

ROZMAN Tomislav, Varna shramba digitalnega dokumentarnega gradiva v skupnem varnem prostoru: celovit pogled. Atlanti, Zv. 19, Trst 2009, str. 137-150.

V organizacijah količina e-dokumentacije narašča hitreje kot kadarkoli prej. Podjetja so dolžna hraniti e-dokumentacije predvsem zaradi zagotavljanja kontinuitete poslovanja, poleg tega so zakonsko primorana k dolgotrajni hrambi e-dokumentacije. Študije kažejo, da le 6% organizacij preživi nesrečo, v kateri so izgubili vse e-dokumente o svojem poslovanju. Ob tem so skrbniki e-dokumentacije postavljeni pred dilemo, kako optimizirati stroške in hkrati zagotoviti dolgotrajno in zanesljivo shrambo za pomembno digitalno dokumentarno gradivo podjetja.
Namen članka je predstaviti rezultate študije, katere cilj je bil osvetliti problematiko varnega shranjevanja digitalnega gradiva z vidika večjih podjetij, ki letno proizvedejo skupaj več milijonov e-dokumentov. Rezultati študije obsegajo celovit pregled problematike varne shrambe e-gradiva: od fizične infrastrukture (prostor, napajanje, klimatizacija, varnost), računalniške in telekomunikacijske infrastruk ture,programske opreme, poslovnih procesov, organizacije in standardizacije (ZVDAGA). Rezultati študije vsebujejo smernice, kateri faktorji vplivajo na odločitev o najemu ali izgradnji lastnega varnega prostora. Ker odločitev o izgradnji ali najemu varne shrambe ni trivialna, so rezultati študije neposredno uporabni za organizacije, ki se šele odločajo o zunanji varni shrambi e-dokumentov. Študija je nastala v okviru konzorcija devetih podjetij

in bazira na realnih potrebah iz prakse.

SUMMARY

Organizations are nowadays producing more digital documents than ever. Organizations must store their digital documents to ensure their business continuity and to comply with the national and international laws. The studies show that only 6% of organizations without safety policy for storing digital documents can survive data-loss disaster. Documentation managers must optimize the costs of digital documents storage and also they must ensure that no digital document is lost. This is no trivial task especially when the budget for information technology is limited.
The purpose of the article is to present the results of the study, which goal was to create a comprehensive view on digital documentation storage factors and needs. The factors to ensure safe storage of digital documents encompass requirements for physical building, information and telecommunication infrastructure, software, business processes, organization, standards(ITIL) and laws (ZVDAGA and ZEPEP-national law). The study is a result of cooperation between nine Slovenian companies and it is based on real-world needs and requirements. Four companies of consortium are customers – producers of digital documents and they provided requirements for unified safe storage location. The study was designed by five IT companies, which are familiar with the technology and its limitations. The customer companies provided the following data: number of documents produced / year, storage requirements, format of the documents, type of information systems that produce digital documents, retrieval requirements (speed, security) and integration requirements. Based on this data, the authors of the study designed the concept of safe document location from business process perspective to physical infrastructure perspective. Results of the study include factors that influence the decision to the question: "Should we lease or build our own safe storage for digital documents?". Therefore, the results of the study can be directly used by organizations, which do not already have an archive for their digital documents.
We should not forget that some certified providers for safe storage of digital documents already exist. Evaluation of such providers and comparison of our own cost model with cost models of existing providers was also performed. We have found out that there are only minor cost differences between rent or build model for the five year simulation. As the price is not the only deciding factor, other possible positive factors of the shared storage of digital documents were examined. The positive sides of building shared digital archive in comparison with renting existing one are: no vendor lock-in, no hidden costs, no price changes, fixed service level agreements and less limited future services. The best possible ap-

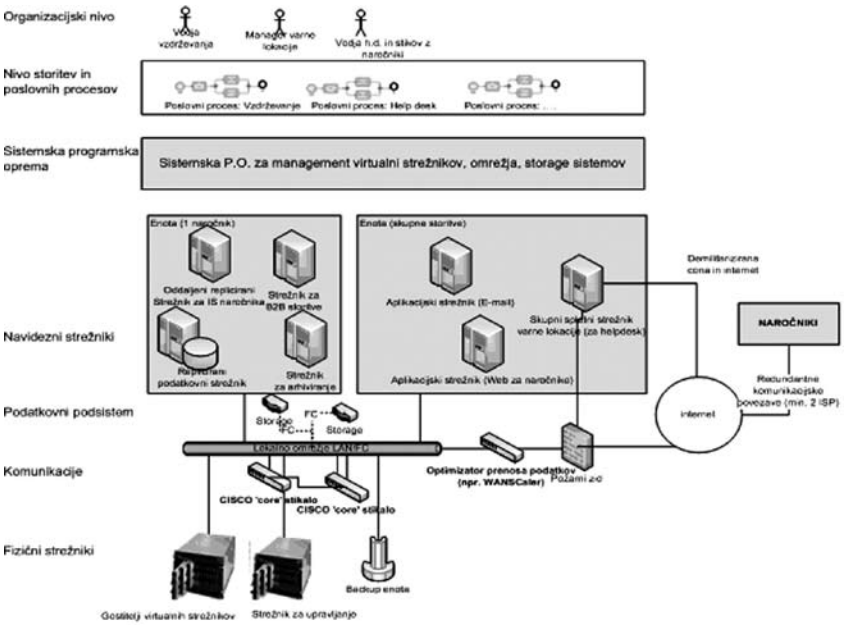
ranje, podatkovna baza),

- politika vzdrževanja in upravljanja varnega prostora (matrika vključenih vzdrževalnih storitev in odzivnih časov, ekonomsko ovrednoteno) in primer SLA (Service Level Agreement) [12],
- opredelitev in okvirna analiza možnosti mreženja podjetij in raziskovalnih organizacij, ki delujejo na ožjem tehnološkem področju.

3. OPREDELITEV ARHITEKTURNIH NIVOJEV VARNEGA PROSTORA E-GRADIVA IN DRUGIH E-STORITEV

V okviru študije smo opredelili arhitekturne nivoje varne lokacije. Pri tem smo uporabili OBASHI [13] metodologijo. Arhitektura varne lokacije je sestavljena iz nivojev:

0. Varen sistemski prostor
1. Fizični strežniki
2. Komunikacijski podsistem
3. Podatkovni podsistem
4. Navidezni strežniki
5. Sistemska programska oprema za nadzor omrežja, podatkovnega podsistema, strežnikov in navideznih strežnikov
6. Nivo storitev in poslovnih procesov
7. Organizacijski nivo



Slika 1. Arhitekturni nivoji - konceptualni nivo

V nadaljevanju opišemo zahteve za opredeljene logične nivoje skupnega varnega prostora.

3.1 Organizacijski nivo

Organizacijska struktura skupnega varnega prostora za digitalno gradivo mora ne glede na to, kakšne storitve ponuja naročnikom, vsebovati delovni mesti: vodja rezervne lokacije in tehnična podpora. V primeru, da skupni varni prostor zagotavlja varno shrambo e-gradiva, mora zaposlovati tudi skrbnika arhiviranja.

3.2 Poslovni procesi

Zaposleni v skupnem varnem prostoru morajo vzpostaviti in izvajati vsaj dva poslovna procesa: vzdrževanje in help-desk/klicni center. Procesa 'vzdrževanje' in 'klicni center' zagotavljata, da varna lokacija deluje nemoteno in da so zahteve naročnikov glede tehnične pomoči in zahtevkov za podporo zadovoljene. V primeru, da skupni varni prostor zagotavlja varno shrambo e-gradiva, mora izvajati tudi poslovne procese: izvajanje arhiviranja, priključitev naročnika v sistem, obnova / vrnitev podatkov iz arhiva.

3.3 Aplikacije

Skupni varni prostor za nemoteno delo uporablja računalniška orodja in aplikacije za podporo delovanja. Na najnižjem nivoju potrebujemo programsko opremo za nadzor delovanja tehnološke opreme (strežnikov, omrežja, diskovnega podsistema in arhivskega sistema). Primer takšne sistemske programske opreme je: programska oprema za nadzor navideznih strežnikov (System Center - Microsoft ali VMWare nadzorna programska oprema), programska oprema za nadzor komunikacijskega pod-sistema (CISCO management SW) in programska oprema za nadzor podatkovnega podsistema (npr. HP OpenView).Poleg te opreme je potrebno zagotoviti programsko opremo za HelpDesk/Klicni center, s pomočjo katere zaposleno osebje sledi zahtevkom naročnikov. Primer programske opreme za klicni center: Microsoft CRM (Customer Relationship Management) v kombinaciji z Microsoft OCS (Office Communication Server) strežnikom. Poleg tega je potrebno zagotoviti programsko opremo za nadzor arhiviranja (na strani varne lokacije) in programske dodatke (agente) na strani naročnika. Agenti predstavljajo specialno programsko opremo oziroma vmesnike, ki zagotavljajo arhiviranje podatkov iz različnih sistemov naročnikov(datotečni sistemi, poštni strežniki, podatkovne baze, poslovni informacijski sistemi, dokumentni informacijski sistemi, intranet/internet portali).

3.4 Sistem - virtualni sloj

Delovanje aplikacij v skupnem varnem prostoru omogoča sistemska programska oprema. Najnovejši trendi in razvoj na področju informacijske tehnologije vriva med nivo strojne opreme in operacijskih sistemov tako imenovane 'navidezne gostitelje' (virtual hosts). Tehnologije virtualizacije oziroma ločitev operacijskega sistema od strojne opreme povzroči več ugodnih učinkov, kot so enostavno seljenje navideznih strežnikov, odpornost proti okvaram strojne opreme, lažje vzdrževanje in predvsem neodvisnost od strojne opreme [3]. V primeru odpovedi na primer pomnilnika se lahko naš arhivski strežnik samodejno preseli na drug fizični strežnik brez izgube arhivskih podatkov. Primeri programske opreme za navidezne strežnike so: Microsoft Hyper-V, VMWare ESX ali ESXi, CITRIX-XEN, KVM, VirtualBox in sorodni. Virtualizacijo operacijskih siste-

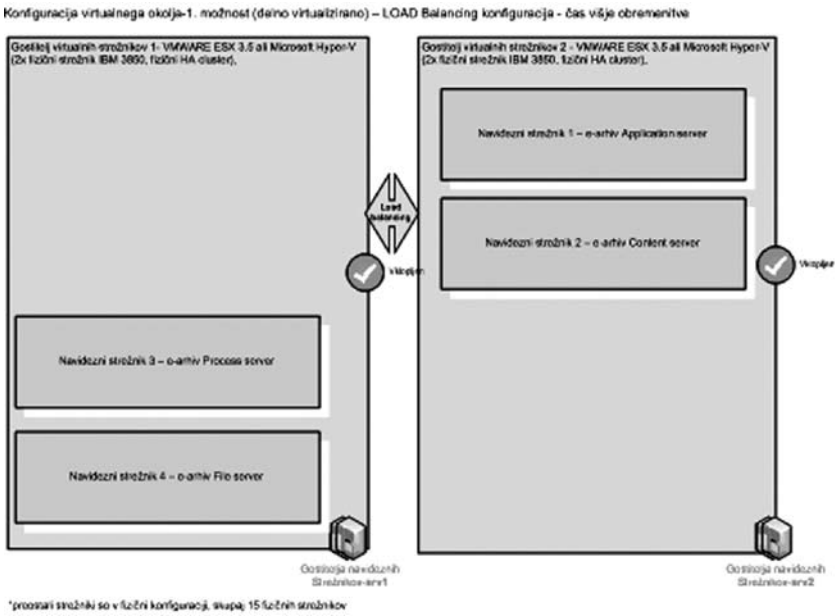
proach is a hybrid: renting a existing Lampertz room with shared IT infrastructure, applications, services and personnel on top. For the core IT infrastructure, the certified servers, storage systems, network infrastructure should be used. Such infrastructure should be build with 'no SPF (Single Point of Failure)' in mind, which means that servers, storage systems, archive systems and network equipment should be redundant and cluster-aware. To prevent data-loss, minimum two remote locations on different tectonic plates should be rented and equipped. The virtualization technologies should be used to minimize the risk of hardware failure. The virtualization of servers ensures that we can replace hardware servers with new ones without the modification or reinstallation of, for example, archive server. The software used in such data centre must also be certified and ensure connectivity with customer's document systems. Shared data centre should also have well-defined business processes, at least: service and help desk, maintenance, incident management. All mentioned levels must be compliant with national laws. If we sum it up, the decision of building data centre for one company is trivial: no, existing services should be used. But, if several similar companies want to rent a data centre services, the construction of the shared data centre can be viable option.

mov lahko vpeljemo na več načinov. V nadaljevanju pričujoče študije predstavljamo tri predloge virtualizacije, ki se razlikujejo v stopnji virtualizacije, ceni, potrebnem številu fizičnih strežnikov in zanesljivosti delovanja.

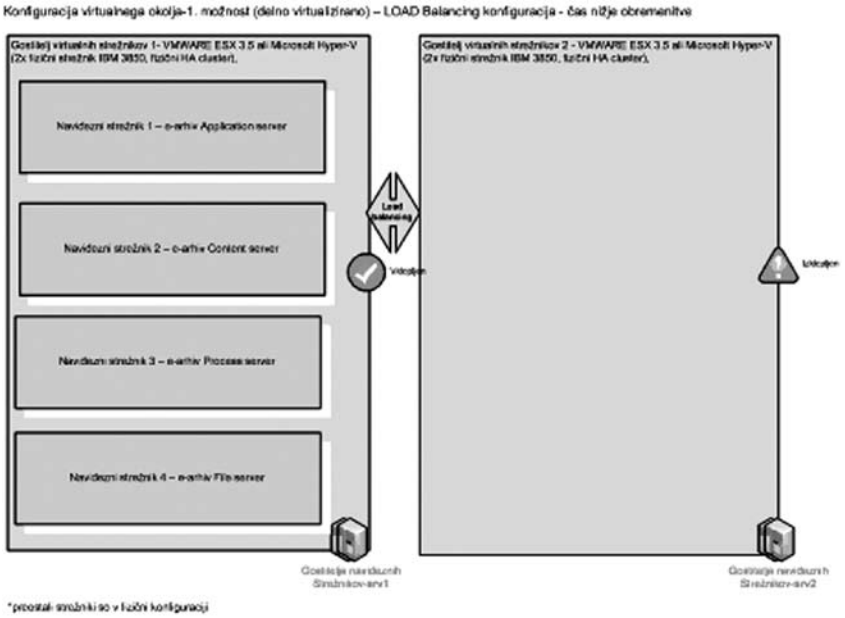
3.4.1 Virtualizacija sistema, prva možnost

Pri tej možnosti namenimo dve fizični strežniški gruči kot gostitelja virtualnih strežnikov za potrebe e-arhiva. Strežniški gruči sta postavljena v načinu samodejnega razporejanja bremena, kar pomeni, da se v času manjše obremenitve virtualni strežniki samodejno preselijo na eno fizično strežniško gručo, pri čeme se druga strežniška gruča izklopi in s tem varčuje energijo. Iz performančnega vidika je to najzmogljivejša izmed treh predlaganih postavitev.

Preostali strežniki (Slika 7) so v fizični postavitvi.



Slika 2. Virtualizacija, 1. možnost, višja obremenitev

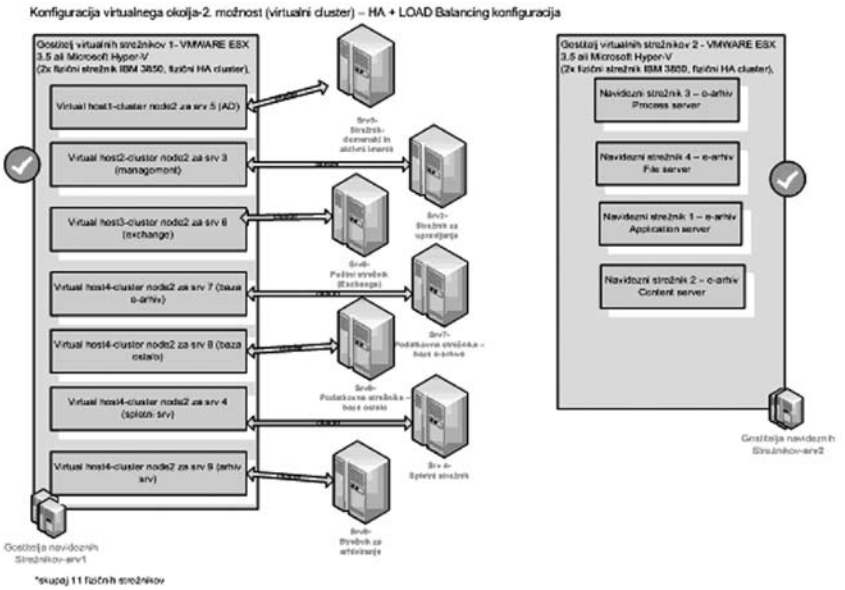


Slika 3. Virtualizacija, 1. možnost, nižja obremenitev

Pri tej postavitvi predvidevamo petnajst fizičnih strežnikov.

3.4.2 Virtualizacija okolja, druga možnost

Ta možnost predstavlja višjo stopnjo virtualizacije kot prva možnost. V tem primeru vse fizične strežniške gruče postavitve (Slika 7) nadomestimo s kombinacijo gručne postavitve fizični-virtualni. Ta postavitev zahteva enajst fizičnih strežnikov. Ta postavitev predstavlja zelo dobro razmerje cena-zmogljivost. Cena postavitve je glede na prvo možnost nižja za 15%.



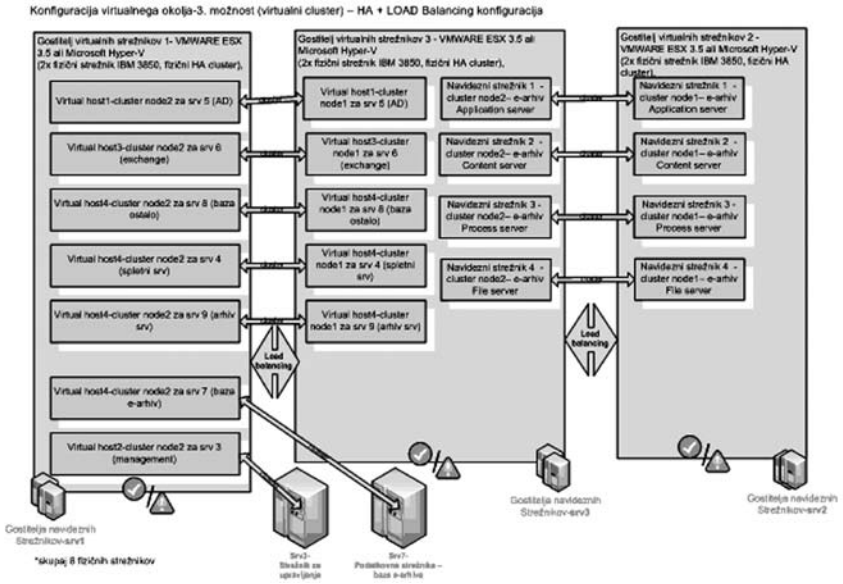
Slika 4. Virtualizacija - 2. možnost

3.4.3 Virtualizacija okolja, tretja možnost

Tretja predstavljena možnost predstavlja najvišjo še priporočljivo stopnjo virtualizacije. Pri tej konfiguraciji predvidevamo tri fizične strežniške gruče - gostitelje navideznih strežnikov (Slika 5) in še dva dodatna fizična strežnika - strežnik za upravljanje in strežnik podatkovne baze e-arhiva. Vsi ostali navidezni strežniki so nameščeni na treh gostiteljih in se glede na breme selijo med njimi. Ta varianta je cenovno najugodnejša, vendar je performančno manj zmogljiva kot druga predlagana varianta.

Pri tej postavitvi predvidevamo samo osem fizičnih strežnikov. Cena postavitve je glede na prvo možnost nižja za 20%.

Pri najvišji stopnji virtualizacije bi tudi podatkovni strežnik in nadzorni strežnik preselili v navidezno okolje, vendar glede na priporočila največjih proizvajalcev in tudi praktične izkušnje te variante ne priporočamo. Razlog tiči v omejitvah pri nižjih hitrostih vhodno/izhodnih operacij med operacijskim sistemom in podatkovnim podsistemom, kar je lahko bistvenega pomena pri arhiviranju digitalnih dokumentov. Ne glede na stopnjo virtualizacije, ki jo izberemo, je v vseh primerih potrebno upoštevati varnostne vidike [4] in jim nameniti posebno pozornost in obravnavo. Neurejena varnostna politika glede dostopa gostitelja virtualnih strežnikov lahko povzroči nenadzorovan dostop do vseh vsebovanih navideznih strežnikov in s tem tudi do digitalnega gradiva.

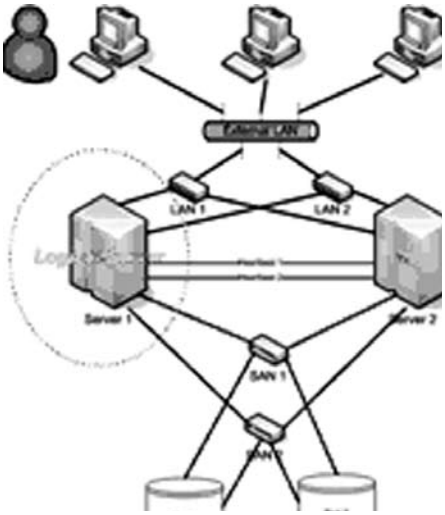


Slika 5. Virtualizacija - tretja možnost

3.5 Operacijski sistemi za skupni varni prostor

Sistemsko programsko opremo predstavlja tudi operacijski sistem. Za skupno varno lokacijo predlagamo operacijski sistem, ki ima vgrajeno podporo prej opisanim virtualizacijskim tehnologijam, kot na primer Microsoft Windows Server 2008 zaradi naprednih nadzornih funkcij. Alternativna rešitev za OS je Linux, na primer distribucija Suse ali RedHat. Priporočamo namestitev gostitelja navi-

deznih strežnikov na visoko razpoložljivem gručnem (cluster) sistemu, ki zagotavlja neprekinjeno delovanje v primeru izpada enega fizičnega strežnika.



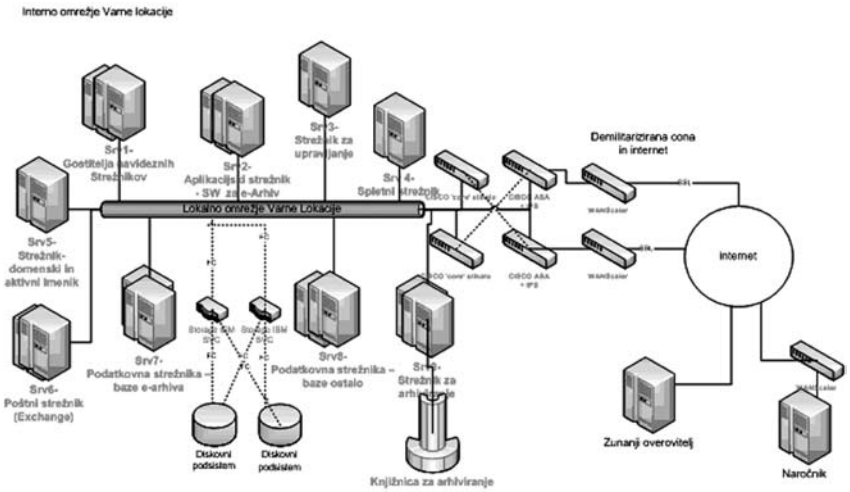
Slika 6. Primer arhitekture visoko razpoložljivege strežniške gruče (vir: Wikimedia foundation www.wikimedia.org)

3.6 Strojna oprema

Strojna oprema, ki zagotavlja delovanje programske opreme v skupnem varnem prostoru mora ustrezeti najvišjim standardom glede zanesljivosti delovanja. V tem trenutku so to IBM ali HP strežniki v izvedbi rezin (na primer HP Blade C-CLASS 8x z FC/Ethernet stikali) in podatkovni podsistem oziroma SAN (Storage Area Network) omrežje, ki ga sestavljajo diskovne kapacitete v redundančni konfiguraciji (na primer HP Storage EVA 4100). Za izvajanje varnostnih kopij podatkov uporabimo klasične ali robotizirane naprave (backup knjižnice), kot so na primer HP knjižnica MSL 2xUltrium 960 SAN.

3.7 Komunikacijski podsistem

Komunikacijski podsistem v varni lokaciji služi dvema funkcijama. Zagotavljati mora prenos arhivskega gradiva od naročnika do varnega skupnega prostora in tudi med posameznimi strojnimi komponentami v varnem skupnem prostoru. Interno omrežje v varnem skupnem prostoru je smiselno zasnovati hierarhično, z redundantnimi jedrnimi stikali (core switch). Potrebna je tudi logična ločitev pod-omrežij (VLAN-i) in prioritizacija prometa glede na zahtevnost uporabljanih storitev. Predlagamo tudi uvedbo optimizatorjev prenosa podatkov (npr. CITRIX WANScaler), ki pohitrijo prenos podatkov med naročnikom in varno lokacijo tudi do 300%. Komunikacijsko infrastrukturo med naročnikom in varnim skupnim prostorom morata zagotavljati najmanj dva ponudnika komunikacijskih poti. Primera vrsta komunikacijske poti je najeti vod ali optična povezava. Druge tehnologije (ADSL, brezžične) naj služijo le kot nadomestna komunikacijska infrastruktura v primeru izpada primarne komunikacijske infrastrukture.



Slika 7. Primer informacijske infrastrukture znotraj skupne varne lokacije - natančneje

3.8 Podporna infrastruktura

Varen sistemski prostor omogoča zaščito pred zunanjimi vplivi, ki bi lahko usodno vplivali na informacijsko tehnologijo: požar, vdor vode, elektromagnetno polje, nepooblaščen dostop, vlom.

V okviru sistemskega prostora morajo biti zagotovljeni naslednji sistemi:

- Sistem fizičnega varovanja, ki vsebuje sistem javljanja vloma, ropa, požara in profesionalno zunanjo službo za varovanje objektov.
- Sistem kontrole pristopa, ki zagotavlja dostop le pooblaščenim osebam. Te zahteve izpolnjuje sistem video nadzora, biometrični nadzor, tehtanje in primerjanje teže oseb pri pristopih/izhodih). Poleg tehničnega varovanja je potrebno zagotoviti osebno varovanje (varnostniki).
- Sistem avtomatskega gašenja požara. Varni prostor mora vsebovati aktivni in pasivni protipožarni sistem. Aktivni sistem sestavljajo iz detektorji dima, ognja in smodečih se komponent (pred- požarni senzorji). Sistem mora vsebovati tudi avtomatski sistem gašenja. Pasivni sistem zajema fizično zaščito pred zunanjim ognjem (stene). Protipožarni sistem vsebuje tudi opremo in postopke ročno gašenje in povezavo s profesionalno gasilsko službo.
- Sistem klimatizacije prostora z zagotovljeno redundanco. Zveza ASHRAE (American Society of Heating, Refrigerating and Air Conditioning Engineers) priporoča sledeče karakteristike za klimatiziranje podatkovnih centrov: Temperatura 20-25oC, vlažnost 40-55%, stopnja rosišča 17oC. Odstopanja od teh priporočil lahko povzročijo kondenzacijo vlage na električnih in elektronskih komponentah oziroma statično naelektritev. Zaradi olajšanja zagotavljanja primernih klimatskih razmer se priporoča podzemna izvedba prostora, predvsem zaradi manjše porabe energije.
- Sistem napajanja sestoji iz enega ali več UPS sistemov in generatorjev električne energije. Priporoča se popolnoma po-

dvojen sistem neprekinjenega napajanja. Kritični strežniki morajo biti priklopljeni na dva vira napajanja, ki sta na ločenih fazah. Sistem mora vsebovati napetostna stikala, ki avtomatsko preklopijo napajanje v primeru izpada ene veje.

- Konstrukcijske značilnosti. Zaradi boljše cirkulacije zraka se priporoča izvedba dvignjenih tal (za 60cm - 100 cm), sestavljena iz odstranljivih panelov. Dvignjena tla so namenjena tudi za napeljavo električnih in / ali podatkovnih kablov. Tla morajo biti pokrita z antistatično prevleko. Pozornost je potrebno nameniti statični obremenitvi tal: teža opreme je lahko tudi 1000kg/m2. Za namestitev strežnikov se priporočajo strežniške omare (rack). Primer varnega sistemskega prostora je varnostna kletka Lampertz.

Slika 8. Varna celica tipa Lampertz (vir: www.lampertz.com)

4. EKONOMSKI, VARNOSTNI IN EKOLOŠKI VIDIKI SKUPNEGA VARNEGA SISTEMSKEGA PROSTORA

4.1 Ekonomski vidiki skupnega varnega prostora

Skupni varni prostor nedvomno prinaša ekonomske prednosti. Ekonomske prednosti so očitne zaradi razlogov:

- Naročniki delijo fizični prostor za strežniško ter ostalo infrastrukturo
- Naročniki delijo stroške porabe električne energije in telekomunikacij
- Naročniki delijo stroške zaposlenih v varnem prostoru, zaradi tega lahko zmanjšajo število zaposlenih v lastnem IT oddelku
- Naročniki prihranijo pri stroških vzdrževanja lastne informacijske infrastrukture

Ekonomski vidik z največjo težo je seveda varovanje poslovnih informacij in podatkov naročnikov. Študije kažejo, da le 6% podjetij, ki izgubi podatke, vzpostavi normalno delovanje v roku enega leta.

Zgornje trditve potrjujejo naslednja dejstva [1]:

- neprekinjeno poslovanje zaradi učinkovitega varovanja poslovnih listin in podatkov naročnikov (študije kažejo, da le 6% podjetij preživi izgubo podatkov),
- posamezni dokument v povprečju kopiramo 9 - 11 krat (fizično ali elektronsko),
- cena fizičnega arhiviranja je zelo visoka (strošek prostora, slaba učinkovitost osebja - 25% časa predstavlja zgolj hoja po arhivu),
- 3 - 5% vseh dokumentov se ali zgubi ali napačno arhivira,
- iskanje ali upravljanje informacij, ki se nahajajo v raznih arhiviranih dokumentih, zahteva v povprečju 20-30% delovnega časa osebja,
- porazdelitev stroškov zaposlenih v skupnem varnem prostoru (skupno kadrovanje),
- nižji stroški zaposlenih v lastnem IT oddelku (zmanjšanje obsega lokalnih storitev),
- porazdelitev stroškov vzdrževanja informacijske infrastrukture skupnega sistemskega prostora,
- nižji stroški vzdrževanja lastne informacijske infrastrukture (zmanjšanje obsega lokalnih storitev),
- občutno nižji stroški potrošnega materiala (papir, pomnilniški in tiskalniški mediji),
- večja učinkovitost zaposlenih,
- dodatni prihodki kot posledica oddaje storitev v najem zunanjim organizacijam.

4.2 Varnostni vidiki skupnega varnega prostora

Skupni varni prostor ima v primerjavi s porazdeljenimi (lastnimi) nedvomne prednosti. Podatki naročnikov so bolj varni predvsem zaradi tega, ker se varni prostor nahaja na fizično oddaljeni lokaciji in ker je zaradi več investitorjev praviloma tudi bolje zasnovan kot lastni varni prostor. Poleg tega se upravitelj varnega prostora s to dejavnostjo profesionalno ukvarja, kar tudi pripomore k večji varnosti naročnikovih podatkov.

4.3 Ekološki vidiki skupnega varnega prostora

Raziskave kažejo, da je strežniška infrastruktura v podjetjih izkoriščena manj kot 30%. Uvedba skupne strežniške infrastrukture, na kateri tečejo navidezni strežniki povzroči skoraj 100% izkoriščenost strojne opreme in s tem manjšo porabo električne energije. Tehnologije, ki so danes na voljo za upravljanje navideznih strežnikov celo omogočajo, da se v času manjše obremenitve navidezni strežniki samodejno preselijo na fizični strežnik, ki še zagotavlja njihovo normalno delovanje, neaktivni strežniki se samodejno izklopijo.

5. OPREDELITEV ZAKONODAJE NA PODROČJU RAVNANJA Z DIGITALNIM GRADIVOM

Pravna varnost hranjenja dokumentarnega in arhivskega gradiva je bistven element pri doseganju ciljev centra. Primarni nivo za zagotavljanje avtentičnosti hranjenega gradiva je upoštevanje zakonskih normativov, sprejetih tako v nacionalnem, kot mednarodnem prostoru. Šele sekundarni nivo predstavljajo visoka tehnologija, aplikativne rešitve in napredni organizacijski ukrepi za zagotavljanje avtentičnosti gradiva [1].

Za primarni nivo je s sprejetjem zakonodaje (ZVDAGA, ZEPEP, MoReq2 [10]) že poskrbel zakonodajalec, sekundarni nivo pa je v domeni centra, ki bo hranil gradivo. Kriptografija predstavlja v tem trenutku najzanesljivejši ukrep za zagotavljanje avtentičnosti digitalnega gradiva.

Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP-UPB1) [5], ureja elektronsko poslovanje, ki zajema poslovanje v elektronski obliki z uporabo informacijske in komunikacijske tehnologije in uporabo elektronskega podpisa v pravnem prometu, kar vključuje tudi elektronsko poslovanje v sodnih, upravnih in drugih podobnih postopkih, če zakon ne določa drugače.

Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih (ZVDAGA) [4], ureja način, organizacijo, infrastrukturo in izvedbo zajema ter hrambe dokumentarnega gradiva v fizični in elektronski obliki, veljavnost oziroma dokazno vrednost takega gradiva, varstvo arhivskega gradiva in pogoje za njegovo uporabo, naloge arhivov in javne arhivske službe ter s tem povezane storitve in nadzor nad izvajanjem.

Uredba o varstvu dokumentarnega in arhivskega gradiva [7], ureja delovanje in notranja pravila subjektov, ki hranijo dokumentarno, oziroma arhivsko gradivo, hrambo tega gradiva v fizični in digitalni obliki, splošne pogoje, registracijo in akreditacijo opreme in storitev za digitalno hrambo, odbiranje in izročanje arhivskega gradiva javnim arhivom, strokovno obdelavo in vodenje evidenc arhivskega gradiva, varstvo filmskega in zasebnega arhivskega gradiva, uporabo arhivskega gradiva v arhivih ter delo arhivske komisije.

Enotne tehnološke zahteve v1.0 [8]. Dokument je namenjen splošni uporabi pri zagotavljanju opreme in storitev, povezanih s hrambo dokumentarnega gradiva v elektronski obliki. Obravnava dve vrsti tehnoloških zahtev, kot so: poslovne, organizacijske in tehnološke pogoje, natančno opredeljuje notranjo organizacijo ponudnika, ki izvaja zajem ali hrambo, s poudarkom na organizacijskih delih, procesih in vlogah zaposlenih, zahteve za zagotavljanje varnih prostorov, pogoje, ki jih mora izpolnjevati strojna in programska oprema, kontrole, ki so pomembne za varnost dokumentov (dostop, kontrolne sledi, rezervne kopije, sledenje dokumentov, avtentičnost), dodatne zahteve, ki niso nujne, njihovo izpolnjevanje pa je zaželeno zaradi naprednejšega in uporabniku bolj prijaznega delovanja sistema ter večje združljivosti. Enotne tehnološke zahteve podrobneje določajo posamezne tehnične standarde, ki zagotavljajo avtentičnost in celovitost gradiva, hranjenega v elektronski obliki. Trenutno je

najzanesljivejši način zagotavljanja avtentičnosti in celovitosti gradiva pravilna uporaba kriptografskih mehanizmov.

Pravilnik o strokovni usposobljenosti uslužbencev javnopravnih oseb ter Delavcev ponudnikov storitev, ki delajo z dokumentarnim gradivom [9]. Predpis med drugim določa vsebino in obvezen preizkus strokovne usposobljenosti s področij (povzetek 3. člena): poznavanja pravnih predpisov, upravljanja z dokumentarnim gradivom v fizični in digitalni obliki, informatike (politika varovanja informacij, upravljanje z informacijskimi sredstvi, o varnosti, fizičnem in tehničnem varovanju opreme in prostorov, obvladovanje dostopa, upravljanje varnostnih dogodkov, zagotavljanje neprekinjenega poslovanja), in področje arhivistike v najširšem pomenu.

6. ZAKLJUČEK

V članku je predstavljen le kratek izvleček ugotovitev iz študije, ki kljub vsemu nakazuje zahtevnost področja varovanja digitalne dokumentacije. Študija je pokazala, da je problematika shranjevanja digitalnega dokumentarnega gradiva kompleksna in ni omejena samo na tehnološko problematiko. Glavna ugotovitev študije je, da je potrebno k reševanje te problematike pristopiti širše, kot je sama tehnologija shranjevanja. Prav tako se je izkazalo, da skupni varni prostor za več podjetij pomeni ekonomsko ugodnejšo varianto kot varni prostor v vsakem podjetju. Skupni varni prostor zaradi manjše porabe električne energije nenazadnje prispeva tudi k ekološkim smernicam današnjega časa.

7. VIRI IN LITERATURA

[1] Rozman, T., Florjanič, M., Varkonji Šajn, M., Romih, J., Brumen, A., Vrankić, D., Kejžar, T., Krajnik, G., Sernec, R., Perme, J., Hržič, R., Korošec, A., Jošt, K., Vindiš, M., Cizel, I., Planinšec, R., Mlakar, P., Tetičkovič, M., Samojlenko, D., Postavitev skupnega varnega prostora ter storitve arhiviranja dokumentov in zapisov, študija, 2009.

[2] Klasinc, P. P., Safety and Security in Archives: Many Questions, and Even More Answers, in «Atlanti. Review for modern archival theory and practice», vol. 18(2008), pp. 53-74.

[3] Mergen, M. F., Uhlig, V., Krieger, O., Xenidis, J., Virtualization for high-performance computing, in «ACM SIGOPS Operating Systems Review», Volume 40 , Issue 2, April 2006.

[4] Vaughan-Nichols, S., J., Virtualization Sparks Security Concerns, in «Computer», vol. 41, no. 8, pp. 13-15, Aug. 2008.

[5] Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih (ZVDAGA), Uradni list Republike Slovenije, št. 30/2006.

[6] Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP), Uradni list Republike Slovenije, št. 57/2000.

[7] Uredba o varstvu dokumentarnega in arhivskega gradiva, Uradni list Republike Slovenije, št. 86/2006.

[8] Enotne tehnološke zahteve v1.0, dokument Arhiva Republike Slovenije, objavljen 1.12.2006.

[9] Pravilnik o strokovni usposobljenosti uslužbencev javnopravnih oseb ter delavcev ponudnikov storitev, ki delajo z dokumentarnim gradivom, Uradni list Republike Slovenije, št. 132/2006.

[10] Model Requirements Specification for the Management of Electronic Records,spletni vir: http://www.moreq2.eu, pridobljeno dne 1.7.2009.

[11] Hoffer, Jim. Backing Up Business - Industry Trend or Event, Health Management Technology, Jan 2001.

[12] OGC, ITIL - Information Infrastructure Library (Incident Management), spletni vir: http://www.best-management-practice.com/gempdf/itSMF_An_Introductory_Overview_of_ITIL_V3.pdf, pridobljeno 1.7.2009.

[13] Wallis, P., Cloughley F., OBASHI, Wikipedia, The Free Encyclopedia, http://en.wikipedia.org/w/index.php?title=OBASHI&oldid=285546814 pridobljeno 1.7.2009.