2012 * apr/maj/jun * letnik XX

2

UPORABNA INFORMATIKA

20let

Izpitni centri ECDL

ECDL (European Computer Driving License), ki ga v Sloveniji imenujemo evropsko računalniško spričevalo, je standardni program usposabljanja uporabnikov, ki da zaposlenim potrebno znanje za delo s standardnimi računalniškimi programi na informatiziranem delovnem mestu, delodajalcem pa pomeni dokazilo o usposobljenosti. V Evropi je za uvajanje, usposabljanje in nadzor izvajanja ECDL pooblaščena ustanova ECDL Fundation, v Sloveniji pa je kot član CEPIS (Council of European Professional Informatics) to pravico pridobilo Slovensko društvo INFORMATIKA. V državah Evropske unije so pri uvajanju ECDL močno angažirane srednje in visoke šole, aktivni pa so tudi različni vladni resorji. Posebno pomembno je, da velja spričevalo v 148 državah, ki so vključene v program ECDL. Doslej je bilo v svetu izdanih že več kot 11,6 milijona indeksov, v Sloveniji več kot 17.000 in podeljenih več kot 11.000 spričeval. Za izpitne centre v Sloveniji je usposobljenih 11 organizacij, katerih logotipe objavljamo.

AGORA

IZOBRAŽEVANJE
INFORMACIJSKE STORITVE

SREDNJA GRADBENA, GEODETSKA
IN EKONOMSKA ŠOLA LJUBLJANA
1000 Ljubljana, Dunajska 102

LJUDSKA UNIVERZA
MURSKA SOBOTA

ISER

ŠOLSKI CENTER VELENJE

ŠOLSKI CENTER
Novo mesto

spin

LJUDSKA UNIVERZA CELJE
Cankarjeva ulica 1, 3000 Celje, Slovenija
Telefon:(03) 428-67-50 Telefax: (03) 428-67-58

UPI LJUDSKA UNIVERZA ŽALEC
šola prijaznih ljudi

Micro Team

U P O R A B N A
I N F O R M A T I K A
2012 ŠTEVILKA 2 APR/MAJ/JUN LETNIK XX ISSN 1318-1882

U P O R A B N A
I N F O R M A T I K A

2012 ŠTEVILKA 2 APR/MAJ/JUN LETNIK XX ISSN 1318-1882

Ustanovitelj in izdajatelj
Slovensko društvo INFORMATIKA
Revija Uporabna informatika
Litostrojska cesta 54, 1000 Ljubljana

Predstavnik
Niko Schlamberger

Odgovorni urednik
Jurij Jaklič

Uredniški odbor
Marko Bajec, Vesna Bosilj Vukšić, Gregor Hauc, Jurij Jaklič, Andrej Kovačič, Katarina Puc, Vladislav Rajkovič, Heinrich Reinermann, Ivan Rozman, Rok Rupnik, Niko Schlamberger, John Taylor, Mirko Vintar, Tatjana Welzer Družovec

Recenzenti
Marko Bajec, Marko Bohanec, Vesna Bosilj Vukšić, Dušan Caf, Srečko Devjak, Tomaž Erjavec, Matjaž Gams, Izidor Golob, Tomaž Gornik, Janez Grad, Miro Gradišar, Jozsef Györkös, Marjan Heričko, Mojca Indihar Štemberger, Jurij Jaklič, Milton Jenkins, Andrej Kovačič, Jani Krašovec, Katarina Puc, Vladislav Rajkovič, Heinrich Reinermann, Ivan Rozman, Rok Rupnik, Niko Schlamberger, Tomaž Turk, Mirko Vintar, Tatjana Welzer Družovec, Lidija Zadnik Stirn, Alenka Žnidaršič

Tehnična urednica
Mira Turk Škraba

Lektoriranje
Mira Turk Škraba (slov.)
Jelka Vintar (angl.)

Oblikovanje
KOFEIN
Ilustracija na ovitku: Luka Umek za KOFEIN

Prelom in tisk
Boex DTP, d. o. o., Ljubljana

Naklada
600 izvodov

Naslov uredništva
Slovensko društvo INFORMATIKA
Uredništvo revije Uporabna informatika
Litostrojska cesta 54, 1000 Ljubljana
www.uporabna-informatika.si

Revija izhaja četrtletno. Cena posamezne številke je 20,00 EUR. Letna naročnina za podjetja 85,00 EUR, za vsak nadaljni izvod 60,00 EUR, za posameznike 35,00 EUR, za študente in seniorje 15,00 EUR. V ceno je vključen DDV.

Revija Uporabna informatika je od številke 4/VII vključena v mednarodno bazo INSPEC.

Revija Uporabna informatika je pod zaporedno številko 666 vpisana v razvid medijev, ki ga vodi Ministrstvo za kulturo RS.

Revija Uporabna informatika je vključena v Digitalno knjižnico Slovenije (dLib.si).

Vabilo avtorjem

V reviji Uporabna informatika objavljamo kakovostne izvirne članke domačih in tujih avtorjev z najširšega področja informatike v poslovanju podjetij, javni upravi in zasebnem življenju na znanstveni, strokovni in informativni ravni; še posebno spodbujamo objavo interdisciplinarnih člankov. Zato vabimo avtorje, da prispevke, ki ustrezajo omenjenim usmeritvam, pošljejo uredništvu revije po elektronski pošti na naslov ui@drustvo-informatika.si.

Avtorje prosimo, da pri pripravi prispevka upoštevajo navodila, objavljena v nadaljevanju ter na naslovu http://www.uporabna-informatika.si.

Za kakovost prispevkov skrbi mednarodni uredniški odbor. Članki so anonimno recenzirani, o objavi pa na podlagi recenzij samostojno odloča uredniški odbor. Recenzenti lahko zahtevajo, da avtorji besedilo spremenijo v skladu s priporočili in da popravljeni članek ponovno prejmejo v pregled. Uredništvo pa lahko še pred recenzijo zavrne objavo prispevka, če njegova vsebina ne ustreza vsebinski usmeritvi revije ali če članek ne ustreza kriterijem za objavo v reviji.

Pred objavo članka mora avtor podpisati izjavo o avtorstvu, s katero potrjuje originalnost članka in dovoljuje prenos materialnih avtorskih pravic. Nenaročenih prispevkov ne vračamo in ne honoriramo. Avtorji prejmejo enoletno naročnino na revijo Uporabna informatika, ki vključuje avtorski izvod revije in še nadaljnje tri zaporedne številke.

S svojim prispevkom v reviji Uporabna informatika boste prispevali k širjenju znanja na področju informatike. Želimo si čim več prispevkov z raznoliko in zanimivo tematiko in se jih že vnaprej veselimo.

Uredništvo revije

Navodila avtorjem člankov

Članke objavljamo praviloma v slovenščini, članke tujih avtorjev pa v angleščini. Besedilo naj bo jezikovno skrbno pripravljeno. Priporočamo zmernost pri uporabi tujk in – kjer je mogoče – njihovo zamenjavo s slovenskimi izrazi. V pomoč pri iskanju slovenskih ustreznic priporočamo uporabo spletnega terminološkega slovarja Slovenskega društva Informatika Islovar (www.islovar.org).

Znanstveni članek naj obsega največ 40.000 znakov, strokovni članki do 30.000 znakov, obvestila in poročila pa do 8.000 znakov.

Članek naj bo praviloma predložen v urejevalniku besedil Word (*.doc ali *.docx) v enojnem razmaku, brez posebnih znakov ali poudarjenih črk. Za ločilom na koncu stavka napravite samo en prazen prostor, pri odstavkih ne uporabljajte zamika.

Naslovu članka naj sledi za vsakega avtorja polno ime, ustanova, v kateri je zaposlen, naslov in elektronski naslov. Sledi naj povzetek v slovenščini v obsegu 8 do 10 vrstic in seznam od 5 do 8 ključnih besed, ki najbolje opredeljujejo vsebinski okvir članka. Pred povzetkom v angleščini naj bo še angleški prevod naslova, prav tako pa naj bodo dodane ključne besede v angleščini. Obratno velja v primeru predložitve članka v angleščini.

Razdelki naj bodo naslovljeni in oštevilčeni z arabskimi številkami.

Slike in tabele vključite v besedilo. Opremite jih z naslovom in oštevilčite z arabskimi številkami. Vsako sliko in tabelo razložite tudi v besedilu članka. Če v članku uporabljate slike ali tabele drugih avtorjev, navedite vir pod sliko oz. tabelo. Revijo tiskamo v črno-beli tehniki, zato barvne slike ali fotografije kot original niso primerne. Slik zaslonov ne objavljamo, razen če so nujno potrebne za razumevanje besedila. Slike, grafikoni, organizacijske sheme ipd. naj imajo belo podlago. Enačbe oštevilčite v oklepajih desno od enačbe.

V besedilu se sklicujte na navedeno literaturo skladno s pravili sistema APA navajanja bibliografskih referenc, najpogosteje torej v obliki: (Novak & Kovač, 2008, str. 235). Na koncu članka navedite samo v članku uporabljeno literaturo in vire v enotnem seznamu po abecednem redu avtorjev, prav tako v skladu s pravili APA. Več o APA sistemu, katerega uporabo omogoča tudi urejevalnik besedil Word 2007, najdete na strani http://owl.english.purdue.edu/owl/resource/560/01/.

Članku dodajte kratek življenjepis vsakega avtorja v obsegu do 8 vrstic, v katerem poudarite predvsem strokovne dosežke.

Intervju s prvim urednikom prof. dr. Mirkom Vintarjem ob dvajsetletnici revije Uporabna informatika

Prva številka revije Uporabna informatika je izšla septembra 1993. Bili ste pobudnik za njeno ustanovitev in tudi avtor programske zasnove revije. Kaj vas je gnalo k temu? Kakšni so bili cilji? Komu je namenjena revija?

Če želimo predstaviti motive, vzgibe in okoliščine, v katerih je začela nastajati revija, potem moramo še posebno zaradi mlajših bralcev nekoliko širše orisati čas na začetku devetdesetih let in stanje informatike v tistem času; potem bo mogoče tudi lažje razumeti, zakaj smo prišli do sklepa o ustanovitvi takšne revije. V tistem času je prišlo do nekega preloma v razvoju informatike in to z več vidikov. Po eni strani je bilo konec obdobja velikih računalniških sistemov, t. i. mainframov. To lahko ilustriramo s tem, da je bil metaforični nosilec tega razvoja, podjetje IBM, takrat skoraj pred propadom. Po drugi strani pa se je začenjalo novo obdobje, ki sta ga izrazito označevala razvoj in nagla širitev uporabe osebnih računalnikov. Čeprav vemo, da so se osebni računalniki pojavili prej, pa je množični razmah osebno računalništvo doživelo konec osemdesetih, na začetku devetdesetih let. To je pomenilo, da informacijska tehnologija oz. njena uporaba ni več omejena na »steklene stolpe« in ozke skupine izbranih profesionalnih uporabnikov, temveč je tehnologija postala dostopna širokim ljudskim množicam. Postala je delovno orodje vseh zaposlenih, ki so takrat delovali v pisarniških okoljih. Hkrati ne smemo pozabiti, da je bila ravno v tem času že na obzorju tudi širša uporaba interneta.

Zdelo se mi je, da je napočil čas, ko potrebujemo revijo, ki bo spremljala vse te razvojne korake, obveščala zainteresirano strokovno javnost o razvoju na tem področju in bo postala forum za prenos znanja, idej in dobrih praks. Takrat sta v Sloveniji obstajali reviji Moj mikro, ki je bila bolj informativnega značaja, in znanstvena revija Informatica, ki jo je izdajalo Slovensko društvo INFORMATIKA. Zdelo se mi je, da potrebujemo prvenstveno strokovno revijo, ki bo zapolnila to vrzel. Sam sem že takrat menil, da bi morala to biti ne le strokovna, temveč strokovno-znanstvena revija, ki bi tako postala tudi most za pretok znanja in idej med akademsko sfero in prakso. Zato smo že na začetku želeli vključiti v oblikovanje in potem v razvoj revije tako učitelje, strokovnjake, ki delujejo na slovenskih univerzah, kot tudi čim več praktikov. Hkrati smo potrebovali poleg znanstvene revije Informatica, ki je izhajala v angleškem jeziku, tudi revijo, ki bo segala v znanstveni prostor in objavljala prispevke tudi v slovenskem jeziku.

To začetno idejo in predlog o izdajanju revije sem predstavil na enem od srečanj informatikov, ki jih je dolga leta v Grimščah organiziral prof. Jože Gričar. Ideja je padla na plodna tla in že na tistem srečanju je bil sprejet sklep, da začnemo s pripravami na izdajanje revije. Imenovan je bil iniciativni odbor. Poleg mene je bila v delo takoj vključena gospa Katarina Puc, ki je bila potem tehnična urednica in za katero moram povedati, da je odigrala ključno vlogo pri nastajanju in nadaljnjem razvoju revije.

Revijo izdaja Slovensko društvo INFORMATIKA. Kakšna je bila vloga društva pri ustanovitvi revije in kasneje, v času izhajanja revije?

Tudi ob tem vprašanju je treba za razumevanje vloge društva najprej osvetliti njegov razvoj v tistem obdobju. Društvo je bilo ustanovljeno že v sedemdesetih letih, vendar je njegovo delovanje v osemdesetih povsem zaspalo. Na začetku devetdesetih smo še posebno po zaslugi gospoda Tomaža Banovca, tedanjega direktorja Zavoda za statistiko, društvo ponovno začeli postavljati na noge. Pod njegovim predsedovanjem in pomembni pomoči dr. Andreja Kovačiča smo uspeli pod okrilje društva od Zveze ekonomistov Ljubljana prenesti organizacijo vsakoletne konference Dnevi slovenske informatike, ki je še danes ena najpomembnejših aktivnosti društva. Dejavnost društva se je širila in začeli smo se spraševati, katere so primerne dejavnosti in poslanstva. Glede na to, da je razvoj stroke eno od poslanstev revije, je izvršni odbor društva pozdravil in podprl idejo o njenem izdajanju. Društvo je takrat pri pripravi in kasneje pri razvoju in izdajanju revije zagotavljalo vso potrebno pomoč, predvsem pa je ves čas zagotavljalo dokaj stabilno financiranje, kar je za razvoj izrednega pomena.

Kdo je sodeloval in še sodeluje pri ustvarjanju revije?

Omenili smo že gospoda Tomaža Banovca, ki je bil v času priprave in izdaje prve številke predsednik društva in je projekt ves čas podpiral. Gospa Katarina Puc ni bila le prva tehnična urednica in lektorica, ki je

to delo potem opravljala deset let, temveč je poskrbela tudi za vse potrebne administrativne postopke, ki so omogočili izhajanje revije, kar bi brez nje trajalo neprimerno dlje. Ko sem te dni ponovno pogledal prvo številko, sem opazil, da je vsaj tretjina članov prvotnega uredniškega odbora še vedno aktivnih, kar kaže na to, da je bil že na začetku ustvarjen »habitat«, ki ga tak projekt potrebuje za svoj dolgoročni obstoj. Sem spadajo vsi deležniki revije, ki so na koncu s kakovostno revijo poplačani za svoj prispevek: uredniški odbor, avtorji, bralci, društvo kot izdajatelj, številni recenzenti, ki so prispevali h kakovosti prispevkov, ne nazadnje pa tudi sponzorji, ki so tudi pripomogli, da je revija lahko ves čas izhajala nemoteno.

Kako je po vašem mnenju revija prispevala k oblikovanju strokovnega jezika informatike?

Poleg razvoja stroke je bila skrb za negovanje slovenskega strokovnega jezika na tem področju ena od pomembnih dimenzij ves čas izhajanja revije. Uporabna informatika je edina strokovno-znanstvena revija na področju informatike, ki dvajset let izhaja v slovenskem jeziku. Avtorji člankov morajo namesto angleških poiskati slovenske izraze ali ustvariti nove. Menim, da je bil prispevek revije na tem področju pomemben. Navsezadnje iz uredniškega kroga Uporabne informatike izhaja tudi skupina, ki že vrsto let deluje kot jedro Islovarja, terminološkega slovarja informatike, in je odigrala pomembno vlogo pri njegovem razvoju.

Prve številke revije so vsebovale štiri strokovne članke in so imele 40 strani. Zdaj je revija obsežnejša in vsebuje tudi znanstvene članke. Kako bi ocenili vsebinski razvoj revije?

Na podlagi izkušenj pri urednikovanju revije v prvem obdobju in nadaljnjem sodelovanju v uredniškem odboru lahko rečem, da so bili vedno tudi vzponi in padci. Res je, da je bila takrat revija po obsegu bistveno skromnejša, danes je obseg skoraj dvakrat večji. Tudi za kakovost prispevkov bi lahko ocenil, da je danes v povprečju na višji ravni, kar lahko v veliki meri pripišemo tudi razvoju stroke.

Vzponi in padci pa so povezani predvsem s prilivom prispevkov. Na začetku smo imeli težave s pridobivanjem prispevkov, še posebno prispevkov iz prakse je bilo bistveno manj, kot bi si želeli glede na programsko zasnovo revije. Proti koncu devetdesetih let se je stanje bistveno izboljšalo, danes pa opažam spet zmanjšanje priliva prispevkov.

Menim, da je to odraz širšega stanja strokovnega tiska v Sloveniji. Praktiki ne čutijo potrebe, da bi svoje znanje posredovali prek tovrstnih kanalov, akademska sfera pa ima drug problem: na raziskovalni agenciji in na slovenskih univerzah dajejo prevelik pomen le objavam v tujih revijah. Preverjanje raziskovalnih dosežkov v mednarodnem okolju je seveda potrebno, vendar bi morali skrbeti za pretok znanja tudi v slovenskem okolju.

Ste član uredniškega odbora revije in od blizu spremljate njeno izdajanje. S kakšnimi dilemami se danes spopada uredniški odbor? Kako danes uresničujemo glavne cilje revije?

Temeljni poslanstvi revije, ki sem ju omenil, se do danes nista bistveno spremenili, spreminjajo pa se okoliščine, prav tako se hitro razvija stroka, zato se mora uredništvo v določenem pogledu odzivati na te spremembe.

Zelo se mi zdi pomembna internacionalizacija. Podpiram pobudo za širitev uredniškega odbora s tujimi strokovnjaki, prav tako je treba pritegniti k sodelovanju več tujih avtorjev – tako praktikov kot raziskovalcev. V preteklosti smo že izdali tematsko številko, ki je bila v celoti v angleškem jeziku. Ta širitev in odpiranje v mednarodni prostor je za revijo nujna.

Pri vključevanju praktikov v delo revije smo bili le deloma uspešni že na začetku delovanja revije in tako je tudi še danes.

Kako ocenjujete spremembe na področju informatike v tem obdobju? Na eni strani se soočamo z izredno hitrim tehnološkim razvojem, spremenila se je vloga informatike v vsakdanjem življenju, podjetjih, upravi. Po drugi strani pa se zdi, da se pogosto srečujemo s podobnimi, če ne enakimi problemi kot pred dvajsetimi leti.

S to oceno se povsem strinjam. V tem obdobju se je zgodil izjemen tehnološki razvoj, ki se še posebno odraža v tehničnih karakteristikah današnjih naprav. Pred dvajsetimi leti je bila informacijska tehnologija za mnoge še bolj »modni trend«. Menedžerji so se radi slikali ob računalnikih, četudi so jih številni še malo uporabljali. Danes pa je to standardna oprema, ki je povsem vtkana v poslovanje organizacij na vseh ravneh. Zgodil se je temeljit premik od tehnoloških k poslovnim vidikom, hkrati pa se konceptualno pogosto vračamo v preteklost.

Naj ilustriram; dejstvo je, da se enaki ali podobni koncepti, ki smo jih že poznali v preteklosti, pogosto pojavljajo v novih preoblekah. Lahko dam za primer računalništvo v oblaku. V sedemdesetih in osemdesetih letih je prevladovala velika centralizacija virov preko velikih računalniških centrov. Z razvojem osebnega

računalništva pa je razvoj začel naglo korakati v smeri vse večje decentralizacije virov in procesne moči, ki je organizacijam poleg prednosti prinesla tudi številne težave. Z naglim vzponom koncepta računalništva v oblaku pa lahko rečemo, da gremo ponovno nazaj v centralizacijo virov. Vendarle se je pri tem zgodil pomemben premik, saj informatiko zdaj vse bolj razumemo kot uporabniško storitev, ki jo lahko najamemo od najugodnejšega ponudnika na trgu.

Kateri so ključni izzivi informatike danes? Katera so vprašanja, s katerimi se največkrat soočajo informatiki v poslovni praksi, in kaj so aktualne raziskovalne teme?

Ključni izzivi, s katerimi se srečujejo vodje informatike danes, so povezani s strahotno konkurenčnostjo na trgu, na katerem nastopajo podjetja – pri čemer je prav inovativna uporaba informatike v poslovanju lahko dodatna prednost organizacije –, in pa z zelo zaostrenimi finančnimi razmerami. To ima za posledico zelo trd način dokazovanja finančne upravičenosti naložb v nove rešitve, česar včasih ni bilo toliko. To predstavlja tudi nov izziv za raziskovalno sfero, ki bo morala dati večji poudarek prav razvoju metod in pristopov za lažje in boljše vrednotenje učinkov informatike, kar je bilo v preteklosti pogosto zanemarjeno.

Delujete predvsem na področju informatike v javni upravi. Kako sta gospodarska kriza in — posledično — varčevanje zaznamovala to področje? Lahko govorimo tudi o priložnostih, ki jih omogoča informatika?

V javnem sektorju lahko govorimo o zlatem obdobju razvoja e-uprave v preteklih letih. Temu področju je bila namenjena izjemna pozornost, številni politiki in vlade so prepoznali strateški pomen informatike. Informatika v javni upravi oz. e-uprava se je v prejšnjem desetletju povzpela na strateško raven in postala predmet obravnave v strateških vladnih dokumentih, kar je bila novost, saj je bila prej vedno obravnavana le na nižjih hierarhičnih ravneh odločanja. To se je odražalo tudi v velikih vlaganjih, npr. v Evropi okoli 50 milijard evrov, kar je v povprečju okrog 2,2 odstotka BDP na letni ravni, v Sloveniji pa med 100 in 120 milijoni evrov, kar predstavlja nekoliko nižji delež BDP.

Študije OECD napovedujejo za razvite države nadaljevanje teh trendov. Pametne vlade bodo prej povečevale kot zmanjševale vlaganja, saj lahko z informatiko naredimo upravo učinkovitejšo in znižujemo stroške, hkrati pa je razvita e-uprava pomemben dejavnik gospodarskega razvoja in rasti BDP.

Skrbi pa me za Slovenijo, saj so pri nas trendi zelo zaskrbljujoči. Področje nazaduje, najrazvitejši, ki smo jim bili že zelo blizu, nam spet uhajajo. Predvideni so dodatni finančni rezi, po drugi strani pa se vse bolj izkazujejo potrebe po večji učinkovitosti javnega sektorja, pri čemer je ta dejavnik – možnosti, ki jih ponuja pri tem informatika – povsem zanemarjen.

Kako vidite razvoj informatike v prihodnje? Katere spremembe bodo ključne? Kako se bodo spreminjali profili informatikov? Kako se bodo spremenila potrebna znanja?

Da se bo razvoj nadaljeval z nezmanjšanim tempom, ni nobenega dvoma. Zdi se mi, da se informatika kot stroka naglo spreminja, predvsem pa nastajajo novi profili informatikov, ki jih bomo potrebovali v prihodnosti. Po eni strani lahko ugotavljamo, da se razvoj informacijskih rešitev še bolj seli v velike razvojne organizacije, specializirane za razvoj aplikacij. Pravega razvoja v manjših organizacijah, bodisi v podjetjih, bodisi v javnem sektorju, tako rekoč ni več. Na eni strani bodo specializirana razvojna podjetja še vedno potrebovala dobro usposobljene strokovnjake, ki bodo obvladovali vse sodobne tehnologije, po drugi strani pa bomo vedno bolj potrebovali nov profil informatika, ki pa še ni čisto izoblikovan in ga tudi v naših študijskih programih nimamo povsem izoblikovanega. Gre za izrazito uporabniški profil informatika, ki bo v veliki meri sposoben ponuditi storitev podpore za rešitve, ki bodo nastajale zunaj.

In na koncu, kako bodo te spremembe vplivale na revijo Uporabna informatika? Kakšno prihodnost bi napovedali reviji glede na razvoj informacijske tehnologije in glede na spremembe v družbi?

Sem optimist. Menim, da sta poslanstvo in položaj revije danes vsaj tako pomembna kot pred dvajsetimi leti. Res pa je, da mora revija skrbno slediti prej omenjenim trendom. Z nekaterimi zadnjimi potezami se je že šlo v pravo smer, predvsem bi izpostavil nujno internacionalizacijo. Želim si, da bi revija vsaj še naslednjih dvajset let opravljala svoje poslanstvo.

Rad bi se zahvalil vsem, ki so sodelovali bodisi pri nastajanju revije bodisi pri njenem dvajsetletnem delovanju. Brez vseh teh prizadevnih posameznikov, ki jih ne bi poimensko navajal, ker bi zagotovo koga pozabil, take revije, kot jo imamo danes, zagotovo ne bi bilo. Hkrati želim sedanjemu uredniku in uredništvu veliko uspeha pri nadaljnjem urejanju revije.

Jurij Jaklič in Katarina Puc

Kvantitativni model za upravljanje informacijskovarnostnih tveganj

Rok Bojanc
ZZI, d. o. o., Pot k sejmišču 33, 1231 Ljubljana Črnuče
rok.bojanc@zzi.si; http://www.zzi.si

Izvleček

Upravljanje informacijskovarnostnih tveganj postaja čedalje bolj pomemben proces v sodobnem poslovanju podjetij. Predlagani model za upravljanje informacijskovarnostnih tveganj temelji na kvantitativni analizi varnostnih tveganj, kar omogoča organizacijam vpeljavo optimalnih varnostnih rešitev. Model je zasnovan kot standardni postopek, ki organizacijo vodi od začetnega vnosa vhodnih podatkov do končnih priporočil za izbiro ustrezne rešitve, ki zmanjšuje določeno varnostno tveganje. Pri analizi varnostnih tveganj model kvantitativno ovrednoti informacijska sredstva organizacije, njihove ranljivosti ter grožnje, ki pretijo informacijskim sredstvom. Vrednosti parametrov tveganja so podlaga za izbiro ustrezne obravnave tveganja in vrednotenje različnih varnostnih ukrepov, ki zmanjšujejo varnostna tveganja. Za posamezen varnostni ukrep določimo kazalnike donosnosti, ki omogočajo primerjavo različnih varnostnih ukrepov. Pri tem so vključene možnosti investicije v tehnološke varnostne rešitve, uvedbe organizacijskih postopkov, izobraževanja ter prenos tveganja na zunanjega izvajalca ali zavarovalnico. Model je bil preverjen z različnimi praktičnimi izračuni iz realnega poslovnega okolja.

Ključne besede: informacijska varnost, upravljanje tveganja, ocena tveganja, sistem upravljanja informacijske varnosti, kvantitativno vrednotenje, optimalna investicija.

Abstract

Quantitative Model for Information Security Risk Management

Information security risk management is becoming increasingly important process in modern businesses. The proposed model for managing information security risks is based on quantitative analysis of security risks, which enables organizations to introduce optimal security solutions. The model is designed as a standard procedure leading the organization from the initial input data selection to the final recommendations for the selection of appropriate solutions, which reduces a certain security risk. In the process of analyzing the security risks the model quantitatively evaluates the information assets, their vulnerability and threats to information assets. The values of risk parameters are the basis for selecting appropriate risk treatment and for evaluating of various security measures that reduce security risks. Economic indicators are determined for each security measure so as to compare of various security measures to each other. This includes the possibility of investment in technology security solutions, the introduction of organizational procedures, training and transfer of risk to an outsourcing provider or to the insurance agency. The model was tested using empirical examples with data from real business environment.

Keywords: information security, risk management, risk assessment, information security management system, quantitative evaluation, optimal investment.

1 UVOD

Danes podjetja poslujejo hitreje, učinkoviteje in ceneje kot kadar koli. Pri tem pomembno vlogo igrajo sodobne informacijske tehnologije, ki podpirajo njihove poslovne procese. Zaradi povečanja elektronskega poslovanja postajajo podjetja čedalje bolj odvisna od zanesljivosti in stabilnosti delovanja svojih informacijskih sistemov. Do množične uporabe elektronskega poslovanja je prišlo po zaslugi interneta kot globalnega medija za dostop do informacij in izmenjavo podatkov. Obenem pa smo priča razmahu novih groženj in nevarnosti za poslovanje podjetij. Negativne posledice mogočega napada na informacijske sisteme so lahko velike in v nekaterih primerih lahko privedejo celo do stečaja podjetja.

Informacijski varnosti v preteklosti niso posvečali veliko pozornosti. Razlog je predvsem v tem, da se je internet kot primarni globalni povezovalni medij razvijal v okolju in času, ko še ni bilo nevarnosti napadov in vdorov v računalniška omrežja. Na začetku je bil internet zaprto omrežje, ki je povezovalo le določene izbrane organizacije in ustanove. Zato

tudi ni bilo posebne potrebe po varnosti in načrtovalci omrežij se z varnostjo niso preveč ukvarjali. Hitra rast in globalizacija interneta povečujeta njegovo heterogenost in kompleksnost. Zaradi distribuiranega upravljanja in nadzora je danes internet medij, ki mu ne moremo zaupati, zato je potreba po večji varnosti postala nujnost (Bojanc & Jerman-Blažič, 2008).

Da se podjetja zavarujejo pred grožnjami, ki pretijo njihovim informacijskim sistemom, morajo vzpostaviti varnostne mehanizme, ki varujejo njihov informacijski sistem. Za uspešno izvedbo varnostnih strategij je ključno, da podjetje pozna grožnje, ki pretijo sredstvom v njihovem podjetju. Obenem se mora podjetje odločiti, katera informacijska sredstva želi varovati pred grožnjami ter v kolikšnem obsegu jih želi varovati. Pogosta varnostna tveganja v podjetju so npr. odpoved delovanja storitev, izguba ali kraja podatkov, nepooblaščen vpogled v podatke ali nepooblaščeno spreminjanje podatkov.

Pred desetletjem je bilo splošno prepričanje, da internetno okolje ni varno zaradi tehnoloških pomanjkljivosti, pomanjkanja kriptografskih tehnik, overjanja, filtriranja mrežnih paketov itd. Zato so varnostni inženirji pospešeno delali na tehničnem področju in izboljševali kriptografske algoritme, postavljali infrastrukture javnih ključev (angl. Public Key Infrastructure, PKI), izboljševali požarne pregrade itd. Raziskovalci s področja informacijske varnosti pa čedalje bolj opozarjajo, da tak pristop ne zadostuje. Informacijska varnost je namreč področje, ki se ga ne da uspešno rešiti zgolj s tehnologijo, temveč je treba upoštevati tudi ekonomski pogled (Anderson & Schneier, 2005). Podjetja, ki upoštevajo ta pogled, se tako pri odpravi mogočih težav na področju informacijske varnosti osredinjajo na to, kar je ekonomsko optimalno, namesto na to, kar je tehnično mogoče (Schneier, 2004). Ko na informacijsko varnost gledamo z ekonomskega vidika, lahko dobimo odgovore na mnoga vprašanja, na katera ne more zadovoljivo odgovoriti samo tehnologija. Taka varnostna vprašanja so npr.: Kako lahko podjetje postane varno? Katera stopnja varnosti je ustrezna? Koliko denarja naj podjetje investira v varnost? Ali podjetje vlaga dovolj denarja, da hekerjem preprečuje vdor v računalniški sistem? Ali podjetje vlaga preveč? Ali podjetje ustrezno vlaga sredstva za varnost?

Uporaba ekonomskega pristopa k obvladovanju varnostnih tveganj omogoča podjetjem vpeljavo optimalnih varnostnih rešitev. Podjetja lahko tako ocenijo posledice, ki nastanejo zaradi neuvedbe določene varnostne rešitve, ter ocenijo, katera izmed rešitev, ki jih imajo na voljo, ima najboljše razmerje med ceno in kakovostjo. Vodstvenim kadrom z dobrim poznavanjem prava in ekonomije predstavlja uporaba ekonomskega izrazoslovja boljše razumevanje problema kot pa tehnični jezik informacijske varnosti. Menedžerji lahko tako bolje razumejo investicije v varnostne rešitve, ker je povzročena škoda ob varnostnih incidentih predstavljena kot finančna izguba.

K uveljavitvi ekonomskega pogleda na informacijsko varnost je pomembno prispevalo zavedanje, da je treba na informacijsko varnost gledati kot na investicijo in ne samo kot na strošek. Ravno varno informacijsko okolje ustvarja dodano vrednost za podjetje in njegove partnerje. Enega izmed prvih okvirov analitičnega odločanja za ocenjevanje različnih politik informacijske varnosti je predstavil Soo Hoo (2000). Gordon in Loeb (2002) sta predstavila ekonomski model za oceno optimalne investicije v informacijsko varnost, ki temelji na izenačevanju mejnih finančnih koristi informacijske varnosti in mejnih finančnih stroškov zaščite. Butler (2002) predlaga metodo analize stroškov in koristi za primerjavo alternativnih varnostnih rešitev z že uvedenimi rešitvami in tako preverja, ali je mogoča bolj stroškovno učinkovita rešitev. Ryan in Ryan (2006) zagovarjata, da se korist investicije meri kot razlika med pričakovano izgubo v primeru investiranja in neinvestiranja. Bojanc in Jerman-Blažič (2008) sta predstavila izhodišča za ekonomski pristop k modeliranju upravljanja z informacijsko varnostnimi tveganji. Na teh izhodiščih so Bojanc, Jerman-Blažič in Tekavčič (2012) predstavili splošen matematični model za kvantitativno vrednotenje investicij v različne varnostne ukrepe in iskanje optimalne varnostne rešitve. Alternativna metoda, ki poskuša analizirati vlaganja v informacijsko varnost, je t. i. teorija iger (Cavusoglu, Mishra & Raghunathan, 2004). Avtorji trdijo, da tradicionalni odločitveno-analitični pristopi za vrednotenje informacijskotehnoloških investicij v varnost obravnavajo varnostne tehnologije kot črno škatlo in ne upoštevajo, da se investicija v informacijsko varnost razlikuje od drugih splošnih informacijskotehnoloških investicij. Avtorji zagovarjajo, da se pri varnosti podjetja srečujejo s strateškimi nasprotniki, ki iščejo priložnosti, da izkoristijo ranljivosti v sistemih. Zato lahko na informacijsko varnost gledamo kot na neke vrste igro med podjetji in napadalci. Teorija iger gleda interakcijo med potencialnim napadalcem in podjetjem in skuša pojasniti

primere vdorov v podjetje, pri čemer ima napadalec motiv za napad in povzroči podjetju določeno škodo. Cremonini in Martini (2005) predlagata izboljšanje ocene donosnosti investicije v informacijsko varnost z novim indeksom, ki se imenuje donosnost napada (angl. Return-On-Attacts, ROA). Gal-Or in Ghose (2005: 86) sta z uporabo teorije iger poiskala, kolikšni so stroški in koristi izmenjave informacij o varnostnih incidentih.

Predstavljeni model podpira analitičen pristop reševanja problematike informacijskovarnostnih tveganj, pri čemer uporablja kvantitativno vrednotenje parametrov tveganja. Prednost takega pristopa je, da omogoča vrednotenje različnih obravnav tveganja in medsebojno primerjavo različnih vrst varnostnih ukrepov. Ti ukrepi so lahko tehnološke rešitve, organizacijski ukrepi, izobraževanja, zavarovanje, zunanje izvajanje storitev ter drugi. Rezultat modela so priporočila, kateri izmed predlaganih ukrepov je najbolj ustrezen za uvedbo v podjetju. Članek povzema matematično formulacijo teoretičnega modela za iskanje optimalnih investicij v informacijsko varnost (Bojanc, Jerman-Blažič & Tekavčič, 2012), vendar je ustrezno prirejen in poenostavljen za preprostejšo uporabo v podjetjih. Obenem pa daje članek večji poudarek samemu procesu upravljanja informacijskovarnostnih tveganj.

Članek je sestavljen iz petih razdelkov. Uvodu, v katerem je na kratko predstavljena problematika informacijske varnosti, sledi predstavitev upravljanja varnostnih tveganj, ki je glavni proces upravljanja sistema informacijske varnosti. V tretjem razdelku je predstavljen matematični model za upravljanje varnostnih tveganj. Model je zasnovan kot standarden postopek, ki podjetje vodi od začetnega vnosa vhodnih podatkov do končnih priporočil za izbiro optimalnega ukrepa, ki zmanjšuje določeno varnostno tveganje. Četrti razdelek vsebuje rezultate praktičnega izračuna, s katerim na podlagi realnih podatkov preverjamo ustreznost in pravilnost modela. Četrtemu razdelku sledi sklep.

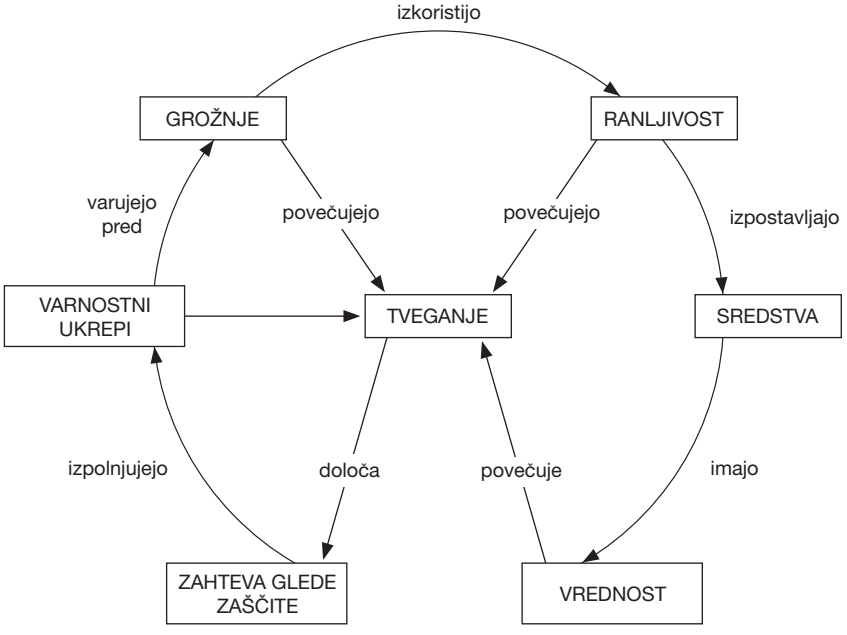
2 UPRAVLJANJE VARNOSTNIH TVEGANJ

Kako varen je informacijski sistem? Kako varen bi moral biti? To sta vprašanji, ki si jih strokovnjaki na področju varovanja informacij neprenehoma zastavljajo. Preprost odgovor na vprašanje, kakšno stopnjo varnosti želimo imeti, je: dovolj dobro varnost (Sandhu, 2003). Žal pa je zelo težko določiti, kaj je dovolj dobro (Geer, 2004). Popolno varnost lahko razumemo kot stopnjo varnosti, ki je sprejemljiva za podjetje (Schneier, 2003). To stopnjo podjetje lahko ugotovi s pomočjo upravljanja tveganj.

Upravljanje informacijske varnosti temelji na obvladovanju varnostnih tveganj. Tveganje je v splošnem opredeljeno kot kombinacija verjetnosti, da se zgodi neželen dogodek, in negativnih posledic, ki lahko nastanejo pri tem (ISO Guide 73, 2002). Na področju informacijske varnosti tveganje lahko natančneje opredelimo kot možnost, da bo določena grožnja izkoristila ranljivosti sredstva ali skupino sredstev ter povzročila škodo podjetju (ISO/IEC 27000, 2009). Tveganje je tako kombinacija grožnje in ranljivosti informacijskega sredstva, kar pripelje do negativnega učinka, ki škoduje enemu ali več informacijskim sredstvom. Grožnje in ranljivosti so del vzroka tveganja, učinek pa je posledica tveganja (Mayer idr., 2007). Npr. heker uporabi socialni inženiring na zaposlenem (tj. grožnjo), kar zaradi slabe ozaveščenosti zaposlenih (tj. ranljivosti) pripelje do neavtoriziranega dostopa do računalnikov in izgube zaupnosti ter celovitosti občutljivih informacij (tj. učinka oz. posledice).

Upravljanje tveganja je celoten proces obvladovanja izpostavljenosti podjetja negotovosti s posebnim poudarkom na identifikaciji, nadzoru in odpravljanju ali minimiziranju negotovih dogodkov, ki lahko potencialno preprečijo podjetju dosego zastavljenih ciljev. Postopek zahteva identifikacijo in oceno informacijskih sredstev podjetja, oceno posledic varnostnih incidentov, oceno verjetnosti uspešnih napadov na informacijske sisteme ter oceno poslovnih stroškov in koristi investicij v varnostne rešitve. Upravljanje tveganja uvaja glavne varnostne elemente: sredstva, grožnje, ranljivosti, tveganja in ukrepe. Slika 1 prikazuje odvisnosti med varnostnimi elementi, ki sodelujejo pri upravljanju s tveganjem.

Danes so mnoga podjetja že spoznala, da je informacijska varnost bolj v domeni vodenja (tj. načrtovanje, usmerjanje, koordinacija, nadzor porabe sredstev za dosego zastavljenega cilja) kot tehnike (Gordon & Loeb, 2005). Podjetja že obvladujejo različne vrste tveganj. Tveganja, povezana z informacijsko varnostjo, so le še dodatna vrsta tveganja. Proces upravljanja s tveganjem je sestavljen iz posameznih faz, preko katerih lahko identificiramo ranljivosti informacijskega sistema v podjetju, ovrednotimo trenutno mogoče varnostne zaščite, sprejmemo odločitve



Slika 1: **Povezave med elementi, ki sodelujejo pri upravljanju s tveganjem** (Vir: ISO 13335-1, 2004)

glede še sprejemljivega tveganja in izberemo najbolj ustrezno stroškovno učinkovito zaščito (Farahmand, 2004). Cilj procesa so stroškovno učinkovite zaščite, ki ne stanejo več, kot je pričakovana izguba ob napadu. Proces obvladovanja tveganja običajno sestavljata dve glavni fazi: ocena tveganja ter obravnava tveganja.

Obstaja veliko različnih načinov za obvladovanje tveganja. Katerega bomo izbrali v danih okoliščinah, je odvisno od podrobnosti le-teh. Za upravljanje s tveganji je na voljo veliko različnih metodologij in tehnik. ENISA (2009) med najbolj priljubljene metode in tehnike uvršča EBIOS, MEHARI, OCTAVE, CRAMM, CORAS, FRAP in IAM. Metode in tehnike za ocenjevanje tveganja lahko razdelimo v dve glavni kategoriji: kvantitativne in kvalitativne. Oba pristopa imata svoje prednosti in slabosti (Bojanc & Jerman-Blažič, 2008).

Kvantitativna metoda tveganja poskuša določiti numerične vrednosti za verjetnost in učinek tveganja ter ovrednotiti stroške in koristi, povezane z uvedbo varnostnih ukrepov. Kvantitativni pristop predpostavlja, da je mogoče vsako tveganje numerično ovrednotiti in izračunati vrednost verjetne škode, če se uresniči tveganje. Ključna prednost kvantitativne metode je, da podpira analizo stroškov in koristi ter da so rezultati predstavljeni tako, ki ga razume vodstvo. Po drugi strani pa kvantitativni pristop običajno zahteva poglobljeno in obsežno raziskavo o grožnjah, sistemu in podjetju, da lahko določimo numerične vrednosti za verjetnosti in stroške. Največja težava kvantitativnega pristopa je pomanjkanje dobrih statističnih oz. zgodovinskih podatkov, ki so potrebni za oceno parametrov tveganja. Statistični podatki so običajno razpoložljivi za tveganja, pri katerih so grožnje naravne nesreče (npr. potres, poplava). Precej težje pa je pridobiti statistične podatke za človeške grožnje.[1]

Kvalitativni pristop poskuša izraziti vrednost sredstev, pričakovano izgubo in stroške uvedbe zaščite v opisnih spremenljivkah, kot so »visoka«, »srednja« ali »nizka«. Pristop zagovarja načelo, da posledic nekaterih vrst izgub (npr. okvare ali spremembe podatkov) ni mogoče izraziti z denarnimi vrednostmi. Kvalitativne metode lahko izvedemo v krajšem času z manjšim številom osebja, pri čemer jih običajno izvajamo v kombinaciji vprašalnikov in

[1] Eden od razlogov je, da večina podjetij sistematično ne odkriva, nadzira in zapisuje varnostnih incidentov. Drugi razlog je, da podjetja, ki doživijo napad, o tem pogosto raje molčijo, kot da bi objavile napad. V primeru javnega razkritja varnostnega incidenta lahko tvegajo zmanjšanje svojega ugleda, izgubo zaupanja strank ali – kar je še huje – razkrivajo svoje ranljivosti drugim hekerjem. Zato veliko resnih varnostnih incidentov ni nikoli objavljenih (Bojanc & Jerman-Blažič, 2008). V zadnji raziskavi CSI (2010) je bilo kljub anonimnosti raziskave le 25 odstotkov sodelujočih pripravljenih razkriti podrobnosti o finančnih izgubah, ki so jih utrpeli.

skupnih delavnic. Največji prednosti kvalitativnega pristopa sta porabljeni čas in strošek za izvedbo ocene. Slabost kvalitativnega pristopa je splošnost in netočnost rezultatov, ki so posledica relativnih vrednosti vhodnih podatkov. Običajno je za manjša podjetja z omejenimi človeškimi viri primernejši kvalitativni pristop.

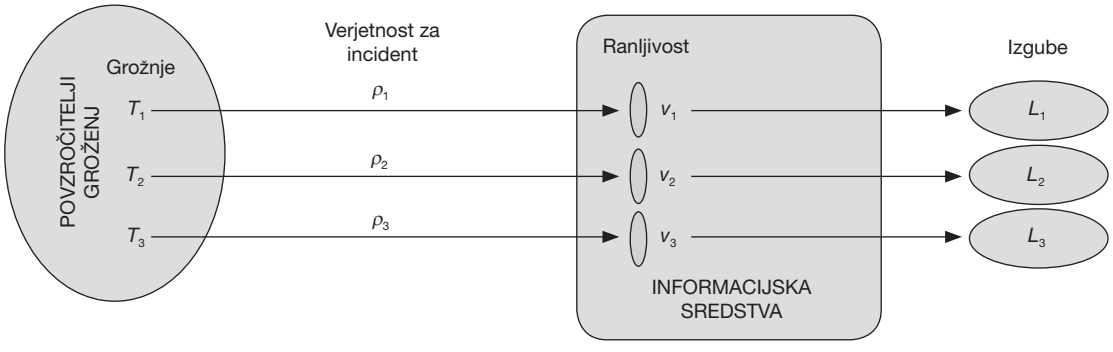
3 MODEL UPRAVLJANJA INFORMACIJSKOVARNOSTNIH TVEGANJ

Za učinkovito upravljanje tveganj informacijske varnosti je uporabljen matematični model, ki uporablja kvantitativni pristop (Bojanc, Jerman-Blažič & Tekavčič, 2012). Model je sestavljen iz štirih faz. Prva faza je ocena tveganja, v kateri za vsako informacijsko sredstvo določimo ter ovrednotimo ranljivosti in grožnje, verjetnost za nastanek incidenta ter izgube v primeru varnostnega incidenta. Druga faza je obravnava tveganja, pri čemer za vsako ovrednoteno tveganje določimo ustrezno obravnavo tveganja glede na njene kvantitativne parametre. Tretja faza je izbira in vrednotenje varnostnih ukrepov ter ocena njihovega učinka na zmanjšanje tveganja. Zadnja faza pomeni medsebojno primerjavo varnostnih ukrepov in ekonomsko analizo donosnosti posameznega ukrepa.

3.1 Ocena tveganja

Cilj ocene tveganja je identifikacija in merjenje tveganja z namenom informiranja procesa odločanja. Ocena tveganja potrebuje podatke o informacijskih sredstvih v podjetju, grožnjah, ki so jim izpostavljena sredstva, in sistemske ranljivosti, ki jih lahko zlorabijo grožnje. Preprosteje povedano je ocena tveganja proces določitve potencialne škode za posamezno tveganje ter verjetnosti, da se bo dogodek zgodil (Bojanc & Jerman-Blažič, 2008).

V predlaganem modelu v postopku ocene tveganj za vsako informacijsko sredstvo določimo ter ovrednotimo ranljivosti in grožnje, ki so vezane na to sredstvo. Izhodni podatek ocene tveganja je parameter tveganja, ki ga opredeljujeta verjetnost za varnostni incident ter posledica varnostnega incidenta. Shematični prikaz parametrov za oceno tveganja je prikazan na sliki 2. Povzročitelji groženj vsebujejo nabor možnih groženj (T), ki imajo neželene učinke na sistem. Grožnje so usmerjene na ranljivosti (v) informacijskih sredstev. Grožnje, ki so izvedene uspešno, so varnostni incident (ρ), ki podjetju povzroči izgubo (L). Zaradi preglednosti so povezave med grožnjami in ranljivostmi na sliki 2 prikazane samo linearno. Model podpira tudi primere, v katerih je ena grožnja usmerjena na več ranljivosti ter več groženj usmerjenih na eno ranljivost.



Slika 2: **Shematični prikaz parametrov za oceno tveganja**

3.1.1 Identifikacija in vrednotenje groženj ter ranljivosti

Informacijska sredstva so izpostavljena grožnjam. Grožnjo lahko opredimo kot potencialni vzrok neželenega incidenta, ki lahko povzroči škodo sistemu ali podjetju (ISO 27000, 2009). Grožnje so vse, kar prispeva k spreminjanju, uničenju ter prekinitvi storitev ali drugih stvari, ki pomenijo vrednost za podjetje. Nabor mogočih groženj se neprestano spreminja in je podjetjem poznan le delno.

Grožnje, ki pretijo informacijskim sredstvom, lahko izkoriščajo ranljivosti v programski opremi, konfiguraciji omrežja, varnostnih procedurah ipd. Večino varnostnih incidentov povzročajo ranljivosti, ki so posledica napak v programski opremi (Arora & Telang, 2005: 20). Strokovnjaki ocenjujejo, da je na vsakih tisoč vrstic programske kode približno dvajset napak in da število prijavljenih ranljivosti z leti narašča (Dacey, 2003). Čeprav so v večini primerov

ranljivosti tehnične narave, je velikokrat razlog za varnostni incident človeške narave. Taki primeri so uporaba šibkih gesel ali neustrezno varovanje gesel, nerazumevanje ali ignoriranje varnostnih politik, nenadzorovano odpiranje priponk v e-poštnih sporočilih, ogled sumljivih spletnih strani ali nameščanje programske opreme, ki vsebuje zlonamerno kodo. Grožnje različno vplivajo na informacijska sredstva. V glavnem so grožnje usmerjene na:

- uničenje informacijskih sredstev,
- spremembo informacijskih sredstev,
- krajo informacijskih sredstev,
- razkritje zaupnih informacij,
- prekinitev delovanja storitev.

Standard ISO 27005 (2008) Information Security Risk Management razvršča grožnje glede na vrsto napada v te kategorije:

- fizična škoda: požar, izliv vode, onesnaženje, uničenje opreme,
- naravni dogodki: potres, izbruh vulkana, poplava,
- izguba ključnih storitev: okvara klimatske naprave, okvara vodovodnega omrežja, izpad elektrike, okvara telekomunikacijske opreme,
- težave zaradi sevanja: npr. elektromagnetno sevanje, toplotno sevanje,
- ogrožanje informacij: prisluškovanje, kraja dokumentov ali opreme, razkritje, pridobitev zavrženih podatkov,
- tehnične napake: odpoved opreme, nepravilno delovanje programske opreme,
- nepooblaščena dejanja: nepooblaščena uporaba opreme, nelegalno kopiranje programske opreme, okvara podatkov, nelegalna obdelava podatkov,
- ogrožanje funkcij: napačna raba, zloraba pravic, ponareditev pravic, odpoved aktivnosti.

Za izračun vrednosti tveganja potrebujemo podatek o verjetnosti grožnje. *Verjetnost grožnje T* zato definiramo kot verjetnost za izveden dogodek, ki ima neželene učinke na informacijska sredstva. Verjetnost grožnje ($0 \leq T \leq 1$) je število napadov na enoto časa. Pri vrednotenju verjetnosti grožnje T se je treba zavedati, da na verjetnost vpliva veliko faktorjev, in sicer kolikšna je vrednost informacijskih sredstev podjetja za napadalca, katere vire ima napadalec na voljo, ali je informacija o stopnji varnosti v podjetju na voljo napadalcu (informacija napadalcu o visoki stopnji varnosti lahko odvrne napadalca, saj zahteva več napadalčevih virov na razpolago) idr. Vsaka grožnja izkorišča določeno ranljivost in je usmerjena na zlorabo zaupnosti, celovitosti ali razpoložljivosti.

Informacijska sredstva imajo ranljivosti, preko katerih lahko grožnje zlorabijo sredstva. Ranljivost sredstva lahko opredelimo kot šibkost sredstva ali nadzora, ki ga lahko zlorabi grožnja (ISO 27000, 2009) ter tako povečuje verjetnost za uspešen napad na ta sistem (Gordon & Loeb, 2005: 13); npr. puščanje prenosnega računalnika v nezaklenjeni namesto v zaklenjeni pisarni znatno poveča ranljivost prenosnega računalnika za grožnjo kraje. Verjetnost, da bo prenosnik dejansko ukraden, je odvisna od grožnje in ranljivosti. Ranljivost sama po sebi ne povzroči škode; ranljivost je samo pogoj (ali niz pogojev), ki lahko omogoči grožnji, da vpliva na sredstva (ISO 13335-1, 2004).

Ranljivost v sredstva opredelimo kot verjetnost ($0 < v < 1$), da bo izvedena grožnja uspešno zlorabila sredstvo, na katerega je usmerjena. Mejna vrednost $v = 0$ bi pomenila, da so informacijska sredstva popolnoma varna, $v = 1$ pa, da so informacijska sredstva popolnoma ranljiva.

3.1.2 Verjetnost za varnostni incident

Nekatere izvedene grožnje so za povzročitelja grožnje uspešne in povzročijo varnostni incident, medtem ko druge grožnje niso uspešne. Varnostni incident lahko opredelimo kot neželen ali nepričakovan dogodek v zvezi z informacijsko varnostjo ali serijo takšnih dogodkov, za katere je zelo verjetno, da bodo ogrozili poslovanje in informacijsko varnost (ISO 27000, 2009).

Varnostni incidenti so različnih vrst. Nekateri incidenti so vezani na zaupnost, kot npr. kraja bančnih računov. Drugi incidenti so vezani na celovitost, kot npr. zlonameren izbris ali sprememba dela podatkovne baze podjetja. Tretji incidenti so vezani na razpoložljivost, kot npr. napadi DoS (angl. Denial-of-Service), ki preprečujejo uporabo storitev vsem (avtoriziranim in neavtoriziranim) uporabnikom.

Varnostni incidenti se med seboj ne razlikujejo samo po vrsti, temveč predvsem po obsegu. Nekateri incidenti vplivajo le na del informacij ali informacijskega sistema podjetja. Drugi incidenti imajo vpliv na celotno podjetje ali celo več podjetij. Incident lahko povzroči verižno reakcijo incidentov ali posredne incidente; npr. izguba zaupnih občutljivih informacij lahko vodi do izgube zaupanja strank.

Verjetnost za varnosti incident ρ $(0 \leq \rho \leq 1)$ določimo kot produkt med verjetnostjo za pojav grožnje T in ranljivostjo v.

$$\rho = T \cdot v \qquad (1)$$

3.1.3 Izguba v primeru varnostnega incidenta

V primeru varnostnega incidenta podjetje utrpi finančno izgubo $L > 0$, ki je merjena v denarnih enotah (npr. evro). Natančno finančno izgubo zaradi varnostnega incidenta je težko oceniti. Dokaj preprosto lahko izračunamo takojšnjo (oz. neposredno izgubo), ki vključuje izgubo prihodkov, izgubo produktivnosti, stroške, povezane z zamenjavo opreme, in sanacijo škode. Precej težje pa je oceniti in ovrednotiti posredno izgubo zaradi varnostnega incidenta. Za lažji izračun izgub razdelimo izgubo na posamezne faktorje:

$$L = L_S + L_r + L_i + L_p + L_{SLA} + L_{posredne} \qquad (2)$$

Podrobna opredelitev in matematična izpeljava posameznih faktorjev, ki nastopajo v enačbi (2) je v Bojanc, Jerman-Blažič in Tekavčič (2012), tukaj je vsebina faktorjev predstavljena le opisno.

Strošek zamenjave opreme L_s je strošek nakupa nove opreme. To vrsto izgub je najpreprosteje ovrednotiti, saj so podatki običajno že na razpolago ali pa jih lahko dokaj preprosto pridobimo. V primeru okvare opreme se lahko ta strošek občutno zmanjša ob investiciji v garancijske storitve, ki jih ponujajo proizvajalci ali razni vzdrževalci opreme.

Strošek popravila L_r so stroški dela zaposlenih ali zunanjih izvajalcev, ki so potrebni, da odpravimo posledice incidenta in ponovno vzpostavimo normalno delovanje sistema ali storitve.

Izguba prihodkov podjetja L_i je izguba, ki jo utrpi podjetje na prihodkovni strani zaradi nedelovanja sistema ali storitve kot posledice incidenta.

Izguba produktivnosti podjetja L_p je zmanjšanje produktivnosti v času nedelovanja sistema ali storitve. V določenih primerih sta lahko izguba prihodkov in izguba produktivnosti medsebojno povezani, zato je treba paziti, da v takih primerih izgube ne vrednotimo dvojno.

Izguba zaradi nespoštovanja zakonskih predpisov ali pogodbenih obveznosti L_{SLA} je odvisna od pogodbe oz. zakonodaje. Za primer poglejmo podjetje, ki strankam ponuja določeno storitev in ima s strankami sklenjeno pogodbo SLA (angl. Service Level Agreement). Če je razpoložljivost storitve, ki jo ponuja podjetje, pod mejo, določeno v SLA, pomeni to za podjetje strošek, saj mora strankam povrniti del plačila.

Posredne izgube $L_{posredne}$ pomenijo zmanjšan ugled podjetja, prekinitev poslovnih procesov, zakonske sankcije, izgubo intelektualne lastnine in izgubo zaupanja strank. Ta izguba je lahko precej večja kot takojšnja izguba ter ima lahko daljnoročne negativne učinke na stranke, dobavitelje, partnerje, finančne trge, banke, zavarovalnice.

Varnostni incidenti lahko povzročijo nedelovanje storitev ali informacijskega sistema. Trajanje nedelovanja je sestavljeno iz časa detekcije t_d, v katerem zaznamo varnostni incident, in časa trajanja popravila t_r, v katerem ponovno vzpostavimo v normalno delovanje informacijski sistem ali storitve. Čas t_d štejemo od trenutka, ko se zgodi incident, do trenutka, ko ga zaznamo. Posamezni faktorji v enačbi (2) lahko vsebujejo bodisi t_r, t_d ali oboje. Časovni parameter t_r vsebujejo faktorji L_r, L_i in L_p, časovni parameter t_d vsebujeta faktorja L_i in L_p, medtem ko faktorji L_s, L_{SLA} in $L_{posredne}$ nimajo časovne odvisnosti (Bojanc, Jerman-Blažič & Tekavčič, 2012). Tako lahko faktorje izgub v enačbi (2) zapišemo tako, da jih ločimo glede na časovna parametra:

$$L = L_1 \cdot t_r + L_2 \cdot t_d + L_3 \qquad (3)$$

Faktor L_1 združuje podatke o L_r, L_i in L_p, faktor L_2 podatke o L_i in L_p ter faktor L_3 podatke o L_s, L_{SLA} in $L_{posredne}$. Faktor L_3 je izražen v denarnih enotah (npr. evro), faktorja L_1 in L_2 pa v denarnih enotah na časovno enoto (npr. evro/uro).

3.1.4 Izračun stopnje tveganja

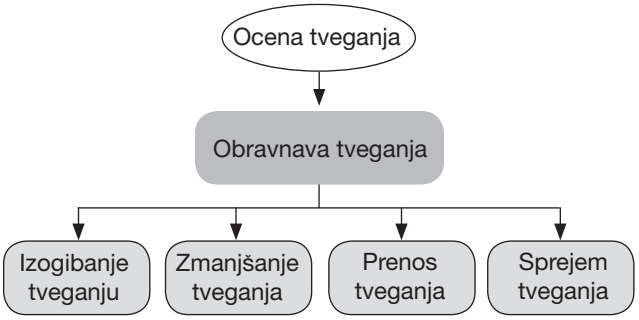
S postopkom ocene tveganja za vsako informacijsko sredstvo ugotovimo in ovrednotimo ranljivosti in grožnje. Rezultat ocene tveganja je izračunani parameter *varnostno tveganje R*, ki pomeni pričakovano finančno izgubo zaradi pričakovanega varnostnega incidenta in je izražen v enakih denarnih enotah kot izguba L (npr. evro). Varnostno tveganje je določeno kot produkt med ocenjeno verjetnostjo za varnostni incident ρ in izgubo zaradi varnostnega incidenta L ter ga ob upoštevanju zapisa izgube (3) in verjetnosti za incident (1) lahko zapišemo:

$$R = \rho \cdot L = T \cdot v \cdot [L_1 \cdot t_r + L_2 \cdot t_d + L_3] \qquad (4)$$

3.2 Izbira ustrezne obravnave tveganja

Za vsako zaznano in ovrednoteno varnostno tveganje je na voljo več možnosti, kako podjetje obravnava to tveganje. Glede na opravljeno oceno tveganja ima podjetje na izbiro obravnave, ki so shematično prikazane na sliki 3:

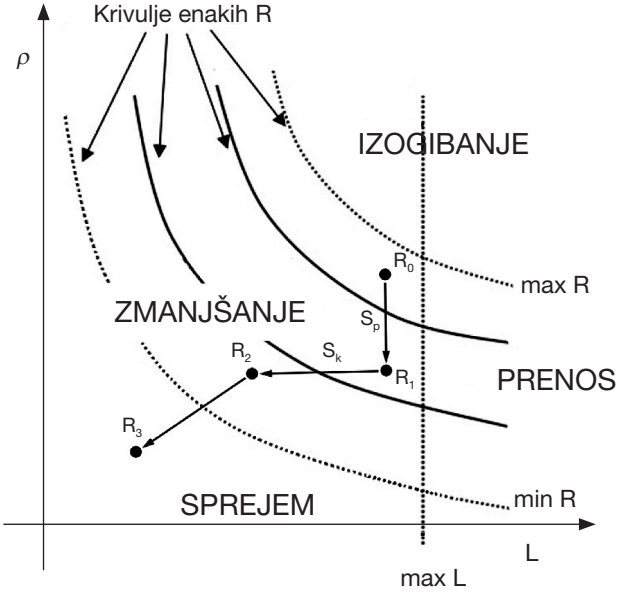
- *zmanjšanje* izpostavljenosti sredstva na tveganje z uvedbo ustreznih tehnologij in orodij (npr. požarnega zidu, protivirusne zaščite) ali uvedbo ustreznih postopkov (npr. varnostne politike, politike gesel, nadzora dostopa itd.): s tem zmanjšamo verjetnost za škodljive dogodke ali omejimo izgubo, ki jo povzroči dogodek. Zmanjšanje tveganja je pogosto glavna strategija obvladovanja tveganja;
- *prenos* tveganja na drugo stranko – lahko preko zunanjega izvajanja storitev (npr. storitve v oblaku) ali z zavarovanjem: strategija prenosa postaja v zadnjem času čedalje bolj pomembna;
- *izogibanje* grožnjam in napadom z omejevanjem izvorov tveganja oz. z izpostavljenostjo sredstev k tveganju večinoma uporabimo v primerih, ko resnost učinka tveganja pretehta koristi, ki jih prinaša posamezno sredstvo (npr. odprt dostop do interneta). Podjetje se z izogibanjem tveganim aktivnostim odpove aktivnosti, vendar pa se zaščiti pred tveganjem, ki bi imelo prevelike posledice;
- *sprejem* tveganja kot posledico poslovanja je smiselna strategija v primeru, ko se ni mogoče izogniti tveganju ali ko so stroški uvedbe zaščitnih ukrepov znatno večji kot skupne izgube zaradi tveganja.



Slika 3: **Različne možnosti obravnave tveganja**

Zavedati se je treba, da izbrana obravnava tveganja lahko privede do novih tveganj, ki jih je treba ravno tako oceniti in obravnavati (Schneier, 2003: 14). V nekaterih primerih je težko določiti mejo med posameznimi obravnavami, npr. požarni zid lahko razumemo kot zmanjšanje tveganja ali pa tudi kot izogibanje tveganju, ker se s tem podjetje odreče prednosti odprtih omrežij, da bi se izognilo tveganju. Zato je izbira ustrezne obravnave tveganja lahko precej težavna in večkrat pri odločanju zahteva sklepanje kompromisov ali uporabo in kombiniranje dveh strategij.

Izbiro ustrezne obravnave tveganja lahko prikažemo na grafu verjetnosti za incident in izgube zaradi incidenta $\rho = \rho(L)$, ki je prikazan na sliki 4. Krivulje na grafu predstavljajo točke z isto vrednostjo tveganja R, ki pa se med seboj razlikujejo v vrednostih ρ in L. Notranje krivulje pomenijo nižje vrednosti tveganja, zunanje krivulje pa višje. Izbrana obravnava tveganja, ki zmanjšuje vrednost tveganja R, prestavi točko tveganja na nižjo krivuljo tveganja. Obravnava tveganja s_p zmanjšuje verjetnost za incident ρ in je na grafu prikazana kot vertikalen premik navzdol iz točke R_0 v R_1. Obravnava tveganja s_k zmanjšuje izgubo in je na grafu prikazana kot horizontalni premik proti levi s točke R_1 na R_2.



Slika 4: **Grafični prikaz porazdelitve posamezne obravnave tveganja glede na vrednosti *L*, *ρ* in *R*** (Vir: Bojanc & Jerman-Blažič, 2012)

Vsaka izmed štirih mogočih obravnav tveganja pomeni določeno področje na grafu. Določiti je treba mejne vrednosti parametrov tveganja, ki so mejne črte, ki področje grafikona razdelijo na štiri enote, katere ustrezajo posameznim obravnavam tveganja (Bojanc & Jerman-Blažič, 2008). Te vrednosti so:

- R_{max} – največja vrednost tveganja, ki je za podjetje še sprejemljiva,
- L_{max} – največja enkratna izguba, ki je za podjetje še sprejemljiva,
- R_{min} – najmanjša vrednost tveganja, ki je za podjetje že zanimiva.

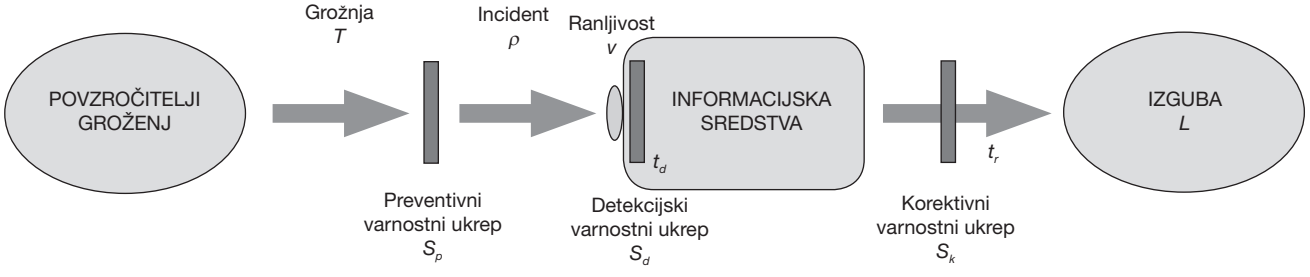
Ustrezno obravnavo tveganja določimo tako, da za posamezno tveganje vrednosti R in L primerjamo z mejnimi vrednostmi R_{max}, L_{max} in R_{min}. Prva mejna črta določa najmanjšo smiselno verjetnost za incident ($R < R_{min}$). Pod to vrednostjo je tveganje zanemarljivo nizko, zato uvajanje varnostnega ukrepa ni finančno upravičeno in sprejmemo tveganja. Druga mejna črta je največja mogoča vrednost tveganja ($R > R_{max}$), nad katero se podjetje izogne tveganju. Tretja mejna črta je največja mogoča izguba zaradi incidenta ($L > L_{max}$). Nad to vrednostjo ima zaradi visoke izgube učinek lahko katastrofalne posledice in je priporočljivo oblikovati prenos tveganja. Schneier (2003: 23) pravi, da zares velike posledice niso sprejemljive ne glede na pogostost. Tveganja v preostalem območju ($L < L_{max}$) odpravimo z zmanjševanjem preko investicij v varnostne ukrepe.

Mogoče so tudi kombinacije teh obravnav; npr. podjetje najprej izvede varnostne ukrepe, ki zmanjšajo izgubo, ter preostanek tveganja prenese na zavarovalnico. Pri tem je treba ugotoviti, ali je investicija v varnostni ukrep manjša od zmanjšanja premije, ki jo plačujemo zavarovalnici.

3.3 Izbira in vrednotenje varnostnih ukrepov

Varnostni ukrepi so aktivnosti, postopki ali mehanizmi, ki preprečujejo ali zmanjšujejo škodo, povzročeno z realizacijo ene ali več groženj. Varnostni ukrepi so lahko fizične ovire, senzorji, programska oprema, algoritmi, izboljšave obstoječih politik ali postopkov. Lahko izvajajo eno ali več funkcij, kot so odkrivanje, odvračanje, preprečevanje, omejevanje, popravljanje, okrevanje, nadzor in ozaveščenost. Lahko varujejo pred grožnjami, zmanjšujejo ranljivosti, zmanjšujejo učinek nezaželenih incidentov, odkrivajo nezaželene incidente in olajšajo okrevanje. Primerna izbira varnostnih ukrepov je bistvenega pomena za učinkovito informacijsko varnost. Kot je prikazano na sliki 5, se pred grožnjami zavarujemo z uvedbo varnostnih ukrepov, ki jih lahko glede na učinek na parametre R, ρ in L razvrstimo v:

- *preventivne varnostne ukrepe* s_p, ki zmanjšujejo verjetnost za varnostni incident ρ (npr. požarni zid, protivirusna zaščita),
- *korektivne varnostne ukrepe* s_k, ki zmanjšujejo izgubo L v primeru incidenta (npr. vzdrževalne pogodbe, načrt neprekinjenega poslovanja, varnostne kopije podatkov, redundantni sistem, uvedba različnih standardov),
- *detekcijske varnostne ukrepe* s_d, ki zmanjšujejo čas, v katerem zaznamo incident t_d in omogočamo zbiranje podatkov o grožnjah (npr. sistem za odkrivanje vdorov, IDS – Intrusion Detection System).



Slika 5: **Učinek uvedbe varnostnih ukrepov na zmanjšanje tveganja** (Vir: Bojanc, Jerman-Blažič & Tekavčič, 2012)

Učinek varnostnih ukrepov je prikazan tudi grafično na sliki 4. Uvedeni preventivni ukrep s_p prestavi stanje na grafu vertikalno navzdol (iz R_0 na R_1) na nižjo krivuljo tveganja, uvedba korektivnih s_k in detekcijskih ukrepov s_d pa prestavi stanje na grafu horizontalno proti levi na nižjo krivuljo tveganja (iz R_1 na R_2).

Vsak varnostni ukrep $s(\alpha, C)$ opredeljujeta dva kvantitativna parametra: učinkovitost ukrepa α in strošek ukrepa C. *Učinkovitost varnostnega ukrepa* α predstavlja vpliv varnostnega ukrepa na zmanjšanje tveganja. *Strošek ukrepa* C je denarna investicija v varnostni ukrep, ki vsebuje vse izdatke, vezane na uvedbo varnostnega ukrepa, od enkratnega izdatka v kapitalske naložbe do operativnih stroškov. Kapitalske naložbe so npr. nabava novega sistema za zaznavanje vdorov v omrežje, ki pomaga podjetju

zmanjševati verjetnost varnostnih vdorov v določenem (npr. triletnem) prihodnjem obdobju. Operativni stroški vključujejo letno vzdrževanje (posodobitve in varnostne popravke), izobraževanje uporabnikov in skrbnikov omrežja ter nadzor delovanja rešitve.

Pri uvedbi varnostnih ukrepov je treba upoštevati tudi proračun podjetja, namenjen za varnostne investicije C_{IT_budget}, ki ga ne sme presegati strošek varnostnih ukrepov v določenem proračunskem obdobju. Če je cena ukrepa višja kot znaša proračun, uvedba tega ukrepa ni mogoča. Po raziskavi CSI (2010) je v povprečju 6 odstotkov proračunskih sredstev podjetja namenjenih za informacijsko varnost.

Uvedba preventivnega varnostnega ukrepa $s_p(\alpha_p, C_p)$ zmanjšuje verjetnost za varnostni incident ρ. Obstaja precej različnih funkcij verjetnosti za varnostni incident ρ, v predstavljenem modelu je uporabljena funkcija, ki je med raziskovalci precej priljubljena (Gordon & Loeb, 2002; Matsuura, 2008):

$$\rho = T \cdot v^{\alpha_p C_p + 1} \qquad (5)$$

Izguba L zaradi varnostnega incidenta se lahko zmanjša z investicijo v korektivni varnostni ukrep $s_k(\alpha_k, C_k)$, ki zmanjšuje čas popravila t_r, ali v detekcijski varnostni ukrep $s_d(\alpha_d, C_d)$, ki zmanjšuje čas za detekcijo t_d. Poseben primer korektivnega ukrepa je prenos tveganja na zavarovalnico. V tem primeru je strošek C mesečna ali letna premija, ki jo podjetje plačuje zavarovalnici; v primeru incidenta pa zavarovalnica izplača podjetju kompenzacijo za kritje izgube v vrednosti I. Izgubo L v enačbi 3 ob uvedbi teh ukrepov lahko zapišemo:

$$L = L_1 \cdot t_r^0 \cdot e^{-\alpha_k C_k} + L_2 \cdot t_d^0 \cdot e^{-\alpha_d C_d} + L_2 - I \qquad (6)$$

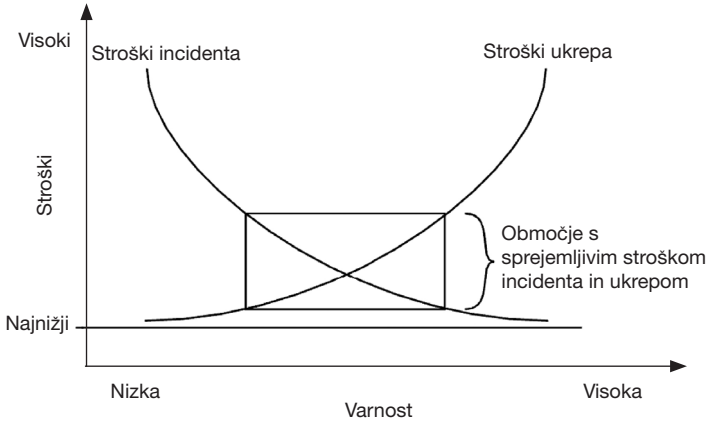
Enačba 4 za varnostno tveganje R ob upoštevanju uvedbe varnostnih ukrepov, ki zmanjšujejo verjetnost za incident (enačba 5) ali izgubo v primeru incidenta (enačba 6), izračunamo kot:

$$R = T \cdot v^{\alpha_p C_p + 1}[L_1 \cdot t_r^0 \cdot e^{-\alpha_k C_k} + L_2 \cdot t_d^0 \cdot e^{-\alpha_d C_d} + L_3 - I \qquad (7)$$

Nova vrednost tveganja R po uvedbi varnostnih ukrepov je grafično prikazana na sliki 4, na kateri nova vrednost tveganja leži na nižji krivulji tveganja R kot prvotna vrednost tveganja.

3.4 Ocena donosnosti ukrepov in izbira optimalnega ukrepa

Odločitev o tem, kako najbolje vlagati sredstva v informacijsko varnost, ni preprosta in se tudi razlikuje od organizacije do organizacije. Pri določitvi optimalnega zneska investicij v informacijsko varnost je treba najti optimalno razmerje med stroški in varnostjo, kar je prikazano na sliki 6. Stroški informacijske varnosti imajo dve komponenti, ki sta povezani med seboj, in sicer »stroški ukrepa« in »stroški incidenta«. Strošek ukrepa je denar, ki ga podjetje porabi za investicijo, s katero se želi izogniti problemu. Ta komponenta se povečuje z večanjem varnosti sistema. Strošek incidenta je denar, ki ga podjetje porabi, ko pride do problema. Ta komponenta se zmanjšuje z večanjem varnosti sistema. Če podjetje ne porabi nič za stroške ukrepa, bo to imelo za posledico povečano porabo stroškov incidenta zaradi sanacije stanja, medtem ko bodo zelo veliki stroški ukrepa močno zmanjšali stroške incidenta. Iskanje optimalne stopnje varnosti, ki upošteva stroške incidenta in stroške ukrepa, ni preprosta naloga. Za določitev optimalne stopnje informacijske varnosti pogosto uporabimo analizo stroškov in koristi.



Slika 6: **Iskanje optimalne rešitve med višino stroškov varnostnega incidenta in stroški ukrepa** (Vir: Kaplan, 2007: 304).

Analiza stroškov in koristi primerja stroške določene aktivnosti s koristmi, ki jih prinaša aktivnost. Predpostavimo, da lahko ocenimo pričakovane skupne koristi in pričakovane skupne stroške za različne ravni aktivnosti informacijske varnosti. Dokler *koristi B* dodatne aktivnosti informacijske varnosti presegajo *stroške C*, je uvedba aktivnosti smiselna.

$$B > C \qquad (8)$$

Cilj podjetja je uvedba varnostnih ukrepov do točke, na kateri so neto koristi (tj. koristi minus stroški) maksimalne. Uvedba varnostnih ukrepov preko te točke pomeni, da so mejni stroški višji od mejnih koristi dodatne varnosti. Z drugimi besedami, neto koristi uvedbe varnostnih ukrepov preko najvišje točke so negativne. Za podjetje nima smisla, da za varnostno rešitev zapravi več, kot znašajo mogoče izgube v primeru incidenta.

Gordon in Loeb (2002) ocenjujeta, da naj bi optimalni strošek za varnostni ukrep znašal od 0 do 37 odstotkov mogoče izgube zaradi varnostnega incidenta. Drugi raziskovalci so to ugotovitev razširili in našli okoliščine, v katerih je upravičeno, da strošek ukrepa znaša celo do 100 odstotkov mogoče izgube (Willemson, 2006). Te ugotovitve so uspešno preverili na empiričnih primerih (Tanaka, Matsuura & Sudoh, 2005; Tanaka, Liu & Matsuura, 2006).

Izračun stroškov vlaganja *C* v informacijsko varnost je opisan v prejšnjem razdelku. Za razliko od stroškov, ki jih je mogoče dobiti dokaj preprosto, pa je precej težje opredeliti, oceniti ali meriti koristi. Varnostne rešitve (npr. požarni zid, protivirusni program in sistemi IDS) same po sebi namreč ne prinašajo finančne koristi, ki jih je mogoče izmeriti. Koristi investicije v informacijsko varnost so lahko različne, npr. zmanjšanje verjetnosti ponovitve incidenta, povečanje učinkovitosti ostalih investicij informacijske varnosti ali zmanjševanju izgub v primeru incidenta.

V splošnem se na koristi zaradi vlaganja v informacijsko varnost gleda kot na prihranek stroškov incidenta zaradi zmanjšanja verjetnosti ali posledic varnostnega incidenta. Te koristi je običajno zelo težko točno napovedati. Največja težava je, ker gre za ocenjevanje prihrankov stroškov, vezanih na potencialne varnostne incidente, ki se še niso zgodili. Bolj kot je informacijska varnost uspešna, težje je opaziti dejanske koristi.

Koristi *B* zaradi investicije v varnostni ukrep so enake zmanjšanju tveganja na račun uvedbe ukrepa, kar lahko zapišemo kot razliko med vrednostmi tveganja pred uvedbo ukrepa R_0 in vrednostmi tveganja po uvedbi varnostnega ukrepa $R(C)$:

$$B = R_0 - R(C) \qquad (9)$$

Za oceno ekonomske upravičenosti uvedbe varnostnega ukrepa v praksi najpogosteje uporabljamo kazalnike donosnost investicije (angl. Return on Investment – ROI), neto sedanja vrednost (angl. Net Present Value – NPV) in notranja stopnja donosa (angl. Internal Rate of Return – IRR) ali kombinacija teh kazalnikov.

Donosnost investicije (ROI) določa, koliko podjetje dobi glede na porabljeni znesek denarja. Kazalnik je izražen kot odstotek vrnjene investicije v določenem času. ROI je enak sedanji vrednosti neto koristi v določenem časovnem obdobju, deljen z začetnim stroškom investicije *C*. Pozitivna vrednost ROI pomeni, da je vlaganje ekonomsko upravičeno.

$$ROI = \frac{B - C}{C} \qquad (10)$$

Izračun ponazorimo s preprostim primerom. Recimo, da je tveganje okužbe z virusom v organizaciji ocenjeno na 8.750 evrov. Z uvedbo varnostnega ukrepa v vrednosti 1.600 evrov tveganje zmanjšamo na 3.400 evrov. K stroškom nakupa ukrepa je treba prišteti še 450 evrov letnih stroškov za vzdrževanje in upravljanje varovanja. Za prvo leto uporabe znaša tako ROI:

$$ROI = \frac{8.750 - 3.400 - 1.600 - 450}{1.600 + 450} = 160\ \% \qquad (11)$$

Izračun ROI lahko navedemo za različne varnostne ukrepe, ki so predstavljeni v razdelku 3.3. Pri tem za posamezne varnostne ukrepe ustrezno prilagodimo enačbo tveganja 7. Če varnostno tveganje rešujemo z vlaganjem v preventivni varnostni ukrep s_p, ki zmanjša ranljivost sredstva, lahko enačbo 10 za ROI zapišemo:

$$ROI = \frac{T \cdot v\,(1 - v^{\alpha_p C_p}) \cdot L - C_p}{C_p} \qquad (12)$$

Če pa tveganje rešujemo z vlaganjem v korektivni varnostni ukrep s_k, ki zmanjšuje izgubo, lahko enačbo 10 za ROI zapišemo:

$$ROI = \frac{TvL_1 t_r^0 (1 - e^{-\alpha_k C_k}) - C_k}{C_k} \qquad (13)$$

Poseben primer je prenos tveganja na zavarovalnico, pri čemer enačbo 10 poenostavimo v:

$$ROI = \frac{TvI - C}{C} \qquad (14)$$

Zavedati se je treba, da ROI pove samo odstotek donosnosti investicije v določenem časovnem obdobju, ničesar pa ne pove o obsegu donosa. Tako lahko 124-odstotna donosnost na prvi pogled zgleda precej mikavno, vprašanje pa je, ali bi raje imeli 124-odstotno donosnost projekta v višini 10.000 evrov ali »samo« 60-odstotno donosnost projekta v višini 300.000 evrov.

Za dolgoročnejša vlaganja v informacijsko varnost je zato primernejša uporaba kazalnika *neto sedanja vrednost (NPV)*, ki upošteva tudi vrednost denarja v času, ki ga kazalnik ROI ne upošteva:

$$NPV = \sum_{t=0}^{n} \frac{B_t - C_t}{(1 + k)^t} \qquad (15)$$

V enačbi 15 je k diskontna stopnja, n pa časovno obdobje. Diskontna stopnja k se običajno razume kot povprečni strošek kapitala. Izbor ustrezne diskontne stopnje je za izračun kazalnika NPV zelo pomemben. Model NPV preko diskontne stopnje uravnava tveganje, pri tem večja diskontna stopnja pomeni manjšo vrednost kazalnika NPV.

Kazalnik NPV je merjen v denarnih enotah, vlaganje pa je ekonomsko upravičeno, če je NPV enak ali večji od nič. Bistvo pristopa NPV je primerjava diskontiranih denarnih tokov, vezanih na prihodnje koristi in stroške z začetnimi stroški investicije, pri čemer so celotne koristi in stroški izraženi v denarni enoti. Zaradi lažjega izračunavanja se pogosto privzame, da so prihodnje koristi in stroški, z izjemo stroškov začetne investicije, realizirani na koncu posameznega obdobja. S tem ko denarne tokove diskontiramo, ustrezno vključimo časovno komponento, tako da so zneski koristi in stroškov v različnih časovnih obdobjih primerljivi.

NPV pogosto uporabljamo v primerih, ko med seboj primerjamo različne alternative, npr. organizacija izbira med dvema varnostnima rešitvama, pri čemer za prvo rešitev plača 15.000 evrov vnaprej, za drugo pa plačuje tri leta po 5.000 evrov na leto. Obe rešitvi staneta 15.000 evrov, vendar je druga rešitev ugodnejša, saj lahko organizacija investira preostali denar za določen čas v druge namene. Tako je dejanski strošek druge investicije manjši od 15.000 evrov.

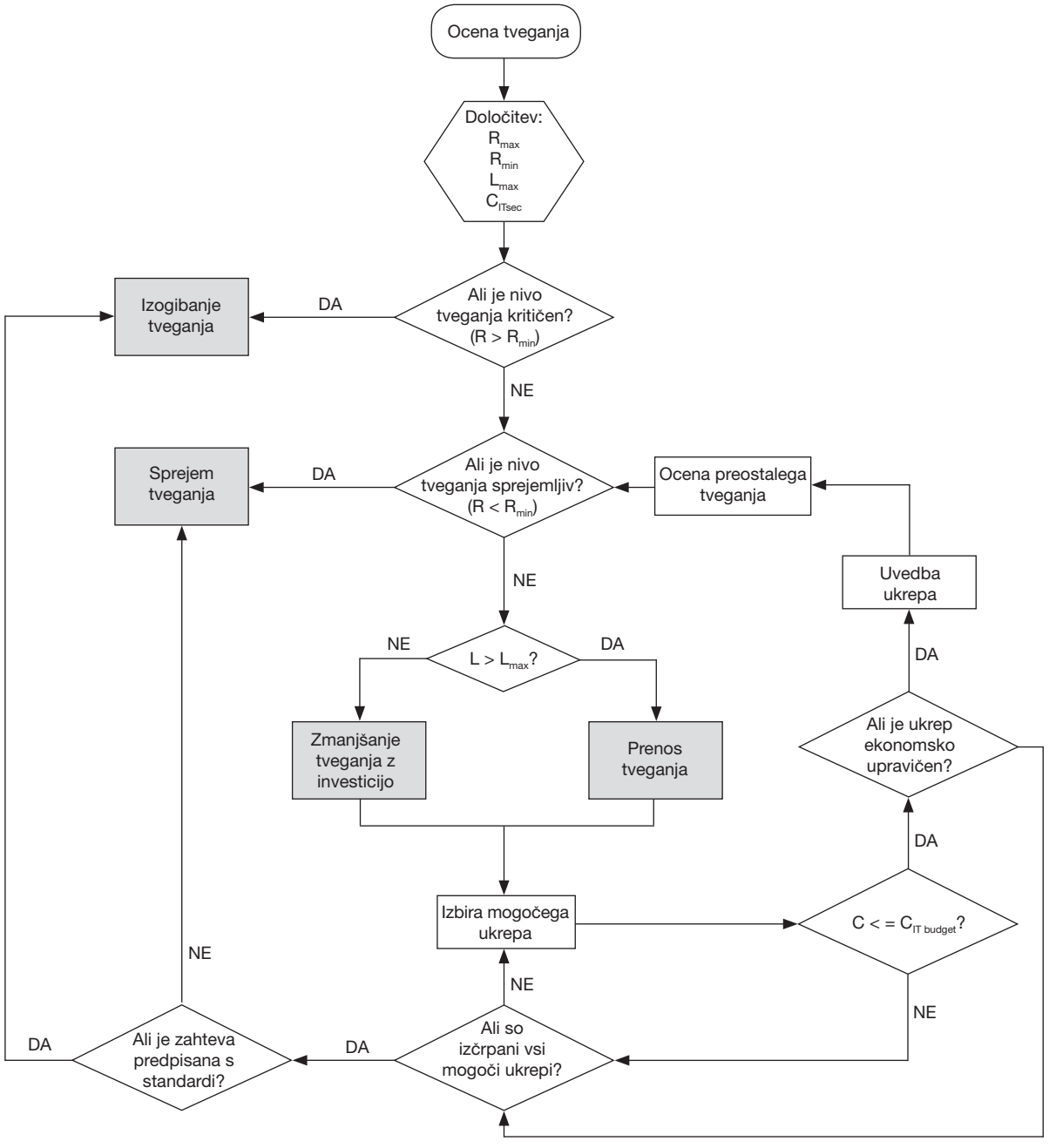
Da bi ugotovili, kolikšna je dejanska stopnja donosnosti projekta, lahko uporabimo kazalnik *notranja stopnja donosa (IRR)*. IRR je enak tisti diskontni stopnji, pri kateri je NPV = 0 oz. pri kateri se izenačita sedanja vrednost prejemkov in sedanja vrednost izdatkov.

$$\sum_{t=0}^{n} \frac{B_t - C_t}{(1 + IRR)^t} = 0 \qquad (16)$$

Odločitev glede uporabe kazalnikov ROI, NPV ali IRR je prepuščena podjetjem in posameznikom, odgovornim za vrednotenje varnostnih investicij. Vsak od teh finančnih kazalnikov ima svoje prednosti in slabosti. Pogosto so rezultati enaki pri uporabi vseh treh kazalnikov, včasih pa se pri odločanju pokažejo razlike. Zato je pri primerjavi dveh ali več alternativnih varnostnih rešitev pogosto treba upoštevati več kazalnikov. Čeprav ima ROI določene pomanjkljivosti v primerjavi z NPV in IRR, je ROI še vedno najbolj priljubljen kazalnik v praksi. Po raziskavi CSI (2010) uporablja kazalnike ROI 54 odstotkov vprašanih, 22 odstotkov jih uporablja NPV, 17 odstotkov pa IRR.

3.5 Proces upravljanja tveganja

Proces upravljanja informacijskovarnostnih tveganj je prikazan na sliki 7. Proces se začne z oceno tveganja in nadaljuje z izbiro ustrezne obravnave tveganja, ki temelji na določitvi mejnih parametrov tveganja R_{min}, R_{max}, L_{max}. Izbira varnostnega ukrepa je odvisna tudi od višine proračuna podjetja za investicije v informacijsko varnost C_{IT_budget}, ki ga cena ukrepov C v določenem proračunskem obdobju ne sme presegati. Če pri zmanjšanju tveganja ni na voljo nobenega ustreznega ukrepa, je treba zmanjšanje tveganja zamenjati za drugo obravnavo (npr. sprejem ali izogibanje) tveganja.



Slika 7: **Proces upravljanja informacijskovarnostnih tveganj** (Vir: Bojanc, Jerman-Blažič in Tekavčič, 2012)

4 PRAKTIČNO PREVERJANJE MODELA

Model upravljanja tveganj je praktično preverjen v raziskavi v realnem okolju, pri čemer je sodelovalo srednje veliko podjetje s področja informacijske tehnologije v Sloveniji. Namen raziskave je uporaba modela v praksi in ocena njegove praktične uporabnosti. Izračuni, v katerih smo preizkušali model, so narejeni na podlagi realnih podatkov in za različne grožnje (virusi, neželena pošta, neavtorizirana sprememba spletne strani, phishing, napad DoS). V nadaljevanju je prikazan izračun za grožnjo okužbe z računalniškim virusom, ki je po raziskavi CSI najpogostejša grožnja (CSI, 2010). Da izračun ni preobširen, je v članku naveden pregled praktične uporabe, celotni izračun pa je prikazan v Bojanc, Jerman-Blažič in Tekavčič (2012).

Pri tveganju okužbe z računalniškim virusom pojem virus razumemo v širšem pomenu, tako da pod tem izrazom upoštevamo tudi črve in trojanske konje. Podjetju se v kratkem izteče naročnina za protivirusni program, ki ga trenutno uporabljajo za zaščito delovnih postaj in strežnikov. Želijo preveriti, ali naj obdržijo sedanji protivirusni program in podaljšajo naročnino ali naj se odločijo za katero drugo rešitev. Ker podjetje želi preučiti tako obstoječo zaščito kot tudi nove zaščite, privzamemo stanje, da trenutno ni uvedena nobena zaščita pred tveganjem okužbe z računalniškim virusom in kot mogoči ukrep upoštevajo sedanjo rešitev.

V prvem koraku pridobimo kvantitativne podatke za oceno tveganja. Ranljivost je verjetnost, da bo računalniški virus okužil sredstvo, na katerega je usmerjen. Ker ocenjujemo stanje, v katerem ni nobene tehnične zaščite zoper grožnje, je ranljivost enaka ozaveščenosti zaposlenih, da v primeru, ko dobijo virus, tega ne aktivirajo. Podjetje ocenjuje, da bi glede na trenutno ozaveščenost in v okolju brez protivirusne zaščite, virus preko okužene datoteke aktivirali dve tretjini zaposlenih ($\nu = 0{,}66$). Verjetnost grožnje je ocena pogostosti prejema okuženih datotek ali drugega načina okužbe in je ocenjena na enkrat na teden ($T = 1/7$ dni = 0,143/dan). Verjetnost za incident je:

$$\rho = T \cdot \nu = 0{,}143 \cdot 0{,}66 = 0{,}0952 \ / \ dan \qquad (17)$$

Parametri izgube v primeru varnostnega incidenta so ocenjeni: $L_1 = 41{,}53$ evrov/uro, $L_2 = 18{,}41$ evrov/uro, $L_3 = 0$, $t_{r0} = 8$ ur, $t_{d0} = 2$ uri. Skupna izračunana izguba je tako: $L = 369{,}07$ evrov. Varnostno tveganje ocenimo na:

$$R = \rho \cdot L = 0{,}0952 \ / \ dan \cdot 369{,}07 \ € = 35{,}15 \ € \ / \ dan \qquad (18)$$

Za reševanje tveganja okužbe z računalniškim virusom so izbrani tile mogoči ukrepi:

- ukrep A: osnovna protivirusna zaščita za delovne postaje, ki ne zahteva letnega podaljševanja naročnine za virusne definicije. Podjetje potrebuje licence za 40 delovnih postaj;
- ukrep B: protivirusna zaščita za delovne postaje in strežnike s centralnim posodabljanjem in analizo, pri čemer je potrebno letno podaljševanje naročnine za virusne definicije. Podjetje potrebuje licence za 40 delovnih postaj. To rešitev podjetje uporablja že sedaj;
- ukrep C: protivirusna zaščita, ki pregleduje promet na požarnem zidu, posredniku SMTP in delovnih postajah (poleg virusov pregleduje tudi za neželeno pošto). Omogoča centralno posodabljanje, potrebno je letno podaljševanje naročnine za virusne definicije;
- ukrep Č: vsakoletno izobraževanje in ozaveščanje uporabnikov s spletnimi izobraževanji;
- ukrep D: izdelava varnostnih kopij sistemov, kar zmanjšuje čas okrevanja okuženih sistemov (to velja le v primeru, če podatki na varnostnih kopijah niso okuženi z virusom). V nasprotju z drugimi ukrepi, ki so preventivni, je ta ukrep korektiven, ker blaži posledice v primeru incidenta;
- ukrep E: kombinacija protivirusne zaščite in izobraževanja uporabnikov (ukrepa B in Č).

Pri izračunu so namenoma izbrani preventivni in korektivni tehnološki ukrepi, izobraževanje uporabnikov ter kombinacija več ukrepov, da tako demonstriramo zmogljivost modela za medsebojno vrednotenje različnih vrst varnostnih ukrepov. Ocena karakteristik za stroške in učinkovitost izbranih ukrepov je zbrana v tabeli 1. V izračunu je časovno obdobje za investicijo štiri leta.

Tabela 1: **Ocena stroškov in učinkovitosti varnostnih ukrepov**

Ukrep	Strošek nabave in nadgradnje opreme	Stroški vzdrževanja	Učinkovitost ukrepa α (v 10^{-3})
A	Začetni stroški 1.766 evrov	Letno vzdrževanje 693 evrov	0,7691
B	Začetni stroški 1.481 evrov, letna nadgradnja 835 evrov (razen prvo leto)	Letno vzdrževanje 138 evrov	2,1018
C	Začetni stroški 6.484 evrov, letna nadgradnja 1.100 evrov	Letno vzdrževanje 277 evrov	1,1607
Č	Začetni stroški 1.646 evrov, nadgradnja 1.600 evrov (razen prvo leto)	Ni letnega vzdrževanja.	1. leto: 0,1482 2. leto: 0,2320 3. leto: 0,3157 4. leto: 0,3995
D	Začetni stroški 3.297 evrov	Letno vzdrževanje 1.387 evrov	0,1284
E	Začetni stroški 3.127 evrov, nadgradnja 2.435 evrov (razen prvo leto)	Letno vzdrževanje 138 evrov	1. leto: 0,9571 2. leto: 1,0062 3. leto: 1,0553 4. leto: 1,1044

Vrednotenje posameznih ukrepov je prikazano v tabeli 2, rezultati izračunov ROI, NPV in IRR pa v tabeli 3. Pri izračunu je upoštevana diskontna stopnja 2,7 odstotka.

Tabela 2: **Ekonomsko vrednotenje koristi in stroškov posameznih ukrepov**

	Ukrep A			Ukrep B			Ukrep C		
Leto	**Koristi (v evrih)**	**Stroški nabave in nadgradnje (v evrih)**	**Stroški vzdrževanja (v evrih)**	**Koristi (v evrih)**	**Stroški nabave in nadgradnje (v evrih)**	**Stroški vzdrževanja (v evrih)**	**Koristi (v evrih)**	**Stroški nabave in nadgradnje (v evrih)**	**Stroški vzdrževanja (v evrih)**
0		1.766			1.481			6.484	
1	2.391	0	693	6.099	0	138	7.535	1.100	277
2	2.391	0	693	6.099	835	138	7.535	1.100	277
3	2.391	0	693	6.099	835	138	7.535	1.100	277
4	2.391	0	693	6.099	835	138	7.535	1.100	277

	Ukrep Č			Ukrep D			Ukrep E		
Leto	**Koristi (v evrih)**	**Stroški nabave in nadgradnje (v evrih)**	**Stroški vzdrževanja (v evrih)**	**Koristi (v evrih)**	**Stroški nabave in nadgradnje (v evrih)**	**Stroški vzdrževanja (v evrih)**	**Koristi (v evrih)**	**Stroški nabave in nadgradnje (v evrih)**	**Stroški vzdrževanja (v evrih)**
0		1.646			3.297			3.127	
1	3.207	0	0	2.887	0	1.387	6.279	0	138
2	5.131	1.600	0	2.887	0	1.387	6.386	2.435	138
3	6.671	1.600	0	2.887	0	1.387	6.473	2.435	138
4	7.903	1.600	0	2.887	0	1.387	6.542	2.435	138

Tabela 3: **Izračun kazalnikov ROI, NPV in IRR za posamezne ukrepe**

Ukrep	ROI	NPV	IRR
A	111 %	4.591 evrov	89 %
B	437 %	18.522 evrov	390 %
C	151 %	16.571 evrov	87 %
Č	255 %	15.173 evrov	209 %
D	53 %	4.191 evrov	48 %
E	134 %	13.634 evrov	166 %

Praktični izračun lepo demonstrira uporabnost modela za vrednotenje in medsebojno primerjavo različnih vrst varnostnih ukrepov. Prva zanimiva ugotovitev je, da dajo vsi ukrepi pri vseh izračunanih kazalnikih pozitiven rezultat. Najbolj ekonomsko optimalna izbira je ukrep B, na drugem mestu je ukrep Č; ukrep E, ki je kombinacija ukrepov B in Č, pa je šele na četrtem mestu. Očitno v tem primeru cena skupnih ukrepov ne upraviči dodatne varnosti. Omeniti je treba še, da izračun za ukrep B, enako kot drugi ukrepi, vsebuje tudi nabavno ceno in uvedbo ukrepa. Če upoštevamo, da ima podjetje že uveden ta ukrep, odpadeta stroška za ukrep B, kar pomeni še boljši rezultat pri vseh kazalnikih.

5 SKLEP

Informacijska varnost je področje, za katerega se hitro povečuje zanimanje. Podjetja se čedalje bolj zavedajo, da je varnost eden izmed temeljnih elementov vsakega informacijskega sistema. Pri tem se zastavljata ključni vprašanji: Kako varen je informacijski sistem? in Kako varen bi moral biti informacijski sistem? Zavedati se je treba, da popolnoma varen sistem ne obstaja. Podjetje mora izbrati takšno stopnjo varnosti, ki je sprejemljiva zanj. Določitev ustrezne stopnje je zahtevna naloga, ki se izvaja v procesu upravljanja varnostnih tveganj.

Proces upravljanja tveganja pomaga podjetjem sprejeti odločitev glede potrebnih investicij v varnostne ukrepe, ki so za poslovanje podjetja najučinkovitejši. Temeljna strategija obvladovanja tveganja je zmanjšanje izpostavljenosti sredstva tveganju z uvedbo ustreznih tehnologij, orodij ali ustreznih postopkov. S tem se zmanjša verjetnost za škodljive dogodke ali omeji škoda, ki jo povzroči dogodek. Vlaganja v rešitve, povezane z informacijsko varnostjo, so torej neizogibna za vsa podjetja, ki so tako ali drugače vključena v proces elektronskega poslovanja. S stališča podjetja je varnost investicija, ki se meri v prihrankih denarnih enot.

Osebe, ki so v podjetjih odgovorne za investicije, seveda najbolj zanima, kam vlagati in predvsem koliko. Preden investiramo v določen produkt ali storitev, je dobro vedeti, ali je investicija finančno upravičena. Informacijska varnost pri tem ni nobena izjema. Zavedati pa se je treba, da je ekonomski pristop k upravljanju varnostnih tveganj in ocenjevanja optimalne investicije v informacijsko varnost obsežen projekt. Zahteva namreč poglobljeno analizo in vrednotenje informacijskih sredstev, analizo groženj, usmerjenih na informacijska sredstva, analizo posledic nedelovanja informacijske tehnologije, analizo verjetnosti za uspešno izveden napad ter oceno stroškov in koristi, ki so posledica vlaganj v informacijsko varnost.

V članku je predstavljen celovit model za upravljanje informacijskovarnostnih tveganj, ki omogoča oceno vlaganj v varnost in zaščito v poslovne informacijske sisteme. Razviti model temelji na kvantitativni analizi varnostnih tveganj in omogoča vrednotenje različnih možnosti investiranja v informacijsko varnost. Model je zasnovan kot standardni postopek, ki podjetje vodi od začetnega vnosa vhodnih podatkov do končnih priporočil za izbiro optimalnega ukrepa, ki zmanjšuje določeno varnostno tveganje. Največja prednost modela je, da omogoča neposredno primerjavo in kvantitativno vrednotenje različnih varnostnih ukrepov, od tehnoloških varnostnih rešitev, uvedbe organizacijskih postopkov, izobraževanja ali prenosa tveganja na zunanje podjetje. Izhodni podatek modela je donosnost posameznega ukrepa, merjena z ROI, NPV in IRR, ter primerjava posameznih ukrepov med seboj. Pri procesu ocene optimalnega obsega vlaganj v informacijsko varnost je treba kvantitativno ovrednotiti tako ranljivosti in grožnje, ki so vezane na neko informacijsko sredstvo, kot tudi ukrepe, ki zmanjšujejo ta tveganja. Kvantitativno vrednotenje teh parametrov je namreč podlaga za presojo ekonomske upravičenosti posamezne investicije s pomočjo kazalnikov ROI, NPV ter IRR. Model je bil praktično uporabljen in preverjen za konkretno podjetje, kar potrjuje njegovo pravilnost in učinkovitost. Zavedati pa se moramo, da so rezultati modela zelo odvisni od natančnosti vhodnih podatkov. Za določene grožnje trenutno primanjkuje dobrih zgodovinskih podatkov, na podlagi katerih lahko natančno določimo vhodne podatke. Pričakujemo lahko, da bo v prihodnje vse več razpoložljivih statističnih podatkov, kar bo pozitivno vplivalo na uporabo kvantitativnih pristopov.

5 LITERATURA IN VIRI

[1] Anderson, R. & Schneier, B. (2005). Economics of Information Security. IEEE Security and Privacy, 3(1), 12–13.

[2] Arora, A. & Telang, R. (2005). Economics of Software Vulnerability Disclosure. IEEE Security and Privacy, 3(1), 20–25.

[3] Bojanc, R. & Jerman-Blažič, B. (2008). An economic modelling approach to information security risk management. International Journal of Information Management, 28, 413–422.

[4] Bojanc, R., Jerman-Blažič, B. & Tekavčič, M. (2012). Managing the Investment in Information Security Technology by use of Quantitative Modeling Approach, Information Processing & Management, 22 str., [URL: http://dx.doi.org/10.1016/j.ipm.2012.01.001].

[5] Butler S. A. (2002). Security Attribute Evaluation Method: a Cost-Benefit Approach. The 24th International Conference on Software Engineering (ICSE '02) (str. 232–240). New York: ACM Press.

[6] Cavusoglu, H., Mishra, B., Raghunathan, S. (2004). A Model for Evaluating IT Security investments. Communications of the ACM, 47(7), 87–92.

[7] Computer Security Institute (CSI). (2010). CSI Survey 2010/2011. The 15th Annual Computer Crime and Security Survey. Dosegljivo na http://www.gocsi.com/survey.

[8] Cremonini, M. & Martini, P. (2005). Evaluating Information Security Investments from Attackers Perspective: the Return-on-Attack (ROA). Workshop on the Economics of Information Security (WEIS 2005). Najdeno 15. novembra 2006 na spletnem naslovu http://infosecon.net/workshop/schedule.php.

[9] Dacey, F. R. (2003). Effective Patch Management is Critical to Mitigating Software Vulnerabilities. United Stated General Accounting Office. GAO-03-1138T. Washington DC: United Stated General Accounting Office.

[10] ENISA. (2009). Inventory of risk assessment and risk management methods. Dosegljivo na: http://rm-inv.enisa.europa.eu/rm_ra_methods.html.

[11] Farahmand, F. (2004). Developing a Risk Management System for Information Systems Security Incidents. Atlanta: Georgia Institute of Technology.

[12] Gal-Or, E. & Ghose, A. (2005). The Economic Incentives for Sharing Security Information. Information Systems Research, 16(2), 86–208.

[13] Geer, D. (2004, 20. oktober). Q&A: Dan Geer on security of information when economics matters. SearchDataManagement.com. Dosegljivo na http://searchdatamanagement.techtarget.com/news/interview/0,289202,sid91_gci1139680,00.html.

[14] Gordon, A. L. & Loeb, P. M. (2002). The Economics of Information Security Investment. Communications of the ACM, 5(4), 438–457.

[15] Gordon, A. L. & Loeb, P. M. (2005). Managing Cybersecurity Resources: A Cost-Benefit Analysis, New York: McGraw Hill.

[16] International Organization for Standardization (ISO). (2004). ISO/IEC 13335-1:2004. Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management. Geneva: International Organization for Standardization (ISO).

[17] International Organization for Standardization (ISO). (2008). ISO/IEC 27005:2008. Information technology – Security techniques – Information security risk management. Geneva: International Organization for Standardization (ISO).

[18] International Organization for Standardization (ISO). (2009). ISO/IEC Guide 73:2009. Risk management – Vocabulary. Geneva: International Organization for Standardization (ISO).

[19] International Organization for Standardization (ISO). (2009). ISO/IEC 27000:2009. Information technology – Security techniques – Information security management systems – Overview and vocabulary. Geneva: International Organization for Standardization (ISO).
[20] Kaplan, R. (2007). A Matter of Trust. V H. F. Tipton & M. Krause (ur.). Information Security Management Handbook, 6th edition (str. 295–310). Boca Raton, Florida: Auerbach Publications.
[21] Matsuura K. (2008). Productivity Space of Information Security in an Extension of the Gordon-Loeb's Investment Model. Workshop on the Economics of Information Security (WEIS 2008). Dosegljivo na http://weis2008.econinfosec.org/program.htm.
[22] Mayer, N., Heymans, P., Matulevičius, R. (2007). Design of a modelling language for information system security risk management. The 1st International Conference on Research Challenges in Information Science (RCIS '07). Dosegljivo na http://www.nmayer.eu/publis/RCIS07-CR_NMA-PHE-RMA.pdf.
[23] Ryan, J. & Ryan, D. (2006) Expected benefits of information security investments. Computers & Security, 25, 579–588.
[24] Sandhu, R. (2003). Good-Enough Sercurity: Toward a Pragmatic Business-Driven Discipline. IEEE Internet Computing, 5(3), 66–68.
[25] Schneier, B. (2003). Beyond Fear: Think Sensibly about Security in an Uncertain World. New York: Copernicus Books.
[26] Schneier, B. (2004). Secrets & Lies, Digital Security in a Networked World. New York: Wiley Publishing.
[27] Soo Hoo, K. J. (2000). How Much Is Enough? A Risk-Management Approach To Computer Security. Palo Alto, CA: Stanford University.
[28] Tanaka, H., Liu, W. & Matsuura, K. (2006). An Empirical Analysis of Security Investment in Countermeasures Based on an Enterprise Survey in Japan. Workshop on the Economics of Information Security (WEIS 2006). Dosegljivo na http://weis2006.econinfosec.org/prog.html.
[29] Tanaka, H., Matsuura, K. & Sudoh, O. (2005). Vulnerability and information security investment: An empirical analysis of e-local government in Japan. Journal of Accounting and Public Policy, 24(1), 37–59.
[30] Willemson, J. (2006). On the Gordon&Loeb Model for Information Security Investment. Workshop on the Economics of Information Security (WEIS 2006). Dosegljivo na http://weis2006.econinfosec.org/prog.html.

▪

Rok Bojanc je zaposlen v ZZI, d. o. o., kot vodja storitev informacijske tehnologije in informacijske varnosti. Na področju informacijske tehnologije deluje že več kot petnajst let, izkušnje je pridobival na različnih področjih — od predavatelja, sistemskega inženirja, arhitekta do vodje projektov. Je avtor in soavtor več člankov in priročnikov s področja informacijske varnosti, elektronskega poslovanja, računalniških omrežij in strežniških sistemov. Pogosto predava na konferencah in seminarjih.

Analiza projektnega menedžmenta in projektne pisarne v izbrani organizaciji

Primož Panjan
Mercator, d. d., Dunajska 107, 1000 Ljubljana
primoz.panjan@mercator.si

Izvleček

Projektni menedžment ima v različnih organizacijah ali znotraj posamezne organizacije različne oblike in stopnje zrelosti, menedžerji in drugi zaposleni pa imajo različna pričakovanja od njegove uvedbe. Strateško planiranje projektnega menedžmenta v organizaciji pospeši njegovo uvajanje, zagotovi, da je projektni menedžment usklajen s poslovnimi cilji organizacije in potrebami ter željami menedžmenta in da v največji meri doprinese k izboljšanju poslovanja organizacije, ki tako laže dosega zastavljene cilje. Namen članka je predstaviti različne poglede na projektni menedžment in njegovo vzpostavljanje v organizaciji. Poleg tega je predstavljenih nekaj analiz trenutnega stanja in vzpostavljanja projektnega menedžmenta in projektne pisarne v izbrani organizaciji.

Ključne besede: projektni menedžment, projektna pisarna, zrelostni modeli, najboljše prakse, zrelost, odličnost.

Abstract

The Analysis of Project Management and Project Office in Selected Organization

Project management has in different organizations or within the same organization different shapes and levels of maturity therefore the managers and other employees have different expectations from its implementation. Strategic planning of the project management speeds up its deployment within the organization, ensures that project management is consistent with organization's business goals and the requests and needs of the management, and that it contributes to the greatest extent to the improvement of business as well as helps the organization to reach its business goals more easily. The purpose of this article is to present different views on project management and its implementation in the organization. In addition, some analyses of the current situation and the establishment of project management and project offices in the selected organization are presented.

Keywords: project management, project office, maturity models, best practices, maturity, and excellence.

1 UVOD

Vprašanja prenove poslovanja podjetij so najpogosteje vezana predvsem na prenovo poslovnih procesov ter zajemajo področja racionalizacije, standardizacije in poenostavitve postopkov ter uvajanja nujnih organizacijskih sprememb in razmer za uvedbo sodobnih konceptov skupinskega dela in sodobne informacijske tehnologije (Kovačič, 2005).

Na svetu ni enotnega recepta ali ene same metodologije, s pomočjo katere bi izboljšali poslovanje organizacije ali dela organizacije. Ne glede na to, kdaj in zakaj se organizacija odloči za korak prenove poslovanja, ima pri tem na voljo mnogo različnih pristopov, metodologij, metod, tehnik in orodij, s katerimi si lahko pomaga. S tem ko organizacije spoznavajo, kako ugoden učinek ima projektni menedžment na profitabilnost, dajejo vse večji poudarek doseganju profesionalizma v projektnem menedžmentu. In vprašanja, ki se porajajo danes, niso več toliko vezana na to, kako vpeljati projektni menedžment, temveč kako hitro ga lahko vpeljemo, kako hitro lahko postanemo zreli na področju projektnega menedžmenta in ali lahko uporabimo najboljšo prakso za pospešitev uvedbe projektnega menedžmenta v organizacijo.

Članek obravnava vzpostavljanje projektnega menedžmenta v organizaciji ter nekaj različnih analiz projektnega menedžmenta in projektne pisarne v izbrani organizaciji.

2 VZPOSTAVLJANJE PROJEKTNEGA MENEDŽMENTA IN PROJEKTNE PISARNE V ORGANIZACIJI

Stanje projektnega menedžmenta v organizaciji bi lahko poenostavljeno opisali kot najboljše prakse, zrelost ali odličnost projektnega menedžmenta. Kerzner (2010) navaja, da so najboljše prakse tiste aktivnosti, ki jih organizacija identificira in izvaja z namenom doseči konkurenčno prednost v projektnem menedžmentu, istočasno pa prinašajo vrednost

organizaciji in strankam. Najboljše prakse obstajajo v obliki nenapisanih priporočil ali v formalni obliki kot brošura. Najboljše prakse lahko oblikujemo v ravni od zelo obsežnih in vsesplošnih najboljših praks do bolj kompleksnih najboljših praks znotraj neke organizacije ali zelo kompleksnih najboljših praks posameznikov. Nekatere organizacije vzdržujejo le knjižnice najboljših praks, nekatere organizacije pa po identificiranju in validiranju najboljših praks pristopijo k pripravi metodologije projektnega menedžmenta. V tem primeru metodologija prevzame vlogo najboljših praks v organizaciji. Kot navaja Kerzner (2010), organizacije, ki vzpostavijo metodologijo projektnega menedžmenta in implementirajo orodje v podporo metodologiji, dosežejo določeno stopnjo zrelosti projektnega menedžmenta v organizaciji. V okviru zrelosti organizacija stremi k standardizaciji postopkov, kar ji prinese koristi v spremljanju in nadzoru projektov ter omogoča bolj učinkovito izvajanje procesov projektnega menedžmenta. Zrelost projektnega menedžmenta pa ni dovolj za nenehno uspešno vodenje projektov. Zato nekatere organizacije še nadgrajujejo svoje poslovno okolje na področjih, ki vplivajo na učinkovitost procesov projektnega menedžmenta in se podajajo na pot doseganja odličnosti projektnega menedžmenta. Organizacije, ki so postale zelo uspešne v projektnem menedžmentu, stremijo k temu, da presežejo dosežke konkurence na področju integracije procesov, kulturi, podpori menedžmenta, usposabljanju, neformalnem projektnem menedžmentu in odličnosti vedenja.

Najboljše prakse pomenijo trenutni, v okviru določene gospodarske veje priznani optimalni način doseganja poslovnih ciljev. V okviru projektnega menedžmenta se najboljše prakse nanašajo na sposobnost organizacije, da izvaja projekte predvidljivo, konsistentno in uspešno ter tako uresničuje svojo strategijo. Najboljše prakse so dinamične, saj se nenehno razvijajo skladno z izboljšanjem obstoječih in razvojem novih načinov doseganja poslovnih ciljev. Uporaba najboljših praks poveča verjetnost uspešnega doseganja poslovnih ciljev (PMI, 2003). Nekateri inštituti, npr. PMI (angl. *Project Management Institute*) z zrelostnim modelom projektnega menedžmenta organizacije (OPM3) in OGC (angl. *Office of Government Commerce*) z najboljšo prakso upravljanja informatike v organizaciji (ITIL), pripravljajo kompleksne publikacije najboljše prakse. Drugi v podporo poslovanju pripravijo enostavne in pregledne najboljše prakse, ki ne presegajo devet alinej, kot npr. organizacija Antares Management Solutions (Kerzner, 2010).

Sowden (2008) navaja, da uporaba modela P3M3 (opisan v nadaljevanju) v organizaciji poveča uspešnost projektov in kakovost projektnih izdelkov ter storitev s tem, da projektni menedžment v organizaciji prevede iz stanja nezrelosti v stanje zrelosti. Nezrele in zrele organizacije pri tem okarakterizira takole:

- nezrele organizacije lahko posamezne iniciative odlično izvedejo, vendar obstaja velika verjetnost, da menedžerji v takem okolju reagirajo bolj reaktivno kot proaktivno. Verjetnost prekoračitve dogovorjenih rokov in stroškov je zaradi slabih tehnik pripravljanja kalkulacij velika, želja po doseganju rokov pa lahko zaradi opuščanja ali slabe izvedbe določenih projektnih aktivnosti ogrozi kakovost izdelkov ali storitev;
- zrele organizacije imajo na ravni organizacije vzpostavljene standardizirane procese projektnega menedžmenta. Procesi so prilagojeni specifikam organizacije in se nenehno izpopolnjujejo. Projektne skupine in deležniki na projektu so seznanjeni s standardnimi procedurami ter jih upoštevajo, projektne aktivnosti pa izvajajo skladno s pripravljenim planom projekta. Vloge in odgovornosti so dobro definirane in sprejete na ravni organizacije. Menedžerji spremljajo izvajanje projekta, kakovost dogovorjenih izdelkov in storitev ter zadovoljstvo strank. Zrele organizacije posedujejo znanje in kvantitativne informacije, s pomočjo katerih merijo dosežke in ocenjujejo doseganje rokov in stroškov projekta, veliko pozornost pa posvečajo tudi učenju iz preteklih projektov ter pridobivanju potrebnih znanj in kompetenc za izvajanje aktivnosti projektnega menedžmenta.

Kot navaja Kerzner (2010), je odličnost v projektnem menedžmentu definirana kot nenehno uspešno vodenje projektov. Če organizacija nekaj projektov konča uspešno, še ne pomeni, da je v celoti uspešna na področju projektnega menedžmenta. Kateri koli projekt je lahko uspešno voden s formalno avtoritativnostjo in pod močnim vplivom menedžmenta. Da bi dosegli nenehno uspešno vodenje in zaključevanje projektov, mora v organizaciji obstajati vidna korporativna zavezanost do projektnega menedžmenta. Preprosta uporaba principov projektnega menedžmenta, čeprav v daljšem časovnem

obdobju, ne vodi nujno v odličnost. Nasprotno, lahko vodi do ponavljajočih se napak ali – kar je lahko še huje – do učenja na lastnih napakah, namesto da bi se učili na napakah drugih.

Kerzner (2010) nadalje navaja, da je organizacija, ki spozna potrebo po uvedbi ali dvigu zrelosti projektnega menedžmenta, postavljena pred izziv, kako to čim hitreje izvesti in kako pri tem izkoristiti mnoga obstoječa znanja in priporočila s tega področja. Uvajanje projektnega menedžmenta lahko skrajša s strateškim planiranjem projektnega menedžmenta, v okviru katerega uporabi že znane principe strateškega načrtovanja in pripravljene zrelostne modele projektnega menedžmenta. Organizacija v okviru strateškega načrtovanja projektnega menedžmenta oblikuje poslanstvo, vizijo in cilje projektnega menedžmenta ter pripravi načrt za doseganje želenega stanja. Kot navaja Kovačič (2005), je razširjena metoda ključnih dejavnikov uspeha uporabna v vseh razvojnih fazah na področju prenove in informatizacije poslovanja, še posebno pa je učinkovita in jo priporočajo na strateškem področju načrtovanja in analiziranja informacijskih potreb ter pri modeliranju poslovnih procesov in podatkov organizacije.

V postopku strateškega planiranja projektnega menedžmenta organizacija spozna stanje, v katerem se nahaja in na podlagi razhajanja med trenutnim in želenim stanjem pripravi korake za doseganje želenega stanja. Organizacija na podlagi svojega strateškega načrta pripravi zrelostni model, ki mu želi slediti, ali pa za to uporabi enega izmed pripravljenih modelov, ki so na voljo. Ti modeli običajno vsebujejo smernice za analiziranje trenutnega stanja projektnega menedžmenta v organizaciji in s tem omogočajo ocenjevanje stopnje zrelosti organizacije na področju projektnega menedžmenta. S pomočjo rezultatov analize ugotovimo razhajanja med tem, kar priporoča stroka, in tem, kar počne organizacija, ter na podlagi ugotovitev pripravimo akcijske načrte oz. strategije za doseganje višje stopnje zrelosti projektnega menedžmenta.

Koncept projektne pisarne nadgrajuje moderen pristop projektnega menedžmenta s področji spremljanja, nadzora in podpore projektnemu menedžmentu. Projektna pisarna je postavljena v vlogo poslovnega integratorja, ki združuje vse ljudi (ključne udeležence projektov), procese (metodologije in prakse) in orodja (avtomatizirane sisteme in delovne pripomočke), s pomočjo katerih vodimo projekte ali ki vplivajo nanje. Projektna pisarna pomaga projektnim menedžerjem in organizaciji razumeti ter usvojiti prakso projektnega menedžmenta in integrirati poslovne interese z aktivnostmi projektnega menedžmenta (Hill, 2004).

Ne glede na to, kako imenujemo projektno pisarno v organizaciji, je njena temeljna vloga izboljšanje učinkovitosti in uspešnosti projektnega menedžmenta v organizaciji. Glede na to, da ima vsakdo v organizaciji svoj pogled na želene rezultate izboljšav, ima lahko projektna pisarna v različnih organizacijah popolnoma različne oblike in naloge (Kendal in Rollins, 2003). Temu pritrjuje tudi Hobbs (2006), ki je v okviru svoje raziskave ugotovil, da so projektne pisarne od organizacije do organizacije različne, podobnosti pa ni moč zaslediti niti v okviru geografskih, ekonomskih ali drugih okvirov.

Nekateri izmed modelov, ki jih lahko organizacija uporabi v pomoč pri strateškem planiranju projektnega menedžmenta ter za doseganje zrelosti v razumnem roku, so:

- ***PMI Organizational Project Management Maturity (OPM3)*** Model OPM3 je model PMI, ki opisuje uvedbo principov projektnega menedžmenta na ravni organizacije. OPM3 je namenjen v pomoč organizacijam pri preoblikovanju strategije v ponavljajoče in predvidljive uspešne rezultate. Tako kot drugi standardi PMI tudi ta ne predpisuje, katere spremembe naj organizacija izpelje in kako, temveč ponuja model kot podlago za nadaljnje študije in samoocenjevanje in da omogoči organizacijam, da same sprejmejo odločitve o potrebnih spremembah;
- ***OGC's Portfolio, Programme and Project Management Maturity Model (P3M3)*** Model P3M3 je model samostojne pisarne ministrstva za finance Velike Britanije (angl. *The Office of Government Commerce (OGC) – an independent office of HM Treasury*). Model se v izhodiščih v veliki meri navezuje na model *Capability Maturity Model* (CMM). S pomočjo modela P3M3 organizacije ocenijo trenutne dosežke in pripravijo načrte izboljšav menedžmenta portfelja, programov in projektov;
- ***Portfolio, Programme and Project Office*** **(P3O)** P3O je OGC-jev zrelostni model projektne pisarne. Model P3O obravnava vzpostavitev pisarne v podporo menedžmentu sprememb na vseh ravneh v organizaciji. Z implementacijo modela P3O

pridobi organizacija strukture, orodja in tehnike, ki jih potrebuje, da vzpostavi prave programe in projekte, da poveže spremembe s poslovnimi potrebami in da si zagotovi ustrezne vire in sposobnosti za njihovo nenehno in kakovostno izvajanje;

- ***ASAPM Performance Rated Organization* (aPRO)** aPRO je standard za ocenjevanje dosežkov projektnega menedžmenta organizacije, ki ga je pripravilo ameriško združenje za napredek projektnega menedžmenta (angl. *American Society for the Advancement of Project Management – ASAPM*). S pomočjo standarda aPRO izmerimo dosežke projektnega menedžmenta v organizaciji; z njim ocenimo mejno kompetenco oz. minimalno stopnjo učinkovitosti (dosežkov), ki je potrebna, da zanesljivo dosežemo uspešne rezultate projektov, ki jih izvajamo;
- ***The Complete Project Management Office Handbook*** (Hill, 2004 in 2008) Avtor modela Hill Gerard ovrednoti zrelost projektnega menedžmenta v organizaciji skozi zrelost projektne pisarne in njenih kompetenc v organizaciji. Model predvideva pet stopenj zrelosti pisarne, pri čemer je v peti, najvišji stopnji, projektna pisarna opredeljena kot središče odličnosti (angl. *Center of Excellence*) s strateško vlogo v organizaciji. Model je osredinjen na to, kaj narediti, če bi želeli v organizaciji vzpostaviti ustrezno funkcionalno projektno pisarno, kot jo potrebuje organizacija;
- ***Gartnerjev zrelostni model za projektno pisarno*** (Fitzgerald, 2008) Model je pripravljen na podlagi izkušenj Gartnerjevih raziskovalcev in pogovorov s strankami. Model nadgrajuje Gartnerjev zrelostni model PPM (Mieritz, Fitzgerald, Gomolski & Light, 2007) s tem, da za posamezno stopnjo zrelosti projektnega menedžmenta v organizaciji predlaga ustrezno obliko projektne pisarne.

Vsaka organizacija zase mora skrbno pretehtati izbiro ustreznega modela, ki bi ga želela uporabiti, in razumeti, kam jih bo pripeljal model, če ga bodo upoštevali.

3 ANALIZA PROJEKTNEGA MENEDŽMENTA IN PROJEKTNE PISARNE V IZBRANI ORGANIZACIJI

V okviru analize je na podlagi interne ankete, lastnega modela in standarda aPRO ocenjeno stanje projektnega menedžmenta v organizacijski enoti informatike izbrane organizacije primerjana trenutna strategija dviga zrelosti projektnega menedžmenta s priporočili stroke ter na podlagi Hillovega modela analizirane trenutne in planirane funkcije projektne pisarne.

3.1 Metode

Z metodo analize sta analizirani stanji projektnega menedžmenta in projektne pisarne v izbrani organizacijski enoti, ki je že v temelju usmerjena projektno, to je informatika (v nadaljevanju bo nevtralno imenovana OE IT). V nadaljevanju so opisana področja analiziranja in uporabljene tehnike.

Analiza načina izvajanja aktivnosti Analiza načina izvajanja aktivnosti je izvedena z uporabo lastne klasifikacije načina izvajanja aktivnosti, ki je podrobneje razložena v razdelku 3.1.1. S pomočjo te klasifikacije in z uporabo interne dokumentacije, ki med drugim vključuje analizo vključenosti zaposlenih OE IT v posamezno vrsto aktivnosti, je pripravljena tabela, ki prikazuje potencialni vpliv projektnega menedžmenta in projektne pisarne na vse vrste aktivnosti, ki jih izvajajo v OE IT.

Ocena stanja projektnega menedžmenta po standardu aPRO V preteklosti so večinoma merili posameznikove kompetence, to je njegovo sposobnost za izvajanje nekega področja dela, zadnjih deset let pa merijo tudi kompetence organizacije. Obstajata dva pristopa za določanje kompetence, to je na podlagi:

- atributov, pri čemer kompetenco določimo na podlagi specifičnih karakteristik organizacije in vnaprej definiranih atributov;
- učinkov (dosežkov), pri čemer za merjenje kompetenc uporabljamo neposredno merljive izide poslovnih aktivnosti.

Standard aPRO spada med t. i. »kompetenčne standarde na podlagi dosežkov« (angl. *performance-based competence standards – PBCS*). S pomočjo standarda aPRO izmerimo dosežke projektnega menedžmenta v organizaciji; z njim ocenimo mejno kompetenco oz. minimalno stopnjo učinkovitosti (dosežkov), ki je potrebna, da zanesljivo dosežemo uspešne rezultate projektov, ki jih izvajamo.

Analizo po standardu aPRO izvedejo šolani ocenjevalci, lahko pa organizacija izvede samoocenjevanje. Samoocenjevanje OE IT smo izvedli štirje zaposleni, ki se v OE IT ukvarjamo s projektnim menedžmentom, samoocenjevanje pa je potekalo na podlagi našega poznavanja načina dela na projektih. Analiza je zajela vse projektne aktivnosti, na katerih

so udeleženi zaposleni OE IT, ne glede na to, ali je projekt injiciran znotraj ali zunaj OE IT.

Analiza strategije dviga zrelosti projektnega menedžmenta V analizi je primerjan pristop OE IT do strateškega planiranja projektnega menedžmenta s priporočili stroke ter heksagonom odličnosti po Kerznerju (2010).

Analiza vzpostavitve projektne pisarne ter njenih vlog in odgovornosti V okviru analize so primerjane obstoječe in planirane funkcije projektne pisarne s Hillovim (Hill, 2008) zrelostnim modelom projektne pisarne. Analiza je dopolnjena s podatki ankete o stanju projektnega menedžmenta, ki se je v izbrani organizaciji izvajala na začetku leta 2011 neodvisno od članka (Panjan, 2011).

3.1.1 Model opredeljevanja načina izvajanja aktivnosti

V okviru raziskovanj nismo zasledili enotne in čiste definicije, kdaj neko aktivnost opredelimo kot projektno ali neprojektno. Tako tudi ne moremo preprosto opredeliti, kdaj in na katere aktivnosti imata principa projektnega menedžmenta in projektne pisarne večji ali manjši vpliv. Podobnosti med operativnim delom in projektnimi aktivnostmi je ugotovil že PMI (PMI, 2008), poleg tega lahko pri opredeljevanju vrst procesov in projektov opazimo podobne definicije, kot npr. glede obvladljivosti (procesi in projekti so lahko deterministični ali stohastični) ali glede ponovljivosti (procesi so lahko diskretni ali kontinuirani, projekti pa enkratni ali multiprojektni). Iz vsega navedenega torej lahko ugotovimo, da v različnih organizacijah glede na različna merila kot projektne različno označimo malo ali pa mnogo aktivnosti. Torej imata lahko projektni menedžment in s tem projektna pisarna večji ali manjši vpliv na mnogo aktivnosti v organizaciji.

Da bi laže ocenili vpliv projektnega menedžmenta in projektne pisarne na aktivnosti v organizaciji, sem pripravil lastno klasifikacijo, kdaj bi aktivnosti opredelili kot projekt oz. kdaj jih ne opredelimo kot projekt in jih raje obravnavamo kot proces. Pri definiciji smo kombinirali predvidljivost in ponovljivost aktivnosti, kar po klasifikacijah procesov in projektov povežemo z obvladljivostjo (predvidljivost) in ponovljivostjo (ponovitev). Klasifikacija je prikazana v tabeli 1.

Tabela 1: **Kako pristopiti k izvajanju aktivnosti: procesno ali projektno**

Predvidljivost / Ponovljivost	Predvidljive aktivnosti	Delno predvidljive aktivnosti	Nepredvidljive aktivnosti
Ponovljive aktivnosti	Proces brez različic ali z dobro definiranimi različicami	Proces z delno definiranimi različicami	Projekt, ki prehaja v proces
Delno ponovljive aktivnosti	Proces z delno definiranimi različicami	Mešano	Projekt
Neponovljive aktivnosti	Proces, ki se izvaja kot projekt	Projekt	Projekt

Vir: P. Panjan, Pomen projektne pisarne za učinkovito izvajanje poslovnih procesov podjetja, 2011, tabela 7.

Tabela 1 opredeljuje pristope k izvajanju aktivnosti v organizaciji glede na karakteristike ponovljivosti in predvidljivosti aktivnosti. Na podlagi teh karakteristik opredelimo, ali naj aktivnosti obravnavamo in definiramo kot procese, naj jih izvajamo in izvedemo kot projekte ali pa se odločimo za eno ali drugo glede na trenutne želje in potrebe. Predvidljive aktivnosti so tiste, za katere smo prepričani, da se v okviru njihovih izvedb ne morejo pojaviti nova tveganja in nepredvideni problemi in katerim dokaj natančno določimo trajanje in rok izvedbe. Nepredvidljive aktivnosti pa so tiste, ki so močno podvržene tveganjem, pri katerih obstaja večja verjetnost pojava problemov in pri katerih sta trajanje ter rok večinoma le predvidena oz. planirana. Ponovljive so tiste aktivnosti, ki se izvajajo nenehno, kot npr. v procesni industriji, neponovljive pa tiste, ki so enkratne ali se izvedejo zelo redko.

Pri klasificiranju je proces opredeljen kot skupek delovnih postopkov in aktivnosti, ki se v organizaciji pogosto ponavlja in je zelo predvidljiv, čisti projekt pa kot skupek delovnih postopkov in aktivnosti, ki se oblikuje vedno znova in je skladno s predhodno definicijo nepredvidljiv.

V tabeli 2 je podana ocena vpliva projektnega menedžmenta in projektne pisarne na posamezen način izvajanja aktivnosti.

Tabela 2: **Vpliv projektnega menedžmenta in projektne pisarne na način izvajanja aktivnosti**

Način izvajanja aktivnosti	Vpliv PM in PP
Proces brez različic	»1 – brez vpliva«
Proces z dobro definiranimi različicami	»1 – brez vpliva«
Proces z delno definiranimi različicami	»2 – nizek vpliv«
Proces, ki se izvaja kot projekt	»3 – srednje močan vpliv«
Projekt, ki prehaja v proces	»4 – močan vpliv«
Mešano	Od »1 – nizek vpliv« do »4 – močan vpliv«
Projekt	»4 – močan vpliv«

Legenda: PM – projektni menedžment; PP – projektna pisarna.

Vir: P. Panjan, Pomen projektne pisarne za učinkovito izvajanje poslovnih procesov podjetja, 2011, tabela 9.

Na splošno bi opredelili, da bolj kot se aktivnosti karakteristično približujejo projektu, bolj za doseganje večje učinkovitosti aktivnosti uporabimo znanja in veščine projektnega menedžmenta, in nasprotno, bolj kot so aktivnosti procesno specificirane, manjši vpliv imata na njih projektni menedžment in projektna pisarna. V vseh vmesnih oblikah aktivnosti izvajamo kombinirano. To pomeni, da za doseganje ciljev uporabimo že definirane procese, trenutna razhajanja med specificiranim procesom in dejanskim stanjem pa zapolnimo s konceptom projektnega menedžmenta.

3.2 Rezultati analize

3.2.1 Analiza načina izvajanja aktivnosti

Rezultati analize so prikazani v tabeli 3. Delež predstavlja odstotek časa, ki ga zaposleni v OE IT porabijo v okviru posameznega načina izvajanja aktivnosti.

Tabela 3: **Vpliv projektnega menedžmenta in projektne pisarne na aktivnosti OE IT**

Način izvajanja aktivnosti	Delež (v %)	Vpliv PM in PP	Način izračuna
Proces brez različic	3	1	
Proces z dobro definiranimi različicami	10	1	
Proces z delno definiranimi različicami	25	2	
Proces, ki se izvaja kot projekt	5	3	
Projekt, ki prehaja v proces	2	4	
Mešano	30	1–4	
Projekt	25	4	
Skupaj			

Način izvajanja aktivnosti	Delež (v %)	Vpliv PM in PP	Način izračuna
Vpliv št. 1	20,5		3 + 10 + 7,5 (¼ od 30)
Vpliv št. 2	32,5		25 + 7,5 (¼ od 30)
Vpliv št. 3	12,5		5 + 7,5 (¼ od 30)
Vpliv št. 4	34,5		2 + 7,5 (¼ od 30) + 25

Legenda: PM – projektni menedžment; PP – projektna pisarna; vpliv glede na klasifikacijo iz tabele 2.

Vir: P. Panjan, Pomen projektne pisarne za učinkovito izvajanje poslovnih procesov podjetja, 2011, tabela 10.

Kot je navedeno v razdelku 3.1.1, bolj kot se aktivnosti karakteristično približujejo projektu, bolj za doseganje večje učinkovitosti uporabimo znanja in veščine projektnega menedžmenta. Glede na tabelo 3 imata projektni menedžment in projektna pisarna močan vpliv (4) na 34,5 odstotka aktivnosti, srednji vpliv (3) na 12,5 odstotka aktivnosti in manjši vpliv (2) na 32,5 odstotka aktivnosti, ki se izvajajo v okviru OE IT. Če se osredinimo le na srednji in večji vpliv, imata projektni menedžment in projektna pisarna relativno močan vpliv na izvajanje 47 odstotkov aktivnosti, ki jih izvaja OE IT, kar pomeni skoraj polovico vseh aktivnosti OE IT.

3.2.2 Ocena stanja projektnega menedžmenta po standardu aPRO

Rezultati analize po standardu aPRO so predstavljeni v tabeli 4. Enote in elementi so v tabeli navedeni v celoti, merila učinkovitosti pa le z zaporednimi številkami. D in N pomenita oceno posameznega merila učinkovitosti, pri čemer D pomeni, da OE IT izpolnjuje merila, N pa, da jih ne izpolnjuje.

Tabela 4: **Rezultati analize po standardu aPRO**

Enota	Element	Merilo učinkovitosti				
		1	2	3	4	5
aPRO-01: Usklajenost projektov s strategijo organizacije	1.1: Oblikovanje in vzdrževanje organizacijskih strateških usmeritev	N	N	N		
	1.2: Menedžment celovitega portfelja projektov organizacije	N	N	N		
aPRO-02: Zagotavljanje podpore vodstva vodenju projektov	2.1: Podpiranje učinkovitega nadzora in kontrole projektov	D	N	N	N	
	2.2: Odzivanje na rezultate projektnega menedžmenta	N	D	N	N	
	2.3: Ocenjevanje realiziranih koristi	D	N	N		
aPRO-03: Zagotavljanje zadostnih virov za izvedbo projektov	3.1: Zagotavljanje zadostne projektne skupine za odobrene projekte	N	D	D	N	D
	3.2: Zagotavljanje zadostnih finančnih virov za odobrene projekte	D	D	D	D	D
	3.3: Zagotavljanje zadostnih drugih virov in druge podpore za odobrene projekte	N	N	N	N	D
aPRO-04: Razvoj skupin projektnega menedžmenta	4.1: Razvoj projektnih menedžerjev	N	N	N	N	
	4.2: Razvoj drugih udeležencev na projektu	D	N	N		
aPRO-05: Zagotavljanje zanesljivih navodil za projektni menedžment	5.1: Oblikovanje in vzdrževanje praks projektnega menedžmenta	N	D	N		
	5.2: Oblikovanje in vzdrževanje definicij življenjskega cikla projekta	N	N	N	N	

Vir: Prirejeno po ASAPM, asapm Performance Rated Organization Standard for Assessing Organizational Project Management Performance, 2010.

Kot lahko ugotovimo iz rezultatov analize, izvaja OE IT skladno s standardom aPRO le v okviru enega elementa vse predlagane aktivnosti, to je zagotavljanje zadostnih finančnih virov za odobrene projekte. Nadalje, OE IT delno izvaja aktivnosti v okviru zagotavljanja zadostne projektne skupine za odobrene projekte, v vseh preostalih elementih pa jih izvaja malo ali nič.

Ocena stanja projektnega menedžmenta v OE IT po standardu aPRO je pokazala, da OE IT dosega kompetence le v okviru enega elementa standarda (3.2). Skladno z oceno po standardu aPRO menimo, da OE IT dokaj dobro obvladuje le elemente standarda, ki omogočajo preživetje projektov, na večini področij projektnega menedžmenta pa dosega slabše rezultate.

3.2.3 Analiza strategije dviga zrelosti projektnega menedžmenta

Skladno z življenjskim ciklom projektnega menedžmenta se je v OE IT v nekem trenutku prepoznala potreba po vpeljavi konkretne oblike projektnega menedžmenta, temeljno gibalo pri tem pa je bila višja učinkovitost in uspešnost projektov. Do tedaj so se projekti sicer izvajali, ni pa obstajal projektni menedžment v taki obliki, da bi bilo mogoče identificirati vse njegove karakteristike (procesi, vloge in odgovornosti, merila uspešnosti ipd.). Strateškega načrta projektnega menedžmenta v neki posebni obliki ni bilo, so se pa v okviru projekta, katerega namen je bil dvigniti raven zrelosti projektnega menedžmenta, vzpostavile nekatere srednjeročne strateške usmeritve. Izmed modelov, ki so bili na voljo, so se v okviru projekta uporabila priporočila PMI in njihovega standarda PMBOK tretje izdaje.

Tak način priprave strateških usmeritev se je izkazal za neuspešnega, saj vodstvo ni imelo pred seboj neprestanega pregleda nad uvedbo in smiselnostjo projektnega menedžmenta. Z interno reorganizacijo je novo vodstvo OE IT pozabilo na nekatere temeljne dogovore in usmeritve in dvigovanje zrelosti projektnega menedžmenta v OE IT je zamrlo. Rezultat projekta je sicer pripravljena metodologija projektnega menedžmenta skladno s standardom PMBOK in orodje v njeno podporo. Nekateri posamezniki so spoznali koristi enega in drugega ter ju do neke mere uporabljajo, a celovita in dokončna izvedba koncepta čaka na boljše čase. Neustrezno planiranje in izvajanje projektnega menedžmenta potrjujejo tudi slabi rezultati analize področij, ki jih opredeljuje heksagon odličnosti: procesi projektnega menedžmenta niso integrirani z drugimi procesi, kultura projektnega menedžmenta je na nizki ravni, menedžment le medlo podpira projektni menedžment, usposabljanje za projektni menedžment se ne izvaja redno, projektne skupine v veliki meri uporabljajo neformalni projektni menedžment, ki ne prinaša ustreznih rezultatov ipd.

3.2.4 Analiza vzpostavitve projektne pisarne ter njenih vlog in odgovornosti

V trenutku vzpostavitve projekta priprave metodologije in orodja projektnega menedžmenta, omenjenega v razdelku 3.2.3, so v OE IT izvajali tri večje projekte, znotraj katerih so obstajale tri projektne pisarne najnižje ravni. Po Wysockovi (2007) umeščenosti v organizacijo bi jih opredelili kot začasne projektne pisarne, glede na stopnje zrelosti projektne pisarne po Hillu (2004) pa v projektne pisarne prve ravni. Če primerjamo cilj projekta z omenjenima konceptoma oblike in stopnje projektne pisarne, je bil cilj projekta vzpostaviti po Wysockem (2007) projektno pisarno poslovne enote z vlogo, kot je predvidena v tretji stopnji po Hillu (2004).

V OE IT so se v okviru projekta združile vse tri začasne projektne pisarne v posebno organizacijsko enoto. Po združitvi in po končanju projekta so izvedli analizo trenutnega izvajanja aktivnosti projektne pisarne glede na model po Hillu (2008). Rezultati analize na najvišji ravni so prikazani v tabeli 5.

Tabela 5: **Analiza trenutnega izvajanja aktivnosti projektne pisarne OE IT (v %)**

Skupina	Področje	Implementirano
Integracija virov	Karierni razvoj	0
	Razvoj skupin	0
	Šolanje in izobraževanje	7
	Ravnanje s človeškimi viri	8
Praksa menedžmenta	Metodologija projektnega menedžmenta	33
	Orodja projektnega menedžmenta	36
	Standardi in metrike	20
	Menedžment znanja projektnega menedžmenta	31
Strokovna podpora	Mentorstvo	8
	Podpora planiranju	31
	Reševanje projektov	8
	Revizije projektov	8
Menedžment infrastrukture	Ocenjevanje	7
	Organizacija in struktura	23
	Menedžment prostora in opreme	18
	Upravljanje projektov	27
Usklajenost s poslovanjem	Menedžment odnosa s kupci	0
	Menedžment odnosa z dobavitelji in s pogodbeniki	0
	Menedžment dosežkov poslovanja	17
	Menedžment portfelja projektov	8
Skupaj		15

Vir: Prirejeno po G. M. Hill, The complete project management office handbook, 2008.

Tabela 5 vsebuje skupine in področja aktivnosti, kot jih je opredelil Hill. V okviru vsakega področja je Hill predvidel več aktivnosti in ravni aktivnosti, ki bi jih izvajala projektna pisarna na lestvici kompetenčne sposobnosti. Glede na to, da naj bi projektna pisarna, ki izvaja aktivnost na določeni stopnji kompetenčne sposobnosti, predhodno že izvajala to aktivnost na nižji stopnji, se zrelost analizirane projektne pisarne kaže v tabeli kot odstotek izvajanja teh aktivnosti. Če projektna pisarna izvaja polovico vseh predvidenih aktivnosti na lestvici od najmanj do najbolj zrelega stanja teh aktivnosti in je na lestvici kompetenčnosti na sredini, to je na stopnji standardne projektne pisarne po Hillu, pomeni, da dosega 50 odstotkov nekega področja.

Rezultati analize kažejo, da je OE IT izpolnila projektne cilje pripraviti metodologijo projektnega menedžmenta in orodja v podporo, saj sta najvišje ocenjeni ravno ti dve področji. Dokaj dobro sta pokriti skupini aktivnosti prakse menedžmenta in menedžment infrastrukture. Po drugi strani pa so izjemno slabo ocenjena področja kariernega razvoja

in razvoja skupin ter menedžmenta odnosa s kupci, z dobavitelji in s pogodbeniki. Vendar navedena nizka ocena še ni razlog za preplah. Kot je navedeno v razdelku 2, si organizacija sama postavi cilje glede funkcionalnosti, ki jih želi obvladovati, in stopnjo kompetenčne sposobnosti, ki jo potrebuje. S pomočjo predpripravljenega modela organizacija ugotovi razhajanja med dejanskim in želenim stanjem ter na tej podlagi pripravi akcijski načrt.

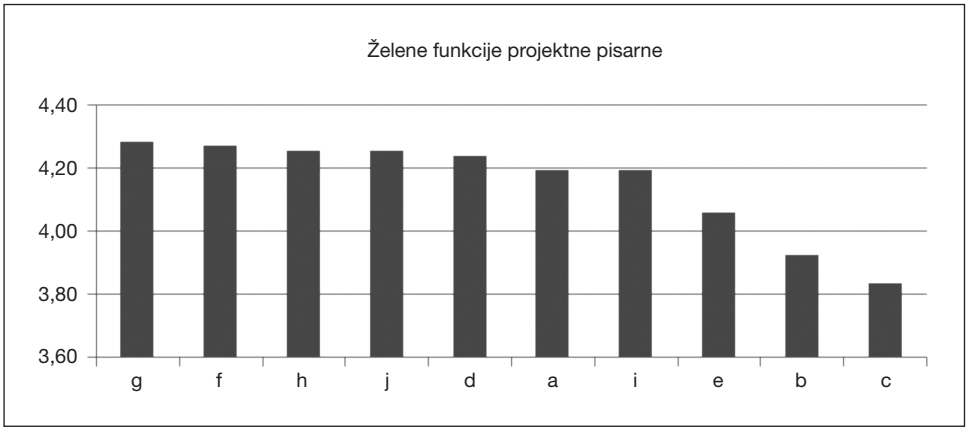
Primerjava analize trenutnega stanja projektne pisarne z rezultati interne ankete nakazujejo, da trenutno vzpostavljena projektna pisarna ne zadostuje željam oz. potrebam zaposlenih v OE IT. Anketiranci namreč menijo, da naj bi projektna pisarna izvajala večino aktivnosti, navedenih v anketi, analiza pa kaže, da se te aktivnosti le delno izvajajo v okviru obstoječe projektne pisarne.

Tabela 6: **Rezultati interne ankete glede funkcij projektne pisarne**

Želene funkcije projektne pisarne	**Ocena**
g) Mentorstvo in svetovanje projektnim skupinam	4,28
f) Šolanje in usposabljanje za projektni menedžment	4,27
h) Priprava in vzdrževanje standardov, obrazcev in predlog	4,25
j) Priprava in usklajevanje metodologije projektnega menedžmenta	4,25
d) Pregled in poročanje o portfelju projektov	4,24
a) Administrativna podpora (pisanje zapisnikov, usklajevanje in rezervacija prostorov, obvladovanje projektne dokumentacije)	4,19
i) Priprava in vzdrževanje orodja v podporo projektnemu menedžmentu	4,19
e) Revizije projektov	4,06
b) Podpora odnosom s strankami (zunanji izvajalci, dobavitelji)	3,93
c) Sodelovanje pri pripravi strategij in letnih planov organizacijskih enot	3,84

Legenda: Ocena pomeni povprečno oceno odgovorov anketiranih na petstopenjski lestvici od »5 — se popolnoma strinjam« do »1 — se popolnoma ne strinjam«.

Vir: Prirejeno po P. Panjan, Pomen projektne pisarne za učinkovito izvajanje poslovnih procesov podjetja, 2011, tabela 13.



Slika 1: **Želene funkcije projektne pisarne**

4 SKLEP

Uporaba zrelostnih modelov in strateško planiranje pospešita uvajanje projektnega menedžmenta in projektne pisarne v organizacijo. Organizaciji je pri tem v pomoč mnogo pripravljenih modelov, s pomočjo katerih oceni trenutno stanje ter na podlagi teh ocen, priporočil stroke in poslovnih potreb pripravi strateške načrte uvedbe ali dviga zrelosti projektnega menedžmenta in projektne pisarne v organizaciji.

Analiza OE IT izbrane organizacije je pokazala, da OE IT večinoma ne upošteva priporočil stroke glede strateškega planiranja projektnega menedžmenta niti po nobenem zrelostnem modelu ne dosega najvišje stopnje zrelosti. Po mnenju strokovnjakov takšne ugotovitve niso razlog za preplah, saj organizacija sama definira pomen projektnega menedžmenta in projektne pisarne ter ravni zrelosti, ki jih želi doseči. Vendar glede na to, da imata projektni menedžment in projektna pisarna velik vpliv na izvajanje aktivnosti OE IT, priporočamo menedžmentu OE IT, da ponovno analizira pomen projektnega menedžmenta in projektne pisarne za OE IT in v primeru, da imata za OE IT velik pomen, v večji meri izkoristi trenutni koncept projektnega menedžmenta v podporo rednemu poslovanju ter strateško pristopi k dvigu njune zrelosti.

5 LITERATURA

[1] American Society for the Advancement of Project Management. (2010). *asapm Performance Rated Organization: Standard for Assessing Organizational Project Management Performance*. Colorado Springs: American Society for the Advancement of Project Management.

[2] Fitzgerald, D. (2008). *PMOs one size does not fit all*. Connecticut: Gartner, Inc.

[3] Hill, G. M. (2004). *The Complete Project Management Office Handbook*. Boca Raton: Auerbach Publications.

[4] Hill, G. M. (2008). *The Complete Project Management Office Handbook* (2nd ed.). Boca Raton: Auerbach Publications.

[5] Hobbs, B. (2006). *Report on the Survey »The Reality on Project Management Offices«.* Univerza Quebec: Montreal.

[6] Kendall, G. I. & Rollins, S. C. (2003). *Advanced project portfolio management and the PMO: multiplying ROI at warp speed.* Conyers, GA: J. Ross.

[7] Kerzner, H. (2009). *Project management: a systems approach to planning, scheduling, and controlling* (10th ed.). Hoboken, NJ: John Wiley & Sons.

[8] Kerzner, H. (2010). *Project management best practices: achieving global excellence* (3rd ed). New York: John Wiley & Sons.

[9] Kovačič, A. & Bosilij Vukšič, V. (2005). *Management poslovnih procesov: Prenova in informatizacija poslovanja.* Ljubljana, GV Založba.

[10] Mieritz, L., Fitzgerald, D., Gomolski, B. & Light, M. (2007). *Toolkit Best Practices–Program and Portfolio Management Maturity Model*. Connecticut: Gartner, Inc.

[11] Panjan, P. (2011). *Pomen projektne pisarne za učinkovito izvajanje poslovnih procesov podjetja* (magistrsko delo). Ljubljana: Ekonomska fakulteta.

[12] Project Management Institute, Inc. (2003). *Organizational Project Management Maturity Model (OPM3): Knowledge Foundation*. Newton Square, Pensilvania: Project Management Institute.

[13] Project Management Institute, Inc. (2008). *A Guide to the Project Management Body of Knowledge: PMBOK Guide* (4th ed.). Newton Square, Pensilvania: Project Management Institute.

[14] Sowden, R. (2008). *Portfolio, Programme and Project Management Maturity Model*. London: Office of Government Commerce.

[15] Vowler, S. (2010). *Business Benefit of P3O Implementation.* Najdeno 13. novembra 2010 na spletnem naslovu http://www.best-management-practice.com.

[16] Wysocki, R. K. (2007). *Effective Project Management: Traditional, Adaptive, Extreme* (4th ed.). Indianapolis: Wiley.

▪

Primož Panjan je leta 2003 diplomiral na Fakulteti za organizacijske vede Univerze v Mariboru, leta 2011 pa je na Ekonomski fakulteti Univerze v Ljubljani dokončal podiplomski študij informacijsko-upravljalskih ved. V organizaciji, v kateri je trenutno zaposlen, vzpostavlja okolje, ki oddelku informatike in tudi drugim oddelkom v organizaciji omogoča doseganje zrelosti na področju projektnega menedžmenta. Področja dela vključujejo razvoj metodologije projektnega menedžmenta (OPPMET), orodja v podporo metodologiji, identifikacijo najboljših praks za učinkovito uporabo metodologije in orodja, pripravo in uvedbo profesionalnih izobraževanj za projektni menedžment. V preteklosti je na različnih delovnih mestih sodeloval pri organizaciji dela in pripravi internih metod dela, nenehno pa se srečuje z različnimi projekti in vidiki projektnega menedžmenta.

Študija ustreznosti implementacije sistema za nadzor kritičnih aplikacij v bančnem sistemu

[1]Simon Sirc, [2]Jože Zupančič
[1]NLB, d. d., Šmartinska cesta 130, 1000 Ljubljana
[2]Univerza v Mariboru, Fakulteta za organizacijske vede, Kidričeva 55 a, 4000 Kranj
simon.sirc@nlb.si; joze.zupancic@fov.uni-mb.si

Izvleček

V prispevku je prikazana študija ustreznosti sistema za nadzor kritičnih aplikacij v bančnem informacijskem sistemu NLB, d. d. Sistem za nadzor smo proučevali z namenom nadgradnje obstoječega nadzornega sistema, s katerim ne moremo nadzorovati delovanja kritičnih aplikacij oz. transakcijskih tokov v realnem času. Cilj novega nadzornega sistema je, da omogoča stalno spremljanje delovanja sistema in kritičnih aplikacij, alarmiranje in v določenih primerih celo avtomatizirano odpravljanje napak. Naš namen je zgraditi čim bolj avtonomen informacijski sistem, kar pa na vseh področjih ni mogoče. Preučevani nadzorni sistem z zmožnostjo sledenja transakcijskim tokovom omogoča tudi odkrivanje ozkih grl v delovanju aplikacij, zato bi z njegovo uporabo lahko optimizirali marsikateri proces, za katerega sedaj niti ne vemo, da obstaja oz. da nam povzroča težave. Predlagani pristop je bil implementiran in preizkušen na kritični aplikaciji, ki podpira plačilne transakcije v državi in skrbi za izmenjavo plačilnih transakcij med notranjimi in zunanjimi sistemi. Podana je tudi ocena implementiranega dela nadzornega sistema in predlogi za nadgradnjo oz. implementacijo preostalih komponent nadzornega sistema.

Ključne besede: informacijski sistem, nadzorni sistem, kritične aplikacije, transakcije, IBM Tivoli, strateški cilji, analiza ustreznosti.

Abstract

The Study of the Implementation of Monitoring System for Critical Applications in the Banking System

This paper presents a feasibility analysis of a system for monitoring of critical applications in the NLB bank. The monitoring system was investigated with the intention to upgrade the existing application of the monitoring system, which doesn't support real-time monitoring of critical applications and transaction flows. The proposed system has the capability to continually monitor the functioning of the entire information system and critical applications, and warn the operators; in some cases even an automated recovery from failure is possible. The capability to monitor transaction flows enables the system to reveal bottlenecks in the existing processes and identify and optimise critical or failure prone processes within critical applications. Although the goal of the study was to propose a widely autonomous system, the monitoring system still requires intervention of IS personnel. The proposed approach was implemented and evaluated on a critical application, i.e., the central application which supports payment transactions within the country and manages exchange of payment transactions between internal and external systems. An evaluation of the implemented monitoring system is presented and proposals for further upgrade and development of the system are given.

Keywords: information system, monitoring system, critical application, transaction, IBM Tivoli, strategic goal, feasibility analysis.

1 UVOD

Z razvojem novih storitev in z njimi povezanih uporabniških rešitev v NLB, d. d., se hitro povečuje tudi kompleksnost informacijskega sistema podjetja, ki ga je vse težje nadzorovati. Čeprav sta zanesljivost in razpoložljivost informacijskega sistema že več let visoki, podjetje stremi k doseganju še boljših rezultatov na tem področju.

Poslanstvo oddelka za informacijsko tehnologijo v NLB je vzpostaviti okolje, v katerem je informacijska tehnologija glavni temelj poslovanja banke in eden od gonilnih sil razvoja. Širše gledano je poslanstvo skupine NLB biti zanesljiv dolgoročni partner, na katerega se stranke lahko zanesejo. NLB hoče svojim strankam zagotavljati prvovrstne in celovite finančne storitve in rešitve, ki jih potrebujejo za doseganje svojih ciljev (NLB, 2011a). Eden od ciljev oddelka za informacijsko tehnologijo v tem letu je zmanjšati število dni z motnjami za uporabnike in s tem zagotoviti, da uporabniki v prihodnje sploh ne bodo zaznavali nepredvidenih motenj delovanja informacijskega sistema.

Glede na heterogenost informacijskega sistema in veliko število sprememb, ki se izvedejo vsako leto, to pomeni zelo velik izziv (NLB, 2011b).

Da bi dosegli omenjene cilje, je treba najprej izpostaviti, da je trenutno največji problem zagotovitev natančnega, hitrega, zanesljivega in celovitega sprotnega pregleda nad delovanjem celotnega informacijskega sistema, kakor tudi pregled nad medsebojno povezanostjo komponent, na katerih se izvajajo poslovne aplikacije oz. transakcije.

Nadzor in spremljanje transakcij z obstoječim načinom nadzora ni mogoč, zato se velikokrat spopadamo z napakami v delovanju kritičnih aplikacij, ko se te že razširijo na druge komponente informacijskega sistema. Takrat je odprava napak zahtevnejša, saj je vzrok oz. mesto nastanka težje odkriti, napake pa se kopičijo. Za nadzor informacijskega sistema trenutno uporabljamo več različnih produktov, ki niso povezani v celoto. Ker nimamo celovitega pregleda nad informacijskim sistemom na enem mestu in ker ne znamo povezovati soodvisnih podatkov, tudi ne moremo razpolagati s podatki o transakcijskih tokovih. Potrebujemo nadzorni sistem, ki bi informacije o sistemu in transakcijskih tokovih prikazoval v dejanskem času na uporabniškem vmesniku, katerega bi uporabljali vsi skrbniki.

Da bi rešili omenjeno težavo, smo v banki izvedli študijo ustreznosti nadzornega sistema IBM Tivoli, ki naj bi omogočal tako nadzor sistema, kakor tudi nadzor nad transakcijami. Ker je celoten nadzorni sistem preobsežen, se je bilo treba odločiti, kateri deli nadzornega sistema so nujno potrebni, katere bi še radi implementirali ter katerih ne potrebujemo.

Glede na visoko stopnjo zanesljivosti in razpoložljivosti bančnega informacijskega sistema bi na prvi pogled lahko sodili, da je obstoječi način nadzora povsem zadosten, saj tudi v praksi uspešno deluje že od vsega začetka. Z njim smo lahko zadovoljni in ga ocenjujemo kot zanesljivega. Spoznanja o zmožnostih naprednih tehnologij nadzora pa kažejo, da z naprednim nadzornim sistemom lahko tudi optimiziramo poslovne procese in dvignemo poslovanje na višjo raven, informacijskemu sistemu pa znižamo obratovalne stroške in stroške, povezane s pojavom in odpravo napak. To pa seveda še ne pomeni, da bi tako lahko odpravili vse napake v delovanju informacijskega sistema in poslovnih aplikacij, vsekakor pa bi bili zmožni nadzorovati transakcijske tokove in celotno delovanje informacijskega sistema z enim samim uporabniškim vmesnikom.

2 KRATKA PREDSTAVITEV INFORMACIJSKEGA POSLOVNEGA OKOLJA BANKE IN NADZORNEGA SISTEMA

Arhitektura informacijskega sistema banke je kompleksna, heterogena in večnivojska. Tvori ga skupek različnih medsebojno prepletenih komponent na različnih ravneh, ki uporabljajo različne tehnologije. Glavni del informacijskega sistema banke je velik osrednji računalnik (angl. host, mainframe) IBM Z196. Na tem sistemu ter podsistemih, kot so CICS TS (angl. Customer Information Control System Transaction Server), DB2 (angl. Database 2), WebSphere MQ (angl. WebSphere Message Queue) idr., se izvajajo programi s poslovno logiko. Predstavitvena logika, torej uporabniški vmesniki, ki v glavnem zajemajo in prikazujejo podatke, pa so ločeni od osrednjega računalnika. Nameščeni so na različnih distribuiranih okoljih, v katerih se tudi izvajajo.

Poleg vmesnih ravni, ki se navezujejo na varnost, prenos podatkov itn., sta z vidika zanesljivosti delovanja najbolj pomembni predstavitvena raven in raven obravnavanja poslovnih podatkov, saj so spremembe (in s tem posledično tudi napake) na teh dveh ravneh najbolj pogoste, poleg tega pa sta za uspešno in pravilno delovanje poslovno kritičnih aplikacij tudi najbolj pomembna. Z vidika zanesljivosti delovanja poslovno kritičnih aplikacij so najbolj izpostavljene transakcije, saj morajo nemoteno delovati ravno tisti trenutek, ko se izvajajo.

V slovenski literaturi opisa termina kritična aplikacija ne zasledimo, tudi slovar informatike (http://www.islovar.org/) ga ne pozna, čeprav se o tem zadnje čase vedno več govori in se to tako rekoč tiče skoraj vsakega podjetja z informacijskim oddelkom. Zato navedbe o kritičnih aplikacijah, ki so predvsem v bančnem poslu nekaj vsakdanjega, povzemamo iz tuje literature.

Tradicionalno so bile poslovno kritične aplikacije opredeljene kot aplikacije, ki so za poslovne procese bistvenega pomena. Podatkovno usmerjeni aplikaciji, kot sta bančni transakcijski sistem ali letalski rezervacijski sistem, sta že od nekdaj ključni za ta dva poslovno kritična procesa. Njuno nedelovanje se običajno pokaže kot izguba dohodkov ali zmanjšanje produktivnosti zaposlenih. Zadnje čase uporabljajo vse več aplikacij, ki veljajo za poslovno kritične. Ta realnost je v velikem številu podjetij spremenila vlogo in funkcijo informacijske tehnologije. V splošnem kot poslovno kritične aplikacije še vedno

lahko označimo tiste, katerih sistemske napake pri uporabniških rešitvah vodijo v izgubo prihodkov, nezadovoljstvo strank in/ali upad produktivnosti. Vendar pa je meja med aplikacijami, ki so kritične za poslovanje, in drugimi aplikacijami vedno bolj zamegljena. Drugačne storitve, pa četudi znotraj enega podjetja, zahtevajo različna merila za opredelitev, kaj je poslovno kritično (Hicks, 2004).

Poslovanje banke temelji na plačilnem prometu, plačilni promet pa na finančnih transakcijah. Transakcija je postopek, ki ga sproži posamezna zahteva in jo izda operater oz. uporabnik. Postopek, izveden glede na podano zahtevo, sproži akcije enega ali več medsebojno povezanih aplikacijskih programov, ki izpolnijo podano zahtevo. Poti transakcij skozi programe in sisteme poznamo le opisno. Nekateri skrbniki aplikacij imajo v dokumentaciji celo izrisane transakcijske tokove skozi sisteme na principu procesnih slik. Kako transakcije določen trenutek dejansko potekajo, kje so ozka grla, kakšni so odzivni časi med posameznimi komponentami informacijskega sistema itn., pa ne znamo spremljati oz. nadzirati. Možnosti boljših načinov nadzora upravljavci informacijskih sistemov iščejo že od vsega začetka informatizacije poslovanja. Skrbniki posameznih področij informacijskega sistema in poslovnih aplikacij so pogosto sami izdelali svoje nadzorne rešitve ali pa so implementirali v okolje kupljene produkte različnih proizvajalcev.

3 PREGLED OBSTOJEČE LITERATURE IN DOKUMENTACIJE

Pregled raziskovalne literature je pokazal, da je se objave v zvezi z nadzorom (kritičnih) aplikacij večinoma nanašajo na lastne rešitve in specifične vidike, npr. na preprečevanje in odkrivanje vdorov v sistem, pa tudi na razvoj algoritmov, postopkov in splošnih rešitev pri nadzorovanju informacijskih sistemov. Abdul-Malek (2010) je v svoji doktorski disertaciji predlagal model in izdelal od računalniškega okolja neodvisno aplikacijo, ki poleg nadzorovanja tekočih in končanih poslov omogoča tudi nadzor napak in alarmiranje operaterjev. Agarwala idr. (2010) so predstavili idejo in praktično rešitev za vmesno programje (angl. middleware), namenjeno nadzorovanju računalniške konfiguracije, ki temelji na najboljših industrijskih standardih in praksah. Izboljšanje učinkovitosti nadzornega sistema na podlagi analize karakteristik aplikacij je poglavitni cilj modela, ki je opisan v Wang idr. (2008). Paxton idr. (2011) predlagajo model za zaščito in nadzorovanje napadov na računalniški sistem »botnet«,[1] Veyard (2003) opisuje aplikacijo za nadzor informacijskega sistema za odkrivanje transakcij, ki so sumljive z vidika pranja denarja. Sengupta idr. (2008) predlagajo od računalniškega okolja neodvisen in »neinvaziven« pristop, ki temelji na analizi vzorcev transakcij izhajajoč iz dnevnikov transakcij (angl. log files). V referatu Yang idr. (2010) avtorji predstavljajo pregled, kako v nekaterih vodilnih azijskih bankah pristopajo k nadzorovanju tveganj, povezanih z informacijsko tehnologijo. Haberkorn in Trivedi (2007) opisujeta metodo za nadzor in prikaz razpoložljivosti računalniškega sistema v realnem času.

Ker nismo uspeli najti ustreznih virov v znanstveni literaturi, ki bi obravnavali praktično implementacijo nadzornega sistema, smo se pri našem delu opirali predvsem na nekatere strokovne članke in na proizvajalčevo dokumentacijo.

Ker se bančno poslovanje neprestano širi, je treba uvesti prožen nadzorni sistem, ki se bo z lahkoto prilagajal razširjenemu ali spremenjenemu poslovanju. Da bi bili stroški čim manjši, mora biti način prilagajanja nadzornega sistema enostaven in ne sme zahtevati stalne pomoči zunanjih svetovalcev. Praviloma bi komercialno dostopen transakcijsko nadzorni sistem moral biti pripravljen za integracijo v bančno okolje, vendar v večini primerov ni tako. Zato lahko pričakujemo, da bosta implementacija in natančno nastavljanje nadzornega sistema tekla uspešno le, kadar je vzpostavljeno tesno sodelovanje med ponudnikom nadzornega sistema in informacijskim oddelkom. Nujna je pogosta fizična navzočnost ponudnika med implementacijo in je priporočljiva tudi kasneje – pri dopolnitvah in nadgradnjah. Zato je izbira ponudnika ključnega pomena. Zaposleni v informacijskem oddelku morajo biti s temi dejstvi dobro seznanjeni in morajo biti pripravljeni sodelovati s ponudnikom (Veyder, 2003).

Če zaposleni niso pripravljeni sodelovati, lahko pričakujemo, da bo njihova absorpcijska sposobnost zelo nizka. Kot ugotavlja Mulej (2003:1), absorpcijska sposobnost pomeni sposobnost in voljo sprejeti in ustvarjalno ter koristno uporabiti znanje, vednost in

[1] Po slovarju informatike (http://www.islovar.org/) pomeni »botnet« večje število računalnikov, nad katerimi napadalec brez vedenja skrbnikov na daljavo pridobi nadzor z namenom izvajanja zlonamernih dejanj; sin. omrežje robotskih računalnikov.

vrednote, ki se ne razvijajo neposredno v praksi, bi pa naj jih tam uveljavili.

Pri izbiri nadzornega sistema je bila zato pomembno merilo tudi združljivost nadzorne tehnologije z obstoječo informacijsko tehnologijo. Ker osrednji del informacijskega sistema banke predstavlja IBM-ov računalnik Z196, je na odločitev o izboru ponudnika najbolj vplivala preprosta združitev nadzorne tehnologije z obstoječo informacijsko tehnologijo. Banka se je odločila za nadzorni sistem IBM Tivoli Monitoring tudi zaradi njegovih karakteristik, saj omogoča podroben nadzor osrednjega računalnika in njegovih sistemskih ter podsistemskih komponent. S tem je mogoče pokriti nadzor skoraj celotnega dela poslovne logike, ki se izvaja na osrednjem računalniškem delu, omogoča pa tudi podroben nadzor logike predstavitvenega dela (uporabniški vmesniki), ki se izvaja na različnih distribuiranih okoljih.

Nadzorni sistem IBM Tivoli Monitoring je kompleksen sistem, sestavljen iz več komponent – tako strojnih kot tudi programskih –, ki omogoča nadzor strojnih in aplikativnih programskih delov (transakcij) poslovnoinformacijskega sistema. Programska oprema Tivoli deluje kot možgani v ozadju osrednjega računalnika. Omogoča performančni in aplikativni nadzor, sistemsko in aplikativno avtomatiko, nadzor omrežja, podatkovni, finančni in varnostni nadzor, omogoča izdelovati finančna poročila in poročila o izvajanju aplikacij, procesov in še več drugih funkcij (IBM Plans New Tools to Support Tivoli System z Management Software, 2007).

V študijah primerov, ki so dosegljivi na IBM-ovih spletnih straneh, avtorji večinoma pišejo o nadzornem sistemu IBM Tivoli za sistemske komponente, bolj malo pa o nadzorni tehnologiji transakcij; italijansko borzno podjetje Consip SpA npr. uporablja Tivoli Business Service Manager za boljše razumevanje odvisnosti in povezave med infrastrukturnimi deli ter poslovnimi storitvami, kar jim omogoča boljši vpogled v dejavnosti in boljše razumevanje vpliva, ki ga problem lahko povzroči uporabnikom (IBM, 2011a). V nemškem podjetju BG-Phoenix GmbH, ki se ukvarja s prodajo strojne in programske opreme socialnovarstvenim ustanovam in strokovnim združenjem, uporabljajo Tivoli Monitoring za zagotavljanje kakovosti njihovih storitev, saj spremljajo celotno informacijsko infrastrukturo vključno z distribuiranimi strežniki zunaj njihove osrednje računalniške infrastrukture (IBM, 2011b).

Sistemski nadzor z uporabo produktov Tivoli Monitoring je torej že dokaj razširjen, medtem ko sam nadzor transakcij ni. Sledenje transakcijam je za banko najbolj zanimivo področje, predvsem pa je povsem novo. Nadzor nad samim sistemom sicer že obvladujemo z drugačnimi prijemi in produkti. Tudi prehod oz. implementacija proizvodov IBM Tivoli za sistemski nadzor ne bi bila problematična, zahtevno pa je uvesti tehnologije nadzora transakcij. Po besedah enega izmed največjih specialistov za to področje in soavtorja članka Hu idr. (2008), Richarda Macklerja, s katerim smo imeli priložnost sodelovati, smo v banki na področju implementacije v tako kompleksen, predvsem pa realen poslovni sistem v svetovnem merilu naredili velik korak v tej smeri.

IBM je že leta 2004 naznanil novo verzijo programa Tivoli Monitoring for Transaction Performance, ki naj bi zelo povečala možnosti sledenja transakcij z različnimi aplikacijami. Ta zmožnost je bila mišljena predvsem za velika okolja, v katerih nadzorujejo več sto različnih transakcij (Musich, 2004).

Zadnje čase se poleg nadzora veliko govori tudi o avtonomnih računalniških sistemih. Avtonomno računalništvo, kot pove že ime, je metafora, ki temelji na biologiji. Avtonomni živčni sistem v telesu je osrednjega pomena za veliko nezavednih dejavnosti, ki nam omogočajo, da nadaljujemo z višjo stopnjo aktivnosti v našem vsakdanjem življenju. Tipični primeri, ki izstopajo, so bitje srca, utrip, dihanje, refleksni odziv po dotiku ostrega ali vročega predmeta itn. Namen uporabe te metafore je izraziti vizijo, da bi nekaj podobnega morali doseči tudi na področju računalništva, tj. ustvariti samodejno upravljanje znatnih količin računalniških funkcij in s tem razbremeniti uporabnike na nižji stopnji upravljanja, da se bodo lahko posvečali skrbi za upravljanje na višji ravni, preizkušanju novih stvari ali zabavi (Sterritt, 2005; Huebscher in McCann, 2008).

Za avtonomno in uporabno delovanje računalnikov stranke potrebujejo zmožnost merjenja, kako se aplikacije obnašajo na sistemu in kako se transakcije izvajajo prek informacijske infrastrukture. Tivoli Monitoring za spremljanje transakcijskih zmogljivosti je korak v tej smeri, saj so za avtomatizacijo popravkov v IBM-u načrtovali sisteme, ki znajo sami skrbeti zase. Tudi programska oprema nadzornega sistema mora zato najprej »razumeti«, kako aplikacije komunicirajo z infrastrukturnimi komponentami na ravni transakcij (Dubie, 2004).

Po trditvah proizvajalca (IBM, 2011c) nadzorni sistem za nadzor transakcij omogoča visoko zanesljiv nadzor transakcij za spletne in organizacijsko-informacijske infrastrukture ter pomaga uporabnikom, da se izognejo kritičnim performančnim problemom. Tako omogoča, da operacije za stranke in končne uporabnike tečejo gladko. Ilog JViews[2] uporabljajo stranke Tivoli, kot so transakcijski ponudniki, da lahko od začetka do konca spremljajo tok in učinek individualnih ali skupnih vplivov transakcij, ugotavljajo transakcijske odzivne čase in vire zakasnitev. Ko nadzorni sistem locira problem, spoznavni grafični model Ilog JView pomaga uporabniku, da s pomočjo vizualizacije locira komponento, ki povzroča zaostanke in s tem pripomore k hitri odpravi problema. Ilog JViews interaktivni prikazi z naprednimi podatkovnimi tehnikami, kot je avtomatsko razvrščeni tokovni diagram, omogočajo uporabnikom lažje razumevanje kompleksnega toka podatkov, ki se pretaka skozi njihove procese.

Ker je IBM Tivoli Monitoring za nadzor transakcij dokaj nov proizvod, ki se v takšnem obsegu, kot ga želimo uporabiti v banki, skorajda ni uporabljal, se je postavilo vprašanje, ali je nadzorni sistem sploh dovolj izpopolnjen in ali sploh stabilno deluje. Zanimalo nas je, ali je glede na heterogeno informacijsko okolje banke res primeren oz. zmožen kakovostno in zanesljivo opravljati funkcijo nadzora transakcijskih tokov poslovno kritičnih aplikacij skozi kompleksno informacijsko omrežje in jih tudi izrisati.

Glede na predstavljena dejstva iz literature in zaradi preproste združljivosti nadzorne tehnologije z obstoječo informacijsko infrastrukturo smo se odločili, da nadzorni sistem IBM Tivoli Monitoring implementiramo in preizkusimo, ali je primeren za NLB. Opravili smo študijo, v kateri so sodelovali zunanji strokovnjaki in naši strokovnjaki za različna področja znotraj banke, kakor tudi skrbniki za posamezne sistemskoaplikativne dele poslovno kritičnih aplikacij. Študija je bila opravljena z namenom, da bi skupaj postavili oceno ustreznosti nadzornega sistema za NLB, d. d.

4 POSTAVITEV KRITERIJEV IN CILJ ŠTUDIJE

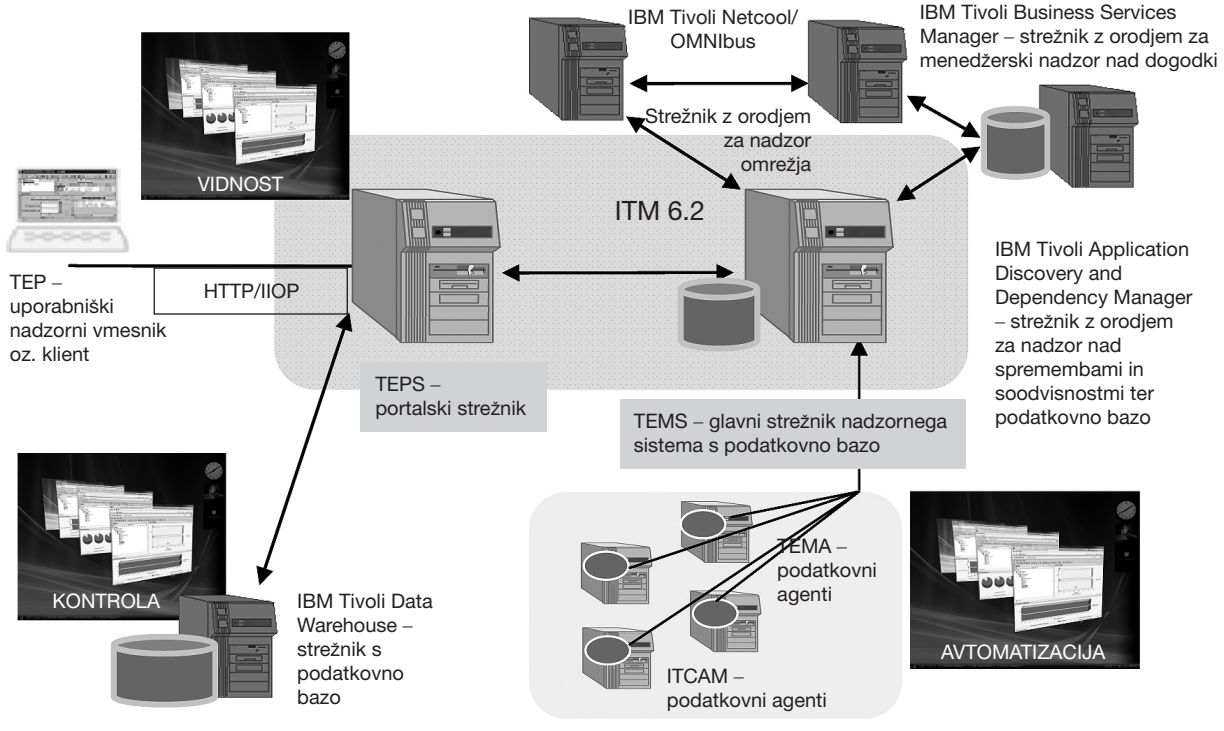
Cilj študije je bilo opraviti analizo ustreznosti sistema za nadzor informacijskega sistema banke, na katerem se izvajajo kritične aplikacije. Prav tako je bil cilj preučiti tudi nadzor kritičnih aplikacij in spremljanje toka transakcij v realnem času. Upoštevali smo, da sam informacijski sistem znamo nadzorovati že dokaj natančno, ne znamo pa nadzorovati toka transakcij. Za oceno primernosti oz. ustreznosti nadzornega sistema smo na podlagi zmožnosti nadzornega sistema, opisanih v proizvajalčevi spletni literaturi (http://www-01.ibm.com/software/tivoli/products/monitor/), določili glavne kriterije, katere mora izpolnjevati nadzorni sistem. Kriterije smo postavili v obliki vprašanj, s pomočjo katerih smo kakovostno ocenili ustreznost nadzornega sistema.

- Ali nadzorni sistem omogoča nadzor celotnega informacijskega sistema in poslovno kritičnih aplikacij na enem uporabniškem vmesniku?
- Ali omogoča sledenje in vizualizacijo celotnega toka transakcij ne glede na heterogenost našega informacijskega sistema?
- Ali nadzorni sistem omogoča spremljanje končnih in vmesnih odzivnih časov transakcij in s tem tudi odkrivanje ozkih grl?
- Ali je nadzorni sistem na podlagi postavljeni pravil zmožen zaznavati, alarmirati, locirati, diagnosticirati in avtomatsko odpravljati napake v doglednem času, ki je v večini primerov krajši od 5 minut (toliko časa navadno traja, da problem zaznajo uporabniki)?
- Ali je poraba sistemskih resursov osrednjega računalnika za izvajanje nadzora manjša od 15 odstotkov celotne porabe resursov?
- Ali so za upravljanje (namestitev, uporaba, nadgradnja) nadzornega sistema dovolj trije skrbniki?
- Ali nadzorni sistem v primerjavi z obstoječim načinom nadzora omogoča lažje obvladovanje informacijskega sistema banke?

Da smo lahko odgovorili na zastavljena vprašanja oz. da bi nadzorni sistem omogočal funkcionalnosti, katere smo preizkušali, smo morali zagotoviti, da je bila na vsaki komponenti informacijskega sistema, ki jo nadzorujemo, nameščena ustrezna komponenta nadzornega sistema. Bolj podrobna arhitekturna slika sestavnih delov nadzornega sistema po komponentah informacijskega sistema, na katerih temelji naš nadzorni sistem, bo predstavljena v nadaljevanju. Na sliki 1 pa je razvidna tipična

[2] Ilog JViews je IBM-ova blagovna znamka za vizualizacijo. Nanaša se na celovito zbirko programskih orodij in knjižnic, ki so namenjeni razvijalcem uporabniških vmesnikov in omogočajo izdelavo interaktivnih grafičnih prikazov. Uporabiti jih je mogoče v različnih razvojnih okoljih in omogočajo izdelavo kompleksnih grafičnih vmesnikov za zahtevna poslovna okolja (http://www.ibm.com/developerworks/offers/lp/demos/summary/ilog-jviews-maps.html).

oz. osnovna zgradba nadzornega sistema, kot so si jo zamislili IBM-ovi strokovnjaki, ki so zasnovali nadzorni sistem. Na sliki je še nekaj gradnikov oz. komponent, katerih funkcionalnosti nismo uspeli preizkusiti, niti jih nismo nameščali, jih pa načrtujemo za prihodnost. Osredinili smo se na osrednji del, ki omogoča nadzor sistema in sledenje transakcijam, in tako izpustili orodja za nadzor omrežja (IBM Tivoli Netcool/OMNIbus), za nadzor nad spremembam in soodvisnostmi (Change and Configuration Management Database in IBM Tivoli Application Discovery and Dependency Manager) in orodju za menedžerski nadzor nad dogodki (IBM Tivoli Business Services Manager).



Slika 1: **Arhitekturna slika – nadzorni sistem IBM Tivoli Monitoring** *(Vir: Implementacija IBM Tivoli Monitoring v NLB)*

Ker je ves nadzorni sistem IBM Tivoli izredno kompleksen, smo sprva za potrebe analize ustreznosti izbrali komponente, ki bodo nadzorovale najpomembnejše dele bančnega informacijskega sistema. Sproti smo dodajali posamezne dodatne dele in tako postavili nadzorni sistem, ki naj bi glede na kriterije odgovoril na naša vprašanja oz. zadostil našim potrebam. Predstavljeni nadzorni sistem sicer temelji na prikazu nadzora ene same poslovno kritične aplikacije in njenih sistemskih komponent, vendar zajema ravni poslovne logike, ki se odvija na osrednjem računalniku, kakor tudi ravni predstavitvene logike iz distribuiranega okolja.

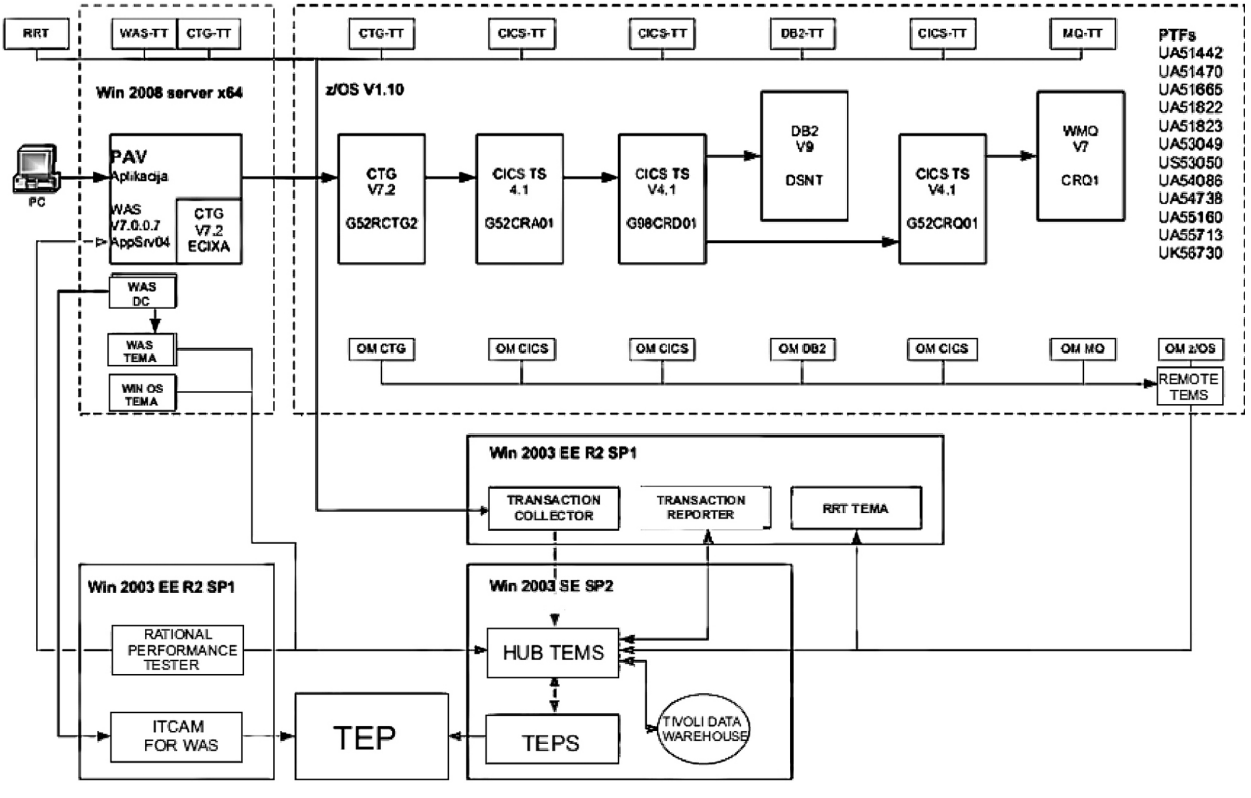
5 PREDSTAVITEV NADZORNEGA SISTEMA

Ker večina aplikacij v plačilnem prometu deluje na podobnem principu (več o tem v nadaljevanju), smo uporabili večino najpomembnejših delov nadzornega sistema, ki bodo podlaga nadaljnjemu razvoju oz. implementaciji nadzornega sistema v informacijskem okolju banke. Nadzorni sistem smo preizkusili na aplikaciji PAV (ime PAV ima po projektu Prenova aplikacije in vmesnika). PAV je osrednja aplikacija za podporo plačilnemu prometu v domovini in skrbi za izmenjavo plačilnih transakcij med internimi in eksternimi sistemi. Večnivojska arhitektura sistemskega dela aplikacije, prikazana na sliki 2, kaže vpletenost te aplikacije v heterogeno informacijsko okolje. Uporabniški vmesnik s predstavitveno logiko

aplikacije PAV oz. klient je na WAS-u (angl. Websphere Application Server), ki je nameščen na strežniku windows. Klient je napisan v programskem jeziku java. Samo izvajanje v okolju windows omogoča javin navidezni stroj, s katerim razpolaga WAS. WAS je preko CICS TG (angl. CICS Transaction Gateway) povezan z aplikativnim CICS TS, ki je nato naprej povezan z drugimi CICS TS, s podatkovno bazo in sporočilnim sistemom WebSphere MQ, ki se nahajajo na osrednjem računalniku z operacijskim sistemom Z/OS (angl. Z Series Operating System). CICS TG je nameščen na USS (angl. Unix System Services), ki je integriran v Z/OS. Na osrednjem računalniškem delu se izvaja poslovna logika. Programi s poslovno logiko so napisani v programskem jeziku cobol.

Za popoln nadzor aplikacije PAV je treba na vsaki sistemski komponenti namestiti po dve komponenti nadzornega sistema: eno za spremljanje sistemskih komponent, drugo za spremljanje transakcij. Slika 2 prikazuje arhitekturo sistemskih in nadzornih komponent, potrebnih za izvajanje in nadzor aplikacije PAV. Komponente za nadzor sistemskih komponent, kot so rešitve Omegamon XE, pokrivajo samo osrednji računalniški del in vsebujejo tudi orodja za poglobljene analize. Posamezni Omegamon s svojimi agenti zbrane podatke pošilja prek oddaljenega TEMS-a (angl. Tivoli Enterprise Management Server) na glavni TEMS, od tu pa na TEPS (angl. Tivoli Enterprise Portal Server), kot je to razvidno s slike 2. TEMS je glavni strežnik nadzornega sistema, njegova naloga je zbiranje, filtriranje, koreliranje, analiziranje itn, TEPS pa je strežnik, namenjen za prenos podatkov do TEP-a (angl. Tivoli Enterprise Portal) in za povezovanje s podatkovnim skladiščem (angl. Data Warehouse). TEP je skupen uporabniški vmesnik za nadzor nad celotnim informacijskim sistemom in kritičnimi aplikacijami.

Z orodji Omegamon XE (na sliki 2 so označeni s kratico OM) pokrivamo osrednji računalniški sistemski del, ki je potreben za delovanje aplikacije PAV. Za spremljanje transakcij na osrednjem računalniškem delu potrebujemo še komponente Transaction tracking, to so komponente za sledenje transakcij. Enako kot za sistemski del je tudi za transakcijski del treba namestiti posamezne dele nadzornih komponent oz. podatkovne zbiralnike na vsako sistemsko komponento. Postaviti je treba še strežnike (v našem



Slika 2: **Arhitektura aplikacije PAV, nadzornega sistema za osrednji računalniški in distribuirani del ter orodja za spremljanje transakcij** (Vir: Implementacija IBM Tivoli Monitoring v NLB)

primeru so to strežniki windows), na katerih so nameščene druge komponente, potrebne za zbiranje in povezovanje podatkov, katerih skupek imenujemo Agregation Agent. Agregation Agent je sestavljen iz sklopa Transaction Collector in agentov, imenovanih Web Response Time Agents. Na sliki 2 je ta skupek prikazan kot Transaction Collector. Komponenta za prikazovanje podatkov v obliki grafov in topologij je na sliki prikazana kot Transaction Reporter.

Vsi podatki se prek TEMS-a stekajo v TEPS, pregledujemo pa jih na TEP-u, ki je dejansko glavni nadzorni uporabniški vmesnik. Z TEMS-i, TEPS-om, Omegamoni, komponentami Transaction Tracking, agenti Agregation Agents in transaction reporterjem smo pokrili nadzor osrednjega računalniškega dela informacijskega sistema, ne pa distribuiranega, v katerem se nahaja uporabniški klient za delo z aplikacijo PAV. Za nadzor sistema distribuiranega dela moramo pokrivati strežniško okolje windows (operacijski sistem – na sliki 2 prikazano kot WinOS TEMA), v katerem je aplikativni strežnik (WAS), na katerem se izvaja klient aplikacije PAV, katerega je tudi treba nadzorovati (s pomočjo nadzorne komponente, ki je na sliki prikazana kot WAS TEMA). Uporabili smo še WAS Data Collector, ki pošilja podatke svojemu strežniku (na sliki ITCAM for WAS Managing Server) in omogoča poglobljene analize in grafične prikaze uporabe resursov, s katerimi razpolagata WAS in aplikacija, ki je nameščena na WAS-u (npr. povezava do baze podatkov, povezava do CICS TS prek CICS TG s pomočjo klicev ECI[3]). Za podatke o transakciji in za končni izris distribuiranega dela transakcijske topologije skrbijo komponente ITCAM, ki so na sliki 2 prikazane v kvadratkih pod zgornjim robom slike (WAS-TT, CTG-TT, CICS-TT, DB2-TT in MQ-TT). Te komponente Transaction Tracking pa zbrane podatke pošiljajo neposredno Transaction Collectorju.

Ves nadzorni sistem za aplikacijo PAV, tj. distribuirani in osrednji računalniški sistemski del, je prikazan na sliki 2. Na sliki je prikazana tudi vpletenost testerja Rational Performance (označen z RRT), ki je popolnoma samostojno orodje za performančno testiranje aplikacij na podlagi posnetkov akcij. Tako lahko posnetek uporabnikovega dela na klientu prenesemo v AMC (angl. Application Management Console) in z njegovo pomočjo simuliramo delo uporabnikov na sistemu, tudi ko noben uporabnik ni aktiven (na sliki 2 je simulirani uporabnik razviden kot RRT). S tem pridobimo nadzor nad delovanjem sistema, tudi ko ta miruje in nihče ne uporablja njegovih virov oz. razpoložljivosti. To je tudi eden izmed načinov, kako nadzorovati informacijski sistem, ko na njem ni aktivnosti.

S pomočjo nameščenih komponent nadzornega sistema na vseh komponentah informacijskega sistema pridobimo polno funkcionalnost nadzornega sistema, vključno z orodji za poglobljeno analizo. Ta orodja nam omogočajo hitre detajlne vpoglede v prav vsak del sistema.

6 PRIKAZ UPORABE IN TESTIRANJE V PRAKSI

Pri analizi ustreznosti nadzornega sistema smo testirali uporabnost z vidika nadzora sistemskih komponent nadzornega sistema, kakor tudi nadzor kritičnih aplikacij oz. transakcij na primeru aplikacije PAV. Za nadzor sistema uporabljamo grafični vmesnik TEP (slika 3), pri čemer lahko uporabimo različne tipe pogledov. Najbolj osnovni je pogled Query-based, ki v tabeli in grafih prikazuje posamezne atribute in njihove vrednosti. Poglede lahko potem, ko iščemo oz. najdemo vzrok problema, prilagodimo zahtevam, npr. atribut, ki nas zanima, prikažemo v obliki grafa.

Nadaljnji tip pogledov so pregledi dogodkov. V teh pogledih sledimo dogodkom, ki nas zanimajo. Ti dogodki so lahko splošni dogodki, ki se dogajajo na sistemu in se zapisujejo v sistemske dnevnike (»loge«), lahko pa se osredinimo na natančno določene dogodke in prednastavimo situacije. Izberemo atribute sistemskih komponent, na katerih pogosto prihaja do odstopanj, in jim določimo zgornje in spodnje meje odstopanj. Na podlagi teh meja oz. stopenj doseganja dogodka (alarmiranje) obveščamo skrbnike.

Alarmiranje je že eden izmed prispevkov nadzornega sistema. Poleg alarmiranja v določenih situacijah je velik doprinos tudi samodejni zagon procesov (preventivni ukrep), ki se izvede kot odziv na prednastavljeno pravilo. Pravila sproti dopolnjujemo in sčasoma jih lahko postavimo toliko, da sistem skorajda skrbi sam zase. Seveda obstajajo situacije, katerih odprave ne moremo avtomatizirati. Preventivne ukrepe določimo na podlagi preteklih situacij, ki jih poznamo, jih predvidimo ali o katerih imamo podatke v podatkovnem skladišču.

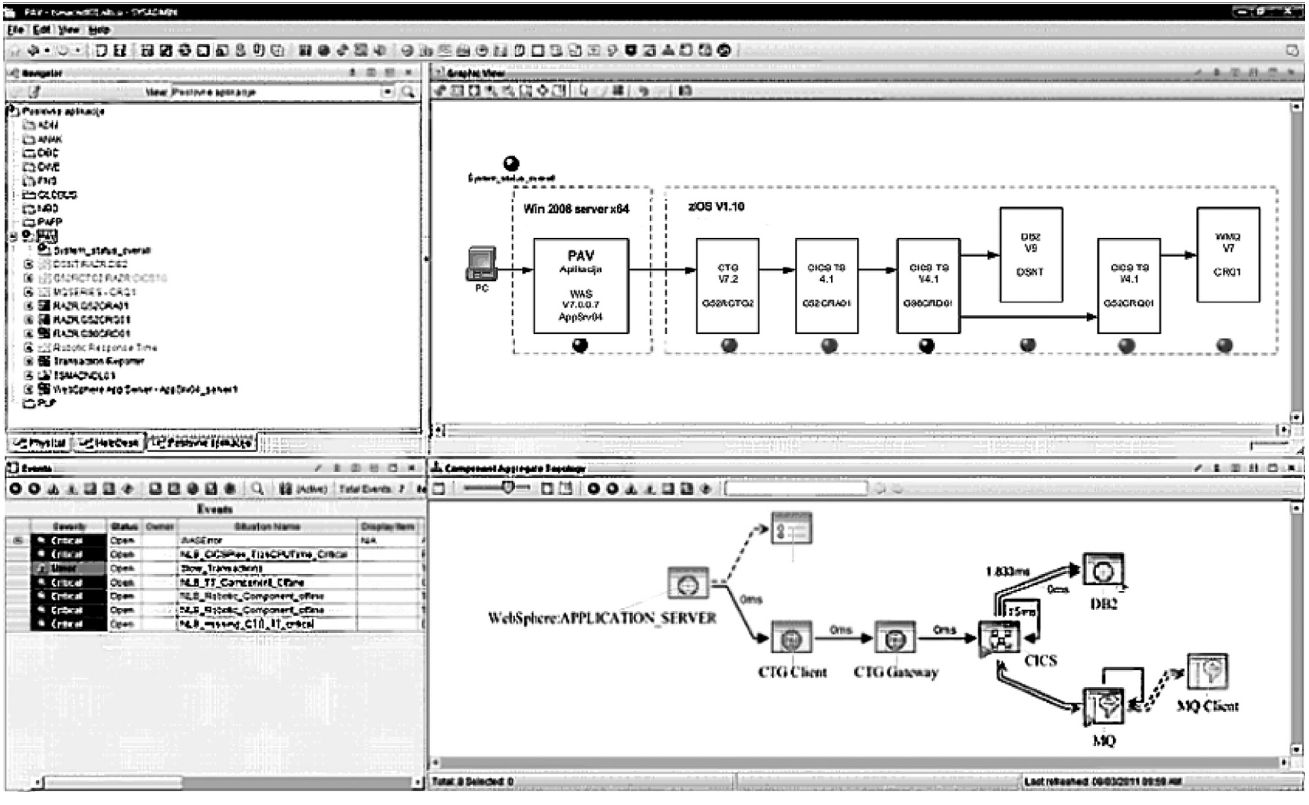
Velik prispevek nadzornega sistema IBM Tivoli je pregled ne le nad celotnim informacijskim sistemom, temveč tudi nad poslovnimi aplikacijami v realnem

[3] ECI (angl. External Call Interface) so klici programov CICS TS iz distribuiranih okolij ali iz paketnih programov osrednjega računalniškega okolja.

času, kar pri obstoječem načinu nadzora ni bilo mogoče. V veliko pomoč pri odpravi napak je tudi samodejno povezovanje in prikazovanje podatkovnih tokov, za katere sploh ne vemo, da obstajajo, ali pa ne vemo, kako potekajo. Na podlagi povezovanja podatkov lahko napako odkrijemo bistveno hitreje. Če bi implementirali še nadzorna orodja za dogodke (Event Management System), kot je Omnibus, bi pridobili še pri t. i. analizi vzroka (Root Cause analysis), ki lahko drastično zmanjša poprečni čas do odprave napake (MTTR – Mean Time To Repair), saj na podlagi zbranih podatkov zna ugotoviti vzrok napake oz. primarno napako, ki je povzročila sekundarno oz. vse ostale napake.

Na sliki 3 v spodnjem desnem okencu je grafični prikaz, na katerem je razviden dejanski transakcijski tok nad njim narisane sheme (skrbniška procesna slika za lažjo predstavnost), na kateri so ob posamezni sistemski komponenti tudi alarmi. Alarmi so v obliki krogcev in prikazujejo, da je napaka na dveh komponentah (na distribuirani WAS, na kateri je nameščena aplikacija PAV, in na osrednji računalniški CICS TS – krogca sta dejansko rdeče barve, na črno-beli sliki pa sta razvidna kot temnejše sive barve, medtem ko so ostali zeleni oz. na sliki svetlo sivi). Napaki sta kritični, sistemski komponenti nista aktivni. Krogci oz. lučke predstavljajo alarme v obliki semaforjev. Kritičnost posamezne napake pa označujejo barve: zelena označuje normalno stanje, modra sporočilo, rumena in oranžna opozorilo, rdeča in črna kritično napako (slika je črno-bela, na sliki so zajete samo zelene – svetlo sive – in rdeče – temno sive – lučke, op. avt.). Alarmi so glede na posamezno komponento tudi opisani v spodnjem levem okencu. V spodnjem desnem okencu pa je razviden realen transakcijski tok v dejanskem času. Med posameznimi komponentami so prikazani tudi odzivni časi (v milisekundah). V tem okencu lahko vidimo, da problematične komponente niso aktivne in so bledе oz. svetlo sive barve.

S klikom na posamezni alarm oz. na povezavo preidemo globlje v prikaz problema, torej na natančno določeno komponento ali sistem in razpolagamo z bolj detajlnimi podatki, ki jih lahko prikažemo tudi v grafih oz. tabelah. Podrobnosti delovanja posameznih sistemskih komponent aplikacije si lahko ogledamo kadar koli.



Slika 3: **Primer nadzora transakcijskega toka** (Vir: Implementacija IBM Tivoli Monitoring v NLB)

7 REZULTATI OZ. UGOTOVITVE

Po uspešni implementaciji nadzornega sistema do stopnje, ki že zagotavlja dejansko uporabno vrednost, kot jo je obljubljal ponudnik nadzornega sistema, smo prišli do spoznanj, da učinki uporabe v primerjavi z obstoječim načinom nadzora pričajo o velikem preskoku k lažjemu zagotavljanju nemotenega delovanja informacijskega sistema banke. Če se sklicujemo na postavljene kriterije, lahko podajamo oceno primernosti kot odgovore na zastavljena vprašanja.

- Nadzorni sistem nam omogoča pregled nad delovanjem celotnega informacijskega sistema banke in poslovno kritičnih aplikacij na enem uporabniškem vmesniku. S tem je poenoten način nadzora, saj vsi skrbniki uporabljajo isti uporabniški vmesnik (TEP), poglede pa si priredijo po svojih potrebah.
- Ne glede na heterogenost informacijskega sistema nadzorni sistem omogoča sledenje transakcijam od začetka do konca in njihovo vizualizacijo.
- S pomočjo vizualizacije in prikaza odzivnih časov je lažje odkrivati ozka grla in locirati mesta napak. Ko je napaka locirana, jo lahko odpravimo – problem lahko odpravimo, preden se razširi še na druge komponente informacijskega sistema. Širjenje problema na več komponent informacijskega sistema po navadi pomeni najdaljše prekinitve v delovanju bančnega informacijskega sistema, saj je težko odkriti vzrok problema in ga ustaviti. Ko poznamo vzrok za nastanek oz. širjenje problemskega stanja, lahko akcijo reševanja problema tudi avtomatiziramo.
- Na podlagi postavljenih pravil je mogoče spremljati določene dogodke in zaznati odstopanja ter alarmirati skrbnike oz. izvajati avtomatske akcije odprave problema. Za večino sistemskih napak imamo na razpolago tudi diagnostiko napake in predlagano rešitev, ki jo izvedemo z nekaj kliki z miško. Sam čas zaznavanja napak je odvisen od nastavitev časa osveževanja podatkov, katere pridobivamo iz posameznih komponent prek podatkovnih zbiralnikov.
- Ravno od časa osveževanja podatkov in od števila atributov, katerih podatke zbiramo oz. osvežujemo, je odvisna tudi poraba resursov osrednjega računalnika, na katerem so nameščene komponente nadzornega sistema. Pri uporabi nadzornega sistema smo večinoma uporabljali osnovne nastavitve, pri katerih smo zbirali podatke o vseh atributih posameznih komponent, čas osveževanja podatkov pa je bil nastavljen na 5 do 15 minut. Povprečno se je poraba resursov osrednjega računalnika za potrebe nadzora gibala okoli 15 odstotkov, ob večji obremenitvi osrednjega računalnika oz. ob nastavitvi hitrejšega osveževanja podatkov pa ta naraste tudi do 20 odstotkov in več. Vsekakor bo treba opraviti več testov v predprodukcijskem okolju, v katerem je število transakcij oz. količina podatkov in obremenitev osrednjega računalnika večja. Porabo resursov osrednjega računalnika za potrebe nadzora bo nujno treba zmanjšati. Omejiti bo treba število nadzorovanih podatkov na tiste, ki indicirajo kritičnost. Tudi čas osveževanja podatkov bo treba nastaviti glede na zahteve nadzora posamezne komponente informacijskega sistema. Nekatere komponente potrebujejo bolj pogost nadzor (npr. CICS TS), druge manj (npr. Websphere Q-ji), torej bomo nekatere podatke osveževali na pet minut ali manj, druge pa na petnajst minut. Obstaja še rešitev, da bi oddaljeni TEMS premaknili iz osrednjega računalnika na distribuirano strežniško okolje.
- Prvi vtisi pri upravljanju (namestitvi, uporabi in nadgradnji) nadzornega sistema niso bili najboljši. Orodje je izredno obsežno. Soočali smo se s težavami pri nameščanju komponent nadzornega sistema zaradi nezdružljivosti z različnimi verzijami komponent informacijskega sistema. Sčasoma so zadeve postale bolj razumljive in lažje obvladljive. Vsekakor nam je primankovalo znanja oz. izkušenj. Brez strokovnjakov IBM bi bila zadeva skorajda neizvedljiva. O tem pričajo tudi številni PTF-ji (angl. Program Temporary Fix), nameščeni na različne komponente informacijskega sistema (gl. sliko 2 za seznam). Začasne rešitve in nasvete so strokovnjaki IBM iskali od svojih kolegov po vsem svetu. Ocenjujemo, da bo za upravljanje nadzornega sistema sprva potrebna večja skupina ljudi, pa tudi stalna navzočnost dobavitelja. Sčasoma se število skrbnikov lahko zmanjša na celo manj kot tri osebe. Za nadzor sistema in kritičnih aplikacij bo potrebno občasno sodelovanje skrbnikov nadzornega sistema s sistemskimi tehniki, pa tudi s skrbniki aplikacij. Takšna je bila tudi praksa pri preizkušanju nadzornega sistema.

- K sodelovanju smo povabili skrbnike posameznih sistemskih in aplikativnih sklopov aplikacije PAV. Posamezni skrbniki so izpostavili najpogostejše težave, s katerimi se soočajo. Skušali smo jih simulirati in odpraviti z novim nadzornim sistemom. Ker se težave nanašajo na sistemske in aplikativne dele informacijskega sistema ter zaradi večje obsežnosti in tudi težje razumljivosti simuliranih primerov, so v tabeli 1 združeni splošni primeri reševanja tako sistemskih kot tudi aplikativnih problemov po starem načinu in po načinu z uporabo nadzornega sistema IBM Tivoli Monitoring.

Tabela 1: **Primerjava starega načina nadzora z novim**

Obstoječi način nadzora	Uporaba nadzornega sistema IBM Tivoli
O napaki v delovanju poslovnih storitev nas preko help deska obvestijo uporabniki.	Sistemske napake v delovanju poslovnih storitev oz. njihov nastanek zaznamo pred uporabniki.
Za pregled nad delovanjem informacijskega sistema uporabljamo več različnih orodij, ki imajo različno urejene dostope in poglede. S celovitim pregledom nad informacijskim sistemom in povezanostjo komponent ter aplikacijami ne razpolagamo. Slika o trenutnem dogajanju na sistemu oz. o stanju delovanja aplikacij ni jasna, odstopanja ne zaznamo najhitreje.	Kljub uporabi različnih nadzornih orodij znotraj celotnega sklopa nadzornega sistema imamo ves pogled združen na enem mestu – portalu (TEP). Razpolagamo s celovitim pregledom in nadzorom nad informacijskim sistemom in aplikacijami. Natančno vemo, kaj se trenutno dogaja na sistemu ali z aplikacijami, hitro zaznamo že najmanjša odstopanja.
S podatki o odzivnih časih razpolagamo le, če smo spremljanje časov programirali v aplikacije oz. opravljali meritve na komponente oz. med njimi.	Nadzorni sistem omogoča spremljanje odzivnih časov med strežniki, aplikacijami, transakcijami.
Napako je treba locirati glede na uporabniške razlage iz logov, iz sistemskih izpisov itn. Izkušnje pri delu in pri uporabi različnih orodij so pomemben dejavnik za hitro lociranje napake.	Nadzorni sistem omogoča hitro lociranje napake in pohitritev postopka odprave napake. Dejansko napako lahko zaznamo, tudi če nismo skrbnik oz. strokovnjak na tem področju.
Napak na sistemu ne znamo predvideti, razen če jih prej nismo izkusili ali namerno povzročili.	Nastanek napake znamo predvideti v dejanskem času, npr. s pomočjo pregleda nad odzivnimi časi, ki se povečajo, ter tako v delovanju opazimo odstopanja od normalnega stanja. (Višja stopnja uporabe orodja nam ob implementaciji podatkovnega skladišča na podlagi povezovanja pretekih dogodkov zna predvideti napako, ki se je v preteklosti že zgodila.)
Ozka grla odkrivamo na podlagi izkušenj, meritev in analiz posameznih sklopov aplikacije oz. komponent informacijskega sistema.	Odkrivanje ozkih grl aplikacij je preprosto, s pomočjo grafičnih prikazov hitro vidimo, kje je treba optimizirati procese, in s tem posledično že lahko zmanjšamo stroške za analizo in načrtovanje za pripravo na povečani obseg poslovanja v prihodnosti.
Za predstavnost aplikacij smo skrbeli s procesnimi slikami, narisanimi s procesnimi orodji, kot sta npr. erwin in visio.	Rešitve Tivoli omogočajo lažjo predstavnost, odkrivanje detajlov v delovanju, povezanosti ter lociranja nameščenih sklopov aplikacije po komponentah informacijskega sistema.
Za izvajanje ukazov na posameznih komponentah moramo poznati veliko število sistemskih ukazov.	Posamezno orodje nadzornega sistema že vsebuje velik nabor sistemskih ukazov za posamezno komponento.
Za nadzor osrednjega računalniškega informacijskega sistema uporabljamo uporabniku oz. skrbniku ne preveč prijazen terminal, grafični prikazi in poročila so redkost. Distribuirana okolja imajo svoje nadzorne produkte.	Uporabniku prijazen vmesnik, poročila so v grafični in tabelarični obliki ter v obliki topologij. Na enem vmesniku nadzorujemo tako osrednji računalniški informacijski sistem, kakor tudi distribuirana okolja.
Prehod med komponentami za različne poizvedbe je počasen, potrebne so večkratne prijave v različne sistemske komponente (npr. v vsak CICS TS se je treba posebej prijaviti, prav tako za delo na produkcijskem LPAR-u,[4] administratorski konzoli za WAS itn.).	Za prehod iz pogleda ene komponente na drugo je potreben le klik, avtorizacija se izvede ob prijavi v TEP.

Iz tabele 1 lahko povzamemo, da je obladovanje informacijskega sistema banke z novim nadzornim sistemom lažje kot z obstoječim načinom nadzora.

Za vodstvo smo sestavili razpredelnico (tabela 2), ki prikazuje prispevek k hitrejši oz. lažji realizaciji strateških ciljev z uporabo nadzornega sistema IBM Tivoli.

[4] LPAR (angl. Logical Partition) – logična enota, navidezno ločevanje strojnih komponent na več logičnih enot, particij.

Tabela 2: **Prispevek k doseganju strateških ciljev po področjih**

Strategija informacijske tehnologije v NLB (Vir: Strategija informacijske tehnologije 2011—2014, interni dokument)		**Prispevek nadzornega sistema k lažjemu doseganju ciljev**
PODROČJE	**CILJ**	
FINANCE	*Optimizacija poslovnih procesov, izboljševanje kakovosti, učinkovitosti ter zanesljivosti izvajanja storitev informacijske tehnologije*	S pomočjo sprotnega spremljanja tako sistemskih komponent kot tudi aplikacij ter z vizualnim pregledom nad ozkimi grli bomo zmanjšali stroške poslovanja in stroške, ki nastanejo ob izpadu v delovanju informacijskega sistema oz. aplikacij. Poznavanje problemov je prvi korak pri optimizaciji procesov. Že z odpravo manjših težav lahko prispevamo k izboljšanju učinkovitosti in zanesljivosti storitev informacijske tehnologije. Z uporabo orodij in novosti, ki jih prinaša nadzorni sistem, bomo dolgoročno zagotovo izboljšali stopnjo zanesljivosti informacijskega sistema.
STRANKE	*Zagotavljanje učinkovite informacijske podpore poslovanju banke, ki bo omogočala uresničevanje ciljev po poslovnih področjih*	Z izboljšanjem zanesljivosti in z optimizacijo procesov bo tudi informacijska podpora poslovanju veliko bolj učinkovita, strankam in poslovnim partnerjem pa bomo ponudili še bolj zanesljive storitve, za katere bomo natančno vedeli, kako delujejo tisti trenutek.
ZAPOSLENI	*Uporaba orodij, ki zagotavljajo hitro in učinkovito delo, vzpostaviti okolje, ki omogoča razvoj zaposlenih in v katerem so zaposleni temeljni vir*	Nadzorni sistem s pomočjo svojih orodij in napredno tehnologijo na področju sprotnega nadzora in vizualizacije pomaga izboljšati predstavnost in s tem hitrost odpravljanja težav ter optimizacijo delovanja. Tudi avtomatizacija odprave težav bo prispevala k skrajševanju časa za odpravo težav in s tem posledično prispevala, da bodo imeli zaposleni več časa za spremljanje novosti in inovativnih pristopov na svojem področju dela.
PROCESI	*Povečevanje stroškovne učinkovitosti informacijske in komunikacijske tehnologije*	S poznavanjem procesnih problemov in ozkih grl ter tudi z odpravo le-teh bomo povečali stroškovno učinkovitost informacijske in komunikacijske tehnologije, poleg tega pa se bomo lažje pripravili na povečan obseg dela v prihodnosti, s katerim se že soočamo ob določenih dnevih.

Dejansko ni nič nenavadnega, da predstavljeni nadzorni sistem posega na vsa področja strateških ciljev. To dokazujejo dejstva, da so si prakse in menedžerski pristopi k izboljšavam strategij informacijske tehnologije pravzaprav zelo podobni. Ustvarjeni so bili različni okviri, da bi pomagali strokovnjakom informacijske tehnologije optimizirati uporabo tehnologije in izboljšati opravljanje procesov informacijske tehnologije. Infrastrukturna knjižnica informacijske tehnologije (angl. Information Technology Infrastructure Library – Itil) zagotavlja nabor najboljših praks, ki pomagajo organizacijam doseči visokokakovostne poslovno usklajene storitve. Osredinja se predvsem na to, kaj je treba storiti, da se zagotovi vrednost storitev informacijske tehnologije, ne razlaga pa, kako to efektivno doseči. To pomanjkljivost lahko premostimo z drugimi pristopi upravljanja storitev (Kastelic in Peer, 2012). Če se vrnemo na ugotovitve v prejšnem odstavku omenjene IBM-ove knjige, pa IBM Service Management in programska oprema IBM Tivoli (ta koncept je prikazan na sliki 1) pomagajo organizacijam, da je opravljanje storitev in ITIL procesov izvedljivo. Rezultat prikazujemo v tem prispevku z opisanim pristopom, ki pomaga izboljšati servisne storitve z izboljšano vidljivostjo, kontrolo in avtomatizacijo.

Tako vodstvo kot tudi skrbniki posameznih področij so bili nad predstavitvijo navdušeni, nekoliko manj pa so bili navdušeni nad kompleksnostjo nadzornega sistema in dokaj veliko porabo virov (CPU) osrednjega računalnika.

Poleg potrebne optimizacije TEMS-a bo moral biti nadzorni produkt nameščen tudi v predprodukcijskem okolju, v katerem bomo v času testiranja aplikacij poleg nadzora delovanja nadzornega sistema, informacijskega sistema in poslovnih aplikacij odkrivali ozka grla, katera naj bi odpravili pred prenosom programske kode in/ali sistemskih nadgradenj v produkcijsko okolje. Informacijski sistem banke naj ne bi dosegel stoodstotne obremenjenosti v produkcijskem okolju, saj bi nas nadzorni sistem na povečanje porabe resursov in/ali na odstopanja od normalnega delovanja opozarjal že veliko prej. Celo več, določene težave bi lahko reševal sam, ko bi nastopile oz. še pred tem.

Seveda pa je pri zaznavanju povečane porabe resursov informacijskega sistema treba ločevati, ali gre za performančne probleme zaradi aplikativnih oz. sistemskih nadgradenj ali je vzrok težav v povečanem obsegu količine podatkov. Ne glede na vrsto težave je treba v takšnih primerih ukrepati zelo hitro. Po Cherkasova idr. (2009) je treba ukrepati takrat, ko uvedemo

posodobitev aplikacije, in/ali takrat, ko se pojavijo nepričakovani performančni problemi. Pomembno je ločiti performančne probleme, katerih vzrok so večje količine podatkov, od performančnih problemov, katerih vzrok so morebitne napake ali neučinkovitosti pri nadgrajeni programski opremi. Po Ganek idr. (2008) so rešitve Tivoli v pomoč pri avtomatiziranem izvajanju korektivnih ukrepov, kakor tudi pri analizi temeljnih vzrokov, saj zagotavljajo korelacijo več informacijskih sistemov na strežniški ravni.

Nekaj komponent nadzornega sistema za potrebe nadzora sistemski komponent smo že namestili v produkcijsko okolje. Uporabljamo jih za zaznavanje odstopanj od normalnega delovanja CICS TS ter za avtomatizirano vključujevanje in izključujevanje obsežnega in potratnega beleženja sistemskih zapisov v primeru povečanega obsega prometa.

Prav tako smo na produkcijskem okolju že avtomatizirali zaznavanje, obveščanje in ponovni zagon enega izmed procesov kupljenega programa ter obsežen ročni poseg, ki ga je treba izvesti ob izpadu delovanja procesa, in tako dosegli, da je ta proces poleg alarmiranja in obveščanja tudi popolnoma avtonomen.

S tem je tudi dokazano, da je vključitev katerega koli produkta pod nadzor pravzaprav mogoča in dokaj preprosta glede na to, za kakšen proizvod gre (lastni razvoj, neki specifični kupljeni proizvod ali prvotni proizvod IBM), pomembno je le, da je nameščen v okolju, ki je pod nadzorom nadzornega sistema IBM Tivoli. Ne moremo se izogniti dejstvu, da je končna rešitev nadzornega sistema velikokrat kombinacija uporabe nadzornega sistema IBM Tivoli Monitoring in programiranih rešitev lastnega razvoja.

Trenutno še nerealizirana naloga in največji izziv bo implementacija nadzornega sistema za potrebe spremljanja transakcijskih tokov v produkcijskem okolju, saj bo transakcijska slika zelo razvejena in prepletena, treba bo odstraniti posamezne, predvsem nepomembne gradnike in narediti sliko pregledno in razumljivo, kar pa ni vedno popolnoma izvedljivo. Tudi z vidika porabe resursov osrednjega računalniškega sistema, velik delež CPU-ja porabi ravno del nadzornega sistema za nadzor transakcij in ga bo nujno treba optimizirati.

Glede na omenjena dejstva iz študije ob uporabi oz. primerjavi nadzornega sistema z obstoječim načinom dela ter skladno s strategijo informacijske tehnologije banke smo opravili analizo SWOT.

Prednosti

- Celovit nadzor informacijskega sistema banke na enem mestu
- Spremljanje oz. nadzor nad sistemom, aplikacijami in transakcijami
- Izris strežniško-sistemske in transakcijske topologije
- Spremljanje in nadzor povezav med osrednjimi računalniškimi in distribuiranimi sistemi.
- Stalen in sproten performančni nadzor v dejanskem času in prikaz odzivnih časov medsebojne komunikacije med programi, aplikacijami oz. strežniki
- Dvig razpoložljivosti infrastrukture informacijske tehnologije in aplikacij
- Hitra izolacija, diagnostika in odprava nastale težave
- Zgodnje odkrivanje težav
- Možnost zaznave nastanka težave, preden ta nastopi oz. se razširi na ves sistem
- Samodejna odprava težave na podlagi prednastavljenih pravil
- V IBM Tivoli vgrajeni nasveti (najboljša praksa), razširljivi z lastno bazo znanja
- Zmanjševanje poprečnega časa odprave napak (MTTR – Mean Time To Repair) in povečanje poprečnega časa med pojavi napak (MTBF – Mean Time Between Failures)
- Večje zadovoljstvo končnih uporabnikov bančnih storitev (večja zanesljivost in razpoložljivost storitev)

Slabosti

- Velika poraba resursov osrednjega računalnika CPU (v produkcijskem okolju je ocenjeno na najmanj 15–20 %)
- Draga in dolgotrajna implementacija
- Dokaj nova tehnologija in s tem povezane napake v novih komponentah nadzornega sistema
- Počasno dobavljanje popravkov
- Potrebno je veliko ljudi za upravljanje in vzdrževanje.
- Ni zadosti znanja za samostojno upravljanje sistema nadzora.
- Nadzor in samodejna odprava težav kupljenih specifičnih programskih produktov znata biti težavna, saj v nadzornem sistemu rešitve niso povsem implementirane in zahtevajo razvoj lastnih dopolnilnih rešitev.

Priložnosti

- Uveljaviti NLB kot sinonim zanesljive banke, ki vedno ve, kaj se dogaja na informacijskem sistemu
- Ponudba zanesljivega informacijskega sistema obstoječim poslovnim partnerjem oz. potencialnim novim
- Uporaba dodatnih orodij za menedžerski nadzor, izdelavo poslovnih poročil
- Nadzor in odkrivanje performančnih problemov kupljenih produktov in specifičnih programskih rešitev zunanjih izvajalcev, ki smo jih doslej lahko obravnavali le kot črno škatlo
- Izboljšanje produktivnosti in stroškovne učinkovitosti z racionalizacijo obstoječih poslovnih procesov (npr. enkratna kontrola nalogov na vhodu in ne večkratna na posameznih podprocesih)

Nevarnosti

- Ob implementaciji na produkcijsko okolje so lahko slike topologij zaradi velikega števila prikazanih podatkov nejasne.
- Morebitna nezmožnost pokrivanja celotnega informacijskega okolja
- Vzdrževanje nadzornega sistema je drago in zahtevno.
- Vpleteni ne bodo sprejeli novega načina dela, ne bo prave motivacije za delo in uporabo.
- Več stroškov z uporabo nadzornega sistema kot z odpravo težav
- Velika stroškovna in časovna izguba v primeru opustitve programa nadzora

Zaradi kompleksnosti nadzornega sistema v testiranje in analizo nismo uspeli namestiti nekaterih komponent in zato tudi nismo mogli preskusiti teh funkcionalnosti:

- predvidevanja in avtomatizacije odprave napak na podlagi pravil iz preteklih dogodkov z uporabo skladišča podatkov (Data Warehousea); dejansko je to ena izmed rešitev, ki omogoča vzpostavitev avtonomnega sistema;
- nadzora omrežja in delovnih postaj;
- menedžerskega pregleda nad dogodki;
- uvedbe produktov za ekološki menedžment (angl. Green Management).

Bistvo celotnega nadzornega sistema ni več samo nadzor, je tudi zmožnost optimizacije informacijskega sistema, predvidevanja nastanka napak, nižanja stroškov poslovanja itn. Nadzorni sistem je zmožen nadzirati tako rekoč vse, tudi porabo energije, in tako tudi spodbuja oz. pripomore k hitri realizaciji ciljev ekološko usmerjenega menedžmenta.

Kot piše Kovačič (1998: 62), mora načrtovanje informatike izhajati iz strateškega načrtovanja potreb podjetja, ki se zrcalijo v smotru poslovanja, ciljih in strategiji podjetja, opredeljenih v strateškem načrtu podjetja. Ker je informacijska tehnologija eden najpomembnejših delov podjetja, moramo za doseganje poslanstva skupine NLB najprej dosegati strateške cilje informacijske tehnologije. Po dosedanjih spoznanjih bi po mnenju avtorja zastavljene cilje veliko lažje in hitreje dosegli z uporabo novega nadzornega sistema, saj je z njim mogoče poseči v vsa najpomembnejša področja strateških ciljev.

8 SKLEP

Implementacija celotnega nadzornega sistema, predvsem nadzor transakcijskih tokov, je zahtevna naloga, za kar potrebujemo razmeroma veliko časa. Na podlagi spoznanj, do katerih smo prišli pri uporabi nadzorne tehnologije, ki smo jo prikazali v članku, ugotavljamo, da je banka naredila korak v pravi smeri. Celovita rešitev pa bo zahtevala še veliko testiranja, nadgrajevanja in optimizacije.

Implementacija predstavljenega nadzornega sistema, predvsem nadzor toka transakcij na produkcijskem okolju banke bo zahtevala tudi strokovno usposobljene in motivirane zaposlene. Usposabljanje in izpopolnjevanje zaposlenih na različnih delovnih področjih že poteka, od ustrezno usposobljenih in motiviranih ljudi pa je odvisna absorpcijska sposobnost. Pomembno je, da gradimo na prednostih in izkoristimo priložnosti, ki nam jih ponuja nadzorni sistem, obenem pa se moramo zavedati nevarnosti in se pripraviti na morebitne negativne scenarije, ki nas čakajo v primeru neuspešne implementacije.

9 LITERATURA

[1] Abdul-Malek, A. (2010). Development of system automation and monitoring tool for heterogeneous platforms. Doktorska disertacija. Tennessee State University. ProQuest Dissertations and Theses, pridobljeno 20. 6. 2012 s http://search.proquest.com/docview/516421401?accountid=28931.

[2] Agarwala, S., Bathen, L. A., Jadav, D. & Routray, R. (2010). Configuration discovery and monitoring middleware for enterprise datacenters. *Network Operations and Management Symposium (NOMS)*, 19–23 April 2010 (2010 IEEE), str. 639–646. DOI: 10.1109/NOMS.2010.5488423.

[3] Cherkasova L., Ozonat K., Mi, N., Symons, J. & Smirni, E. (2009). Automated anomaly detection and performance modeling of enterprise applications. *ACM Transactions on Computer Systems*, 27(3), Article No. 6, DOI: 10.1145/1629087.1629089.

[4] Dubie, D. (2004). IBM Tivoli digs deeper into app transactions. *Network World*, 21(40):72.

[5] Ganek, A. G., Hilkner, C. P., Sweitzer, J. W., Miller, B. & Hellerstein, J. L. (2004). The response to IT complexity: autonomic computing. V: *Network Computing and Applications, 2004. (NCA 2004). Proceedings. Third IEEE International Symposium*, 30 Aug.–1 Sept. 2004, str. 151–157. DOI: 10.1109/NCA.2004.1347772.

[6] Haberkorn, M. & Trivedi, K. (2007). Availability Monitor for a Software Based System. *High Assurance Systems Engineering Symposium, 2007. HASE '07*. Dallas, Texas, 14–16 Nov. 2007, str.321–328. DOI: 10.1109/HASE.2007.49.

[7] Hicks, M. (2004). *Optimizing Applications on Cisco Networks*, Cisco Press.

[8] Hu, Y. B., Feng, F., Gucer, V., Huang, J., Jiang, B. & Mackler, R. (2008). Monitoring the IBM Tivoli Composite Application Management Server V6.1, IBM Corp. Redpaper, 24 januar 2008, pridobljeno 20. 6. 2012 s http://www.redbooks.ibm.com/redpapers/pdfs/redp4353.pdf.

[9] Huebscher, M. C. & McCann, J. A. (2008). A survey of autonomic computing-degrees, models, and applications. *ACM Comput. Surv*., 40(3), 7–1 – 7–28. DOI: 10.1145/1380584.1380585.

[10] IBM (2011a). Simplifying administration with IBM Integrated Service Management, (22. 3. 2011), pridobljeno 20. 3. 2012 s http://www-01.ibm.com/software/success/cssdb.nsf/CS/LWIS-8LXG57?OpenDocument&Site=tivoli&cty=en_us.

[11] IBM (2011b). BG-Phoenics extends the benefits of mainframe computing, With the world's first production deployment of IBM zEnterprise with the zBladeCenter Extension, (8 december 2011), pridobljeno 20. 3. 2012 s http://www-01.ibm.com/software/success/cssdb.nsf/CS/STRD-8PBJCA?OpenDocument&Site=tivoli&cty=en_us.

[12] IBM (2011c). Tivoli Monitoring for Transaction Performance (12. 11. 2011), pridobljeno 5. 3. 2012 s https://www.ibm.com/developerworks/wikis/display/tivolidoccentral/Tivoli+Monitoring+for+Transaction+Performance.

[13] IBM Plans New Tools to Support Tivoli System z Management Software (2007). Wireless News (5. december 2007), pridobljeno 10. 4. 2012 s http://business.highbeam.com/165048/article-1P1-146775679/ibm-plans-new-tools-support-tivoli-system-z-management.

[14] Kastelic M. & Peer, P. (2012). Managing IT Services: Aligning Best Practice with a Quality Method. *Organizacija*, 45: 31–37. DOI: 10.2478/v10051-012-0004-6.

[15] Kovačič, A. (1998). *Informatizacija poslovanja*. Ljubljana: Ekonomska fakulteta.

[16] Mulej, M. (2003). Mehanizmi in ukrepi za prenos znanja iz akademske in raziskovalne sfere v gospodarstvo v luči novih inovacijskih paradigem – stanje in trendi razvoja v Sloveniji glede na razvite države EU – absorpcijska sposobnost. Skrajšana verzija raziskovalnega poročila, 5. avgust 2011, pridobljeno 20. 6. 2012 s http://leonardopublic.innovation.si/9.Innovation%20and%20R&D%20support%20system/Mulej-za%20LdV-03Povzetek-absorbSpos%20(Slovenian).doc.

[17] Musich, P. (2004). IBM Broadens Tivoli Tracking; IBM is launching a new version of its IBM Tivoli Monitoring for Transaction Performance software that will greatly expand the range of application transactions it can track. *eWeek*, 21(41): 32, pridobljeno 20. 12. 2011 s http://www.highbeam.com/doc/1P3-712996261.html.

[18] NLB (2011a). Strategija informacijske tehnologije 2011–2014. Nova Ljubljanska banka, interni dokument, 23. 2. 2011.

[19] NLB (2011b). Novice informacijske tehnologije: Predstavitev Oddelka za razvoj upravljanja s podatki in integracijo informacijskega sistema banke. Nova Ljubljanska banka, interni dokument, 20. 7. 2011.

[20] Paxton, N. C., Ahn, G. & Shehab, M. (2011). MasterBlaster: Identifying In»uential Players in Botnet. *Transactions. 35th IEEE Annual Computer Software and Applications Conference*, München, 18–20 July 2011, str. 413–419. DOI: 10.1109/COMPSAC.2011.61.

[21] Sengupta, B., Banerjee, N., Bisdikian, C. & Hurley, P. (2008). Tracking transaction footprints for non-intrusive, end-to-end monitoring. *Cluster Computing*, 12: 59–72, DOI 10.1007/s10586-008-0066-7.

[22] Sterritt, R. (2005). State of the art: Autonomic computing. *Innovations Syst Softw Eng,*1, 79–88, DOI 10.1007/s11334-005-0001-5.

[23] Veyder, F. (2003). Case study: Where is the risk in transaction monitoring? *Journal of Financial Regulation and Compliance*, 11(4): 323–328. DOI: 10.1108/13581980310810606.

[24] Wang, K., Wu, Z., Luan, Z. & Qian, D. (2008). Reducing the Cluster Monitoring Workload by Identifying Application Characteristics, *GCC '08 Proceedings of the 2008 Seventh International Conference on Grid and Cooperative Computing*, IEEE Computer Society Washington, DC, USA, str. 525–531. DOI: 10.1109/GCC.2008.56.

[25] Yang, F., Shao, P., Le, Q., & Li, D. (2010). Commentary on the Supervision of Foreign Banking IT Risks. *International Conference on E-Business and E-Government (ICEE)*, Guangzhou, 7–9 May 2010, str. 2026–2028. DOI: 10.1109/ICEE.2010.512.

▪

Simon Sirc je zaposlen kot samostojni sistemski analitik v NLB, d. d., v sektorju za razvoj informacijskega sistema banke, kjer skrbi za razvoj in nemoteno delovanje sklopa poslovno kritičnih aplikacij plačilnega prometa v domovini. Leta 2006 je diplomiral na Fakulteti za organizacijske vede Univerze v Mariboru. Na isti fakulteti končuje magistrski študij.

▪

Jože Zupančič je upokojeni redni profesor na Fakulteti za organizacijske vede Univerze v Mariboru. Njegovi raziskovalni interesi so razvoj in uvajanje računalniških rešitev in informacijskih sistemov.

Ekonomika virtualizacije namizij

[1]Miha Potočnik, [2]Mirko Gradišar
[1]Občina Jesenice, Cesta železarjev 6, 4270 Jesenice; [2]Univerza v Ljubljani, Ekonomska fakulteta, Kardeljeva ploščad 17, 1000 Ljubljana
miha.potocnik@fov.uni-mb.si; miro.gradisar@ef.uni-lj.si

Izvleček

Virtualizacija računalniških namizij je alternativa klasičnim osebnim računalnikom. Na dolgi rok zmanjšuje stroške lastništva osebnih računalnikov, zagotavlja lažje vzdrževanje, boljši izkoristek in veča varnost in zanesljivost. Članek obravnava koristi in slabosti virtualizacije namizij in podaja pregled njihovega delovanja. Na primeru prikaže ekonomiko virtualizacije namizij v primerjavi s klasičnimi osebnimi računalniki.
Ključne besede: virtualizacija namizij, tanki odjemalec, analiza stroškov in koristi, ekonomika.

Abstract

The Economics of Desktop Virtualization Infrastructure

Virtual computing is an alternative to conventional desktop PC. In the long run it reduces the cost of ownership of personal computers, provides easier maintenance, better efficiency and increases safety and reliability. This paper addresses the benefits and disadvantages of desktop virtualization and gives an overview of these. A practical example shows the economics of desktop virtualization compared to conventional PCs.
Keywords: desktop virtualization, thin client, cost-benefit analysis, economics.

1 UVOD

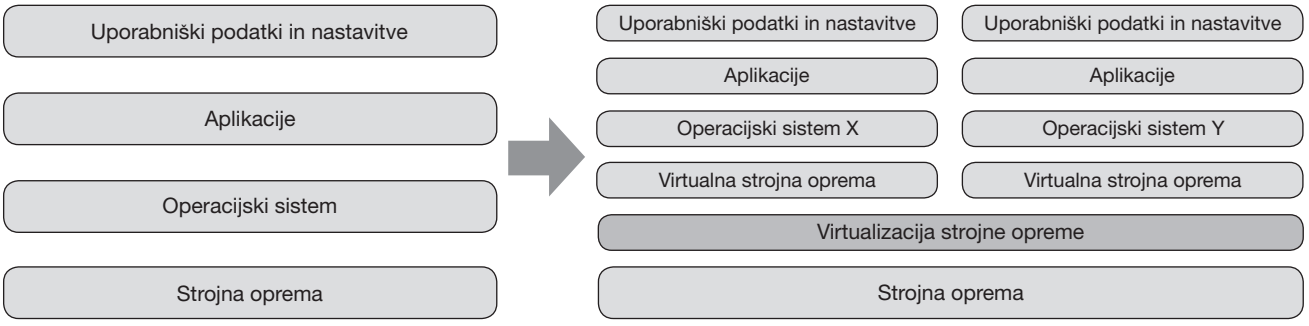
Virtualizacija danes v večini organizacij ni več novost. Oddelkom za informatiko je omogočila znižanje stroškov za strojno opremo, izboljšanje upravljanja strežnikov in prihranke pri porabi električne energije. V mislih imamo virtualizacijo strežnikov, ki je informacijskim oddelkom prinesla tudi avtomatizacijo mnogih časovno potratnih opravil, medtem ko so nekatere druge oblike virtualizacije, kot je npr. virtualizacija namizij, še bolj na začetku uveljavljanja. Virtualizacija namizij (tudi virtualizacija odjemalcev) je koncept, ki ločuje namizje osebnega računalnika od fizične naprave, na kateri dela uporabnik. Virtualizirano namizje z vsemi programi, aplikacijami, procesi in podatki se pri tem zagotavlja in shranjuje v oddaljenem strežniku v podatkovnem centru. Končni uporabnik se s svojim računalnikom v podatkovnem centru povezuje s pomočjo posebne programske rešitve, pri čemer lahko uporablja zelo različne naprave, od običajnih osebnih računalnikov do pametnih telefonov, tankih odjemalcev ali celo ničnih odjemalcev (angl. zero client). Koristi strežniške virtualizacije so zelo oprijemljive, saj lahko s številkami preprosto ponazorimo doseženo zmanjšanje števila strežnikov ali prihranke pri energiji. Poleg tega pa so koristi tudi posredne in se kažejo predvsem v učinkovitejšem upravljanju informacijske infrastrukture.

V nadaljevanju bomo pregledali temeljne gradnike virtualnega namizja ter analizirali več mogočih rešitev virtualizacije namizij. Nanizali bomo tudi prednosti in slabosti virtualizacije namizij ter na primeru izvedli analizo stroškov in koristi.

2 TEMELJNA IDEJA VIRTUALIZACIJE

Pri virtualizaciji strojne opreme (Čuk in Harej, 2011) imamo na računalniku nameščeno programsko opremo, katere naloga je priprava simuliranega računalniškega okolja – virtualnega računalnika. V tem okolju se izvaja programska oprema gostujočih sistemov. Sistemsko programsko opremo, ki dodeljuje vire virtualnim računalniškim sistemom, imenujemo nadzornik (Hypervisor). Virtualizirane računalniške sisteme imenujemo gosti, osnovni sistem pa gostitelj.

Gostujoči sistemi se v celoti izvajajo enako, kot da bi potekali neposredno na strojni opremi. Nadzornik poskrbi, da dobi vsak sistem ustrezne virtualizirane različice računalniških virov, ki jih potrebuje za svoje izvajanje, in da pri dostopu do fizičnih virov ne prihaja do konfliktov. Nadzornik omogoča tudi uveljavljanje različnih varnostnih politik za dostop do vhodno-izhodnih naprav, procesorja in drugih virov.



Slika 1: **Grafični prikaz principa virtualizacije**

3 TEMELJNI GRADNIKI VIRTUALNEGA NAMIZJA

- ***Nadzornik (Hypervisor) – programska oprema, ki omogoča virtualizacijo in gosti slike namizja*** Obstajata dve vrsti nadzornikov. Prvi je sistem, ki poteka neposredno na gostiteljskem strežniku. Operacijski sistem teče na drugi ravni nad strojno opremo gostitelja. Po navadi imenujemo to vrsto nadzornika primarni nadzornik. Druga vrsta pa je program, ki teče znotraj operacijskega sistema. Gostujoči operacijski sistem teče na tretji ravni nad strojno opremo gostitelja.
- ***Upravitelj navideznega strežnika (Virtual machine manager)*** je program, s katerim upravljamo z navideznimi napravami. Upravitelj lahko zaganja, ustavlja in nadzoruje preko konzole navidezne naprave. Spremlja lahko statistiko, zmogljivosti in statuse navideznih naprav.
- ***Programska oprema, nameščena na drugem ločenem strežniku (Connection broker)***, ki usmerja zahteve tankih odjemalcev in jih povezuje s pripadajočimi navideznimi namizji.
- ***Navidezna naprava, skupek programske opreme, ki izvaja programe kot pravi računalnik (Virtual machine)*** Navidezna naprava je izolirana od strojne opreme. Poznamo dve vrsti navideznih naprav, in sicer procesno navidezno napravo, ki je sposobna poganjati le en program, in sistemsko navidezno napravo, ki je sposobna poganjati celoten operacijski sistem. Taki napravi rečemo tudi strojna navidezna naprava.

3.1 Vrste virtualnih namizij

Poznamo dve glavni arhitekturi virtualnega namizja pri uporabnikih, in sicer statično in dinamično (Petrović in Fertalj, 2009). Katero bomo izbrali, je odvisno od naših potreb. Če potrebujemo za vsakega uporabnika edinstveno virtualno namizje, bomo izbrali statično arhitekturo. Pri statični arhitekturi ima vsak uporabnik navidezno namizje, ki je prilagojeno njegovim potrebam. Več kot imamo uporabnikov, več navideznih namizij moramo ustvariti in upravljati. Navidezna namizja so običajno shranjena na skupnih diskih SAN ali NAS, povezanih na gostiteljski strežnik. Navidezna namizja so preko virtualne namizne infrastrukture VDI posredovana odjemalcem, ki so lahko navadni računalniki ali pa tanki oziroma nični odjemalci.

Pri dinamični arhitekturi pa imamo le eno navidezno napravo in eno navidezno sliko namizja, katera se replicira vsakemu uporabniku na podlagi njegovega profila in pravic. S tem ko imamo le eno glavno sliko namizja, se izognemo upravljanju in vzdrževanju več sistemov. Stroški upravljanja so tako zmanjšani, prihranimo pa tudi čas.

4 VIRTUALIZACIJA NAMIZIJ

Virtualizacija računalniških namizij (VDI – virtual desktop infrastructure) s stališča vzdrževanja in vseh stroškov lastništva (TCO – total cost of ownership) obljublja cenejšo in preprostejšo alternativo običajnim osebnim računalnikom (Kroeker, 2009). Za virtualna namizja (VDI – Virtual Desktop Infrastructure) potrebujemo le lahke odjemalce, na katere priključimo lokalne zunanje naprave.

Osebne računalnike, na njih delujoče operacijske sisteme, uporabniško namizje in programe, nadomestimo z navideznimi računalniki, ki delujejo na strežnikih v podatkovnem centru. Uporabniku ostane le preprost strojni odjemalec – kot vmesnik za zaslon, tipkovnica in miška –, ki na daljavo upravlja oddaljeni računalnik v podatkovnem centru. Koncept je na moč podoben že desetletja znanemu terminalskemu načinu dela, vendar je zasnovan na drugačnih temeljih.

Odjemalec je zaradi tehnologije VDI lahko zelo preprosta naprava, je bodisi lahki odjemalec (thin client), starejši osebni računalnik, ki sicer ne bi bil kos sodobnim operacijskim sistemom in programom, ali sodoben, a cenejši prenosnik. Za uporabnika osebnega računalnika se glede na dosedanje računalniško okolje spremeni zelo malo, če le zahteve niso prevelike ali specifične. Prehod na VDI je zato za večino uporabnikov nemoteč in prijazen.

Po drugi strani pa VDI pomeni ogromno spremembo za upravitelje sistemov. Olajša jim delo, saj lahko tako precej poenostavijo ter avtomatizirajo pripravo, razdeljevanje in vzdrževanje tovrstnega okolja, obenem pa zagotovijo večjo zanesljivost delovanja računalniškega namizja kot v primeru vzdrževanja fizičnih računalnikov pri uporabnikih (Bevec, 2010).

Po Fegreusu (2010) je poraba sistemskih sredstev, kot sta procesorski čas in pomnilniški prostor, racionalnejša. Lažje je izdelovati varnostne kopije, nadgrajevati in vzdrževati navidezne računalnike. S tehnologijo VDI lahko hitreje zagotovimo nov računalnik ali zamenjamo nedelujočega z novo svežo kopijo. Ker računalniki delujejo na strežnikih z visoko zanesljivostjo, je za njihovo brezhibnost in varnost delovanja bolje poskrbljeno kot pri navadnih osebnih računalnikih.

VDI prinaša prednosti za podjetja, v katerih upravljajo veliko število osebnih računalnikov, toda z napredkom izdelkov in s cenovno politiko proizvajalcev postaja VDI zanimiva alternativa tudi za manjša podjetja. Analitske družbe področju VDI v poslovnem okolju pripisujejo svetlo prihodnost. Pri družbi Gartner napovedujejo, da bo že leta 2014 približno 40 odstotkov vseh namizij uporabljalo eno od oblik virtualizirane namizne infrastrukture (Gartner, 2010).

Veliko navdušenje nad tehnologijo VDI je povzročilo, da se je na trgu v razmeroma kratkem času pojavilo veliko število ponudnikov teh rešitev. V ospredju je kljub temu le nekaj podjetij. Danes lahko ponudbo na trgu razdelimo na dva dela, in sicer na programske in strojne rešitve. V prvem primeru imamo opravka s programi odjemalci, lahko tudi za različne operacijske sisteme, ki dostopajo do navideznih računalnikov na strežnikih. Tovrstni odjemalci so zanimivi zlasti tam, kjer želimo kot terminale uporabiti obstoječe računalnike, ali pa kjer želimo imeti večjo prilagodljivost oz. možnost uporabe kombinacije krajevnega in oddaljenega namizja.

Bruzzese (2010) pravi, da se pravi učinki pokažejo šele z uporabo namenskih strojnih naprav tankih odjemalcev. Ti so preprostejši, navadno nekoliko cenejši od osebnih računalnikov, predvsem pa precej preprostejši za vzdrževanje. Največ, kar moramo postoriti pri njih, je vzdrževanje sistemske programske opreme (firmware), kar pomeni, da jih brez posebnih posegov lahko uporabljamo tudi več let. Ko se pokvarijo, jih preprosto nadomestimo z drugimi. Uporabnik ima vse nastavitve na varnem v navideznem računalniku v podatkovnem centru, zato je zamenjava hitra in preprosta.

Pri tehnologiji VDI odjemalci (programski ali strojni) dostopajo do navideznih računalnikov v strežniškem okolju. To pomeni, da moramo na strani strežnikov uporabljati eno od rešitev za virtualizacijo, ki pa tokrat ne gosti navideznih strežnikov, temveč navidezne odjemalce z okolji windows, redkeje z linuxom ali drugimi operacijskimi sistemi.

Na strežniški strani podprte izdelke predpisujejo proizvajalci. Načeloma bi izbrani izdelek lahko bil poljuben, vendar tu igra vsak proizvajalec svojo politiko odprtosti/zaprtosti za konkurenco. Čas bo pokazal, ali bo trajno ostalo tako ali pa se bodo morali prilagoditi in odpreti za druge.

Navidezne računalnike lahko pripravimo na različne načine, odvisno od potreb uporabnikov. Najbolj zanimiva je možnost, da nove navidezne računalnike ustvarimo na podlagi enotne začetne predloge diskovnih slik (nameščenega sistema in programov). Novi računalniki so tehnično gledano kloni prvotnega računalnika, s čimer jih hitreje pripravimo in lažje vzdržujemo. Poleg tega tovrstni kloni v nekaterih primerih porabijo na disku precej manj prostora, saj vsaka instanca (klon) zavzema na disku le toliko prostora, kolikor se razlikuje od diskovne slike izhodiščne predloge.

Tako pripravljene klone zopet lahko delimo na dva tipa – na stalne (persistent) in nestalne (non-persistent), ki jih po rabi zavržemo (VMware, 2011). V prvem primeru uporabnik dobi navidezni računalnik, ki se prvič samodejno (ali ročno) generira iz predloge, od tedaj dalje pa bo vselej tak, kot ga je uporabnik pustil pri predhodni rabi. Zanimivi so računalniki, ki jih po rabi preprosto zavržemo. Uporabnik bo pri naslednji prijavi zopet dobil svežo kopijo. To je uporabno zlasti takrat, ko želimo zavreči vse spremembe oziroma vselej začeti z začetnimi nastavitvami. Tak način tudi ne zahteva kasnejšega

vzdrževanja navideznih računalnikov, saj lahko le-tega vselej generiramo iz najnovejše predloge. Nazadnje so tu še najzahtevnejši uporabniki, ki imajo bodisi posebne zahteve ali pa uporabljajo specifične programe – zanje pripravimo računalnike ročno.

Cilj upraviteljev rešitev VDI je seveda ta, da si kar se da olajšajo delo in s tem avtomatizirajo tako strežnik kot tudi pripravo navideznih računalnikov. Tu se izdelki najbolj razlikujejo med seboj, saj imajo proizvajalci različne tehnologije in strategije.

Pri vzpostavitvi navideznih računalnikov si kmalu zastavimo vprašanje, koliko navideznih računalnikov lahko poganjamo na enem fizičnem strežniku s podporo za virtualizacijo operacijskih sistemov. Brez tega podatka ne moremo izračunati vseh stroškov lastništva za celovito rešitev, ki vključuje odjemalce, strežnike in potrebno programsko opremo. Odgovor ni preprost. Vse je odvisno od tipa operacijskega sistema, števila in tipa nameščenih programov v posameznem navideznem računalniku in povrhu vsega še od oblike izvedbe navideznega računalnika (namenski, klon itd.).

Število navideznih računalnikov, ki jih lahko poganjamo na enem gostujočem strežniku je do neke mere odvisno od števila procesorjev, predvsem pa od velikosti pomnilnika, ki ga imamo v strežniku. Če imamo, denimo, 8 GB RAM in vsakemu navideznemu namizju namenimo 512 MB, bomo teoretično lahko imeli največ 10–12 sočasnih sej (nekaj bo strežnik porabil za svoje delovanje). V splošnem tudi velja, da bomo prej porabili prosti pomnilnik kot proste zmogljivosti procesorjev (VMvare, 2006).

4.1 Prednosti VDI

Virtualizacija namizij prinese nekatere koristi. Podatki so bolj varni. Podatki so shranjeni na skupnih diskovnih poljih in ne na končnih odjemalcih. Če je odjemalec ukraden, vsi podatki ostanejo na skupnem diskovnem polju.

Poenostavljeno je tudi upravljanje navideznih namizij. Upravljanje več sto računalnikov je lahko zelo zamudno in drago. Z implementacijo navideznega namizja na odjemalcih pa postane opravljanje hitro in učinkovito. Administrator se lahko iz enega mesta poveže na katero koli navidezno namizje in prevzame celoten nadzor.

Z enostavnim upravljanjem virtualnih namizij, ki temelji na predlogah navideznih računalnikov, zagotovimo, da vsi uporabniki upoštevajo in spoštujejo pravila, ki so za vse zaposlene enaka in zagotovljena z vnaprej pripravljenimi predlogami.

Implementacija VDI ne zahteva posodobitve strojne opreme. Uporabimo lahko odjemalce, ki temeljijo na računalnikih, katere že uporabljamo. Teh računalnikov ni treba nadgrajevati, saj za dostop in prikaz do navideznega namizja potrebujemo zelo malo zmogljivosti. Dovolj je že dostop do medmrežja, enostavna grafična kartica, monitor za prikaz slike in priklopljene periferne enote. Lahko pa se odločimo tudi za tanke ali nične odjemalce, ki so višji strošek, vseeno pa kasneje ne terjajo posodobitev in nadgrajevanj. Strojna oprema ne zastara, saj vse procesiranje opravi strežnik, odjemalec pa prikazuje le rezultate, zato so stroški vzdrževanja v vsakem primeru na dolgi rok nižji.

Vsak navidezni računalnik je predstavljen kot slika, katero lahko kopiramo in premikamo iz enega strežnika na drugega. S pomočjo virtualne tehnologije ustvarjamo posnetke sistema (angl. Snapshot) in s tem hitro povrnemo navidezni računalnik v predhodno stanje. Z uporabo tankih odjemalcev zmanjšamo negativen vpliv na okolje, saj porabimo manj električne energije kot navadni namizni računalniki.

Z uporabo navideznega namizja se zelo poveča uporabnost in mobilnost računalnika. Če ima uporabnik dostop do interneta, se lahko praktično s katero koli napravo poveže do oddaljenega namizja od koder koli na svetu. Vse, kar potrebujemo, je VPN račun in pravilno nastavljeno in dodeljeno virtualno namizje.

Na enem strežniku lahko konsolidiramo več navideznih namizij, s tem pa zmanjšujemo stroške. Implementacija virtualnega namizja je dokaj enostavna in stroškovno nezahtevna. Odjemalec je lahko praktično katera koli naprava z dostopom do omrežja in procesorjem 300 MHz in 128 Mb delovnega pomnilnika ali še manj. Ni potrebe, da bi kupovali močnejše odjemalce, da bi uspešno implementirali virtualno namizje.

4.2 Slabosti VDI

Virtualna namizja so velikokrat manj zmogljiva kot fizični računalniki. Predvsem grafične in multimedijske zmogljivosti so slabše. Slaba stran je tudi ta, da moramo vedno imeti dostop do omrežja, saj je drugače odjemalec nekoristen in neuporaben. Če imamo probleme z omrežjem, ne moremo delati.

Velikokrat lahko postane problem tudi strojna oprema, saj če odpove ključna komponenta, ki nima zagotovljene redundance, lahko odpovejo vsi navidezni računalniki.

Poleg tega je drago zagotavljanje redundantnosti, še posebno skupnih diskovnih polj, napajanja in kopiranja varnostnih kopij.

4.3 Alternativne oblike virtualizacij namizij

Možnosti, kako realizirati strežniško podprte virtualizacije namizij, je več. V najenostavnejših primerih gre lahko le za upravljanje oddaljenega strežnika z uporabo VNC-ja, oddaljenega dostopa ali Terminal services v okoljih windows. Tako lahko do poljubnega namizja dostopamo s kakršne koli naprave. Te rešitve so na voljo že dlje časa. Pravo vrednost pa virtualizacija namizij pokaže, ko razmišljamo, kako bi čim bolj zmanjšali stroške upravljanja z računalniškimi sistemi. Večkrat je cenejši nakup enega močnejšega strežnika in veliko tankih oziroma ničnih odjemalcev kakor več samostojnih računalniških sistemov. Ker se celotno procesiranje izvaja na strežniku, so lahko odjemalci računalniški sistemi z zelo omejenimi viri, lahko tudi starejši računalniki, ki bi jih sicer v podjetju ne uporabljali več. Take rešitve se označujejo s kratico VDI – Virtual Desktop Infrastructure.

Razlika med VDI in oddaljenim upravljanjem je zelo velika. Pri VDI ima vsak odjemalec svoj oddaljeni virtualni stroj, pri oddaljenem upravljanju pa lahko dela več uporabnikov na istem računalniškem sistemu.

5 ANALIZA STROŠKOV IN KORISTI NA PRIMERU UVEDBE VIRTUALNIH NAMIZIJ ZA 60 DELOVNIH MEST NA OBČINI JESENICE

Turk (2005, 153) pravi, da podjetja zaradi doseganja boljših poslovnih rezultatov na eni strani skušajo zmanjševati stroške (zato moramo vsako naložbo posebej utemeljiti), po drugi strani pa želimo razkriti, v čem so tiste prednosti, ki nam jih prinaša določena tehnologija.

»V analizo skušamo zajeti celotno obdobje uporabe rešitve oz. celotno dobo, v kateri nam bo rešitev povzročala stroške in prinašala koristi. Navadno je časovni obseg izražen v letih,« pravi Turk (2005, 156).

5.1 Opis investicijskega projekta

Ključna sprememba je prehod s 60 fizičnih računalnikov na virtualna namizja z ničnimi odjemalci. Investicija vsebuje nakup ničnih odjemalcev, strežniške infrastrukture in licence.

Primerjali bomo obstoječe stanje z stanjem prehoda na virtualna namizja (VDI). Ocenili bomo gibanje stroškov in koristi.

5.2 Vrsta analize stroškov in koristi

Analizirali bomo ekonomičnost projekta virtualizacije namizij. Zanima nas neto korist za projekt implementacije VDI.

5.3 Časovni obseg analize

Implementacija VDI zahteva sorazmerno velik delež sredstev, zato smo določili petletni časovni obseg analize. Pri diskontiranju bomo uporabili za izhodiščno leto leto 2012.

5.4 Enota mere

Glavni prikaz ekonomike VDI bo viden v izkazu denarnega toka. Z ustreznimi pristopi bomo vse količnike in kvalitativne podatke izrazili v denarju.

5.5 Kategorizacija stroškov in koristi

Stroške bomo razdelili na začetne stroške, stroške zamenjav, stroške delovanja ter neotipljive stroške. Enako bomo kategorizirali koristi, koristi delovanja ter neotipljive koristi. Po potrebi bomo prihranek stroškov prikazali kot korist, upadanje koristi pa kot strošek.

5.6 Diskontna stopnja

Splošna diskontna stopnja je sedemodstotna in jo kot javna ustanova po zakonu moramo upoštevati. Minister, pristojen za finance, lahko skupaj z ministrom, pristojnim za razvoj, določi drugo splošno diskontno stopnjo ali družbeno diskontno stopnjo na podlagi spremenjenih gospodarskih razmer, ki se objavi v Proračunskem memorandumu Republike Slovenije. (Uradni list RS, 2006) Ta odstotek bomo uporabili pri diskontiranju denarnih tokov na sedanjo vrednost, ter tako dobili diskontirani denarni tok, ki bo podlaga za presojanje.

5.7 Uporabljene metode za presojanje

Odločili smo se za uporabo dinamičnih metod, saj te upoštevajo časovno vrednost denarja. Presojali bomo z metodo neto sedanje vrednosti (NVS), razmerja stroškov in koristi (indeks donosnosti – ID), ter metode relativne neto sedanje vrednosti (RNSV).

5.8 Začetni stroški

V začetne stroške prištevamo nakup ničnih odjemalcev, dva strežnika, diskovno polje SAN in licence za uporabo programske opreme. Začetni stroški so podani v tabeli 1.

Tabela 1: **Prikaz začetnih stroškov**

Začetni stroški	2012
Število clientov zero	60
Cena clienta zero	400,00 €
Število strežnikov	2
Cena strežnika	5.000,00 €
Število data centrov SAN	1
Cena data centra SAN	4.000,00 €
Brezprekinitveno napajanje	1.200,00 €
Skupaj strežniki	10.000,00 €
Skupaj client zero	24.000,00 €
Licence	10.000,00 €
Skupaj začetni stroški	**45.200,00** €

Podatke smo pridobili iz predračunov, mogoča so le manjša odstopanja v primeru prilagoditev in sprememb, ki pa ne vplivajo na končni izid vrednosti investicije.

5.9 Stroški zamenjav

Tabela 2: **Stroški zamenjav v življenjski dobi projekta**

Stroški zamenjav/ Leta	2012	2013	2014	2015	2016	2017
Nadomestna baterija UPS			150,00 €		150,00 €	
Diskontirana vrednost		–	131,02 €	–	114,43 €	–

Ocenjujemo, da imajo strežniki, nični odjemalci in diskovno polje dolgo življenjsko dobo (vsaj pet let), katera se upošteva tudi pri izračunu amortizacije osnovnih sredstev, zato ne predvidevamo posebnih stroškov zamenjav. Menjati bo treba le baterijo pri brezprekinitvenem napajanju. Predvidevamo, da bo treba v petih letih baterijo zamenjati najmanj dvakrat. Ta strošek ocenjujemo na 300 evrov.

5.10 Stroški delovanja

Pri uvedbi virtualnih namizij predvidevamo stroške delovanja, ki so prikazani v tabeli 3.

Tabela 3: **Prikaz stroškov delovanja v petih letih**

Stroški delovanja/Leta	2013	2014	2015	2016	2017
Poraba električne energije	1.809,60 €	1.809,60 €	1.809,60 €	1.809,60 €	1.809,60 €
Posodobitve	360,00 €	360,00 €	360,00 €	360,00 €	360,00 €
Administracija in odpravljanje napak	2.500,00 €	2.500,00 €	2.500,00 €	2.500,00 €	2.500,00 €
Izobraževanja	700,00 €	700,00 €	700,00 €	700,00 €	700,00 €
Skupaj stroški delovanja	5.369,60 €	5.369,60 €	5.369,60 €	5.369,60 €	5.369,60 €
Diskontirana vrednost	5.018,32 €	4.690,02 €	4.383,19 €	4.096,44 €	3.828,45 €

Poraba in posodobitve

Poraba dveh strežnikov, izražena v kilovatih (0,8 KW/strežnik), pomnožena s povprečno ceno kilovatne ure 0,1 evra, če strežnika tečeta 24 ur na dan in 365 dni na leto, je strošek električne energije, ki jo strežnik porabi v enem letu. K temu prištejemo še porabo ničnih odjemalcev (34 W), če ti delujejo 8 ur na dan 250 dni v letu. Pri fizičnem pristopu pa smo upoštevali, da računalniki porabijo več energije (300 W) in delujejo 8 ur na dan 250 dni v letu. Lahkih odjemalcev tako rekoč ni treba vzdrževati. Vzdržujemo le strežnike, na katerih tečejo navidezna namizja.

Stroške posodobitve lahko izrazimo z izračunom:

število posodobitev na leto x potreben čas za posodobitev zlate slike x število zlatih slik

Izraz zlata slika se nanaša na glavno kopijo operacijskega sistema, na katerem temeljijo vsi fizični računalniki. V praksi pogosto najdemo več kot eno zlato sliko sistema. Pogosti vzroki temu so različne konfiguracije računalniške opreme, različne potrebe uporabnikov ali pa le slaba politika upravljanja. Vzdrževanje in posodabljanje različnih sistemov je drago in zamudno opravilo. Z virtualizacijo namizij število zlatih slik precej zmanjšamo. Imamo jih le toliko, kolikor imamo različnih potreb uporabnikov.

Izobraževanje

V primeru vzpostavitve novega okolja se mora sistemski administrator primerno izobraziti za upravljanje virtualnih namizij in gostiteljev. Cena začetnega dvodnevnega tečaja po ceniku znaša 700 evrov z DDV. (Housing, 2012)

5.11 Začetne koristi

Tabela 4: **Začetne koristi ob vpeljavi virtualnih namizij**

Začetne koristi	
Odprodaja stare računalniške opreme	1200 €

Leta 2013 bomo po sedanji vrednosti odprodali staro računalniško opremo po simbolni ceni 20 evrov. Začetna korist tako znaša 60 x 20 = 1200.

5.12 Koristi delovanja

Tabela 5: **Koristi delovanja VDI glede na fizične računalnike**

Koristi delovanja	**2013**	**2014**	**2015**	**2016**	**2017**
Prihranek električne energije	1.790,40 €	1.790,40 €	1.790,40 €	1.790,40 €	1.790,40 €
Prihranek pri posodobitvah	6.840,00 €	6.840,00 €	6.840,00 €	6.840,00 €	6.840,00 €
Racionalizacija administracije	10.000,00 €	10.000,00 €	10.000,00 €	10.000,00 €	10.000,00 €
Skupaj koristi	18.630,40 €	18.630,40 €	18.630,40 €	18.630,40 €	18.630,40 €
Diskontirana vrednost	17.411,59 €	16.272,51 €	15.207,96 €	14.213,04 €	13.283,22 €

Pri virtualizaciji namizij lahko predvidimo prihranek električne energije. Prihranek lahko izrazimo med razliko porabe fizičnih odjemalcev in seštevkom porabe ničnih odjemalcev in strežnikov, ki so potrebni za delovanje navideznih namizij.

Prihranek električne energije = *(poraba fizičnega računalnika x število računalnikov x število delovnih dni v letu x število ur delovanja na dan x cena kilovatne ure) – ((poraba strežnikov x število strežnikov x število dni v letu x število ur delovanja na dan x cena kilovatne ure) + (poraba tankega odjemalca x število tankih odjemalcev x število delovnih dni v letu x število ur delovanja na dan x cena kilovatne ure))*

V našem primeru smo vzeli povprečno ceno kilovatne ure 0,1 evra.

Ravno tako lahko izrazimo prihranek pri posodobitvah in racionalizaciji administracije, da primerjamo razliko stroškov administriranja fizičnih računalnikov in navideznih namizij ter strežnikov.

Stroški administracije = *število incidentov na dan x čas, potreben za popravilo x urna postavka administratorja x delovni dnevi v letu*

V našem primeru smo vzeli za fizične računalnike pet incidentov na dan, za čas popravila 1 uro, za urno postavko administratorja 10 evrov in 250 delovnih dni.

Pri virtualnih namizjih pa smo na podlagi prakse drugih podjetij in javnih ustanov vzeli en incident na dan, eno uro za popravilo, 10 evrov za urno postavko in 250 delovnih dni.

Tabela 6: **Neto sedanja vrednost ob vpeljavi projekta VDI**

Neto sedanja vrednost	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**	**Skupaj**
Koristi	–	8.630,40 €	8.630,40 €	8.630,40 €	8.630,40 €	8.630,40 €	43.152,00 €
Stroški	45.200,00 €	2.869,60 €	2.869,60 €	2.869,60 €	2.869,60 €	2.869,60 €	59.548,00 €
Sedanja vrednost stroškov	45.200,00 €	5.018,32 €	4.690,02 €	4.383,19 €	4.096,44 €	3.828,45 €	67.216,42 €
Sedanja vrednost koristi		17.411,59 €	16.272,51 €	15.207,96 €	14.213,04 €	13.283,22 €	76.388,32 €
Preostala sedanja vrednost		1.200,00 €	– €	– €	– €	– €	1.200,00 €
Neto sedanja vrednost	– 45.200,00 €	13.593,27 €	11.582,50 €	10.824,76 €	10.116,60 €	9.454,77 €	10.371,90 €
Neto koristi	– 45.200,00 €	– 31.606,73 €	– 20.024,23 €	– 9.199,47 €	917,13 €	10.371,90 €	

5.13 Metode presojanja

Neto sedanja vrednost (NSV) projekta prikaže razliko med diskontirano sedanjo vrednostjo prihodnjih koristi (SVK) in diskontirano sedanjo vrednostjo prihodnjih stroškov (SVS).

$$NSV = SVK - SVS$$

Pozitivna neto sedanja vrednost govori v prid sprejetju projekta, saj koristi presegajo stroške. Med več projekti bo izbran tisti z najvišjo neto sedanjo vrednostjo (Campbell in Brown, 2003).

Neto sedanja vrednost našega projekta znaša 10.371,90 evra.

Indeks donosnosti (razmerje stroškov in koristi)

Indeks donosnosti spada med kazalnike neto sedanje vrednosti in je pravzaprav drugačen način primerjanja sedanje vrednosti koristi ter sedanje vrednosti stroškov. Pri neto sedanji vrednosti smo v izračunu upoštevali neto koristi (koristi minus stroški) in jih diskontirali na sedanjo vrednost. Ta kaže razmerje med koristmi in stroški projekta, zato jih moramo izraziti ločeno, kar lahko ponazorimo z izrazom:

$$ID = SVK/SVS$$

Indeks donosnosti našega projekta znaša 1,13645.

ID = 76.388,32/67.216,42 = 1,13645

Relativna neto sedanja vrednost (RNSV) je razmerje med neto sedanjo vrednostjo (NSV) denarnega toka v celotnem časovnem obsegu in sedanjo vrednostjo investicijskih stroškov (SVI).

Kazalnik izraža akumuliran neto donos, ki ga ustvari enota investiranega kapitala (Senjur, 2002).

Izračunamo ga po enačbi:

$$RNSV = NSV/SVI$$

V našem primeru je relativna neto sedanja vrednost enaka 0,22947 (10.371,90/45.200 = 0,22947).

6 SKLEP

Ali se bomo odločili za navidezno namizje, je odvisno od potreb in zahtev, ki jih imamo v podjetju. Za nekatera dela so vseeno primernejši klasični namizni računalniki. Pri odločitvi je pomembno, ali želimo zmanjšati stroške delovanja ali stroške investicije.

Kot smo ugotovili na podlagi analize in izračuna, se pri implementaciji virtualnega namizja predvsem zvišajo začetni stroški investicije, kasneje pa z delovanjem in upravljanjem virtualnih namizij prihranimo v primerjavi s klasičnimi računalniki. Prihranek pri stroških delovanja ob upoštevanju posodobitev programske opreme, porabi električne energije in poenostavljeni administraciji se pokaže šele po štirih letih.

Pomembno je, ali želimo upravljati vse z enega mesta, obenem pa smo pripravljeni investirati v nova znanja in izobraževanje administratorjev in jih usposobiti za delo z virtualnimi namizji in njihovim upravljanjem ter vzdrževanjem. Vse to prinaša neotipljive koristi, ki jih lahko delimo na dva dela (Hares in Royle,1994). Prvi je interno izboljšanje infrastrukture, drugi pa je povezava z uporabniki. Prav drugi se navezuje predvsem na servisiranje uporabnikov in na njihovo zadovoljstvo.

Vrednotenje neotipljivih faktorjev zahteva podrobno preučitev posameznih postavk z uporabo različnih metod, te pa časovno podaljšajo analizo in zvišujejo stroške raziskave.

Odločitev za prehod na virtualna namizja s tankimi odjemalci je odvisna predvsem od usmerjenosti podjetja in od želje po fleksibilnosti in skalabilnosti. Podjetja, ki so dinamična in se njihove potrebe po virih spreminjajo hitro ter so se sposobna hitro prilagajati zahtevnim razmeram na trgu, bodo znala upravičiti višje začetne nabavne stroške in izkoristiti možnosti, ki jih prinaša virtualizacija namizij.

7 LITERATURA IN VIRI

[1] Bevec, M. (2010). Sprememba zunanjega izvajanja IT storitev zaradi uporabe virtualizacije. Koper: Actual I.T., d. d.

[2] Brumec, S. (2011). Računalni oblaci kao dio servisno orijentirane arhitekture. Varaždin: Svečilište u Zagrebu, Fakultet organizacije i informatike.

[3] Bruzzese, J. P. (2010). Desktop virtualization clients: Fat, thin, or zero?, InfoWorld.com. Dosegljivo na http://www.infoworld.com/d/windows/desktop-virtualization-clients-fat-thin-or-zero-638 (9. 9. 2011).

[4] Campbell, H., Brown, R. (2003). Benefit – cost analysis.The University of Queensland: Cambridge University Press.

[5] Čuk, R. & Harej, J. (2011). Virtualizacija strojne opreme. Vzdrževanje sistemske programske opreme. Ljubljana: Zavod IRC.

[6] Fegreus, J. (2010). Leverage Scale-out SAN Storage to Hone ROI for Virtual Desktop Infrastructure, open Bench Labs.

[7] Gartner (2010). Inc, Get Ready for Hosted Virtual Desktops. Dosegljivo na http://www.gartner.com/id=1386535 (22. 4. 2012).

[8] Glavač, Z. (2009). Računalništvo v oblaku in virtualizacija. Diplomsko delo. Maribor: Univerza v Mariboru, Fakulteta za elektrotehniko, računalništvo in informatiko.

[9] Hares, J. & Royle, D. (1994). Measuring the value of information technology. Chichester, Wiley.
[10] Housing, cenik tečajev. Dosegljivo na http://www.housing.si/sl/VMware_vSphere_5_Whats_new_V5_1/ (27. 8. 2012).
[11] Kroeker, L. K. (2009). The evolution of virtualization, Communicationsofthe ACM – Being Human in the Digital Age, Volume 52, Issue 3.
[12] Petrović, T., Fertalj, K. (2009). Demistifying desktop virtualization, Proceedings of the 9th WSEAS International Conference on applied computer science, ISSN: 1790-5109, ISBN: 978-960-474-127-4.
[13] Senjur, M. (2002). Razvojna ekonomika. Ljubljana: Ekonomska fakulteta.
[14] Turk, T. (2005). Analiza stroškov in koristi naložb v informatiko. Uporabna informatika, 3: 153–169.
[15] Uredba o enotni metodologiji za pripravo in obravnavo investicijske dokumentacije na področju javnih financ. Uradni list RS, št. 60/2006 z dne 9. 6. 2006, str. 6559. Dosegljivo na http://www.uradni-list.si/1/objava.jsp?urlid=200660&stevilka=2549, (17. 7. 2012).
[16] VMware (2006). Inc, The Role of Memory in VMware ESX Server 3. Dosegljivo na http://www.vmware.com/pdf/esx3_memory.pdf (24. 7. 2012).
[17] VMware, (2011). Inc, VMware VDI Solution. Dosegljivo na http://vipl.co.nz/index.php/virtualisation/vmware-vdi-solution (1. 9. 2011).

▪

Miha Potočnik je leta 2007 diplomiral na Fakulteti za organizacijske vede v Kranju, smer Analiza in načrtovanje informacijskih sistemov. Na isti fakulteti končuje podiplomski študij znanstvenega magisterija Organizacija in management informacijskih sistemov. Zaposlen je na občini Jesenice, kjer skrbi za administracijo informacijskega sistema, podatkovne baze in podporo uporabnikom.

▪

Mirko Gradišar je zaposlen na Ekonomski fakulteti Univerze v Ljubljani kot redni profesor za področje poslovne informatike. Raziskovalno se ukvarja predvsem z razvojem informacijskih sistemov in zahtevnejših algoritmov na področju operacijskih raziskav. Kot vodja ali sodelavec je sodeloval pri številnih domačih in mednarodnih znanstvenih in strokovnih projektih. Glavna tri področja, na katerih pedagoško deluje, so razvoj in uvajanje informacijskih sistemov, elektronsko poslovanje in menedžment informatike. Je avtor več univerzitetnih učbenikov, znanstvenih monografij in več kot šestdesetih znanstvenih člankov.

Iz Islovarja

Islovar odlikujejo odprtost, ažurnost, kakovost. Spletni računalniški program je tako kot vse računalniške programe mogoče spreminjati in prilagajati, hkrati pa ga je treba tudi vzdrževati, sproti odpravljati napake v njem. Brez stalnega vzdrževanja računalniškega programa in slovarske vsebine spletni slovar kaj kmalu zastari. Islovar je odprt za prispevke uporabnikov, njegova prednost pa je v tem, da ga uredniki sproti pregledujejo, posodabljajo in popravljajo. Tudi sestavke, ki so bili pred časom že urejeni, slovaropisna skupina ponovno pretrese in če se ne ujemajo s sorodnimi izrazi ali so zastareli, spremeni izraze ali njihovo razlago.

Zbirko, ki jo predstavljamo tokrat, smo zbrali pod naslovom »namestitev«, vendar smo vanjo vključili tudi številne starejše izraze, ki smo jih ponovno prevetrili. Vabimo vas, da v Islovar *www.islovar.org* prispevate svoje pripombe ali predloge.

izvédba -e ž *(angl. implementation)*
ena od faz razvoja informacijskega sistema, ki zajema uresničitev podrobnega načrta računalniškega programa ali informacijskega sistema, namestitev uporabniškega programa, prenos podatkov, usposobitev uporabnikov; prim. uvedba, uvajanje

izvêsti -vêdem dov. *(angl. implement)*
uresničiti podrobni načrt računalniškega programa ali informacijskega sistema, z namestitvijo uporabniškega programa, prenosom podatkov, usposobitvijo uporabnikov; prim. postaviti

konfigurírati -am dov., nedov. *(angl. configure)*
sestaviti naprave in/ali programe v delujoč računalniški sistem; prim. prilagoditi (2)

nadzórna plôšča -e -e ž *(angl. control panel)*
del grafičnega uporabniškega vmesnika, s katerim uporabnik pregleduje in spreminja osnovne nastavitve sistema, programa

nastavítev -tve ž *(angl. setup, setting)*
1. vrednost, ki je bila določena med optimiranjem delovanja računalniškega programa, sistema, naprave
2. določitev parametrov, pomembnih za delovanje računalniškega programa, sistema, naprave

nastavítev gêsla -tve -- ž *(angl. password setup)*
izbor, določitev in vsako nadaljnje spreminjanje gesla

nastavítvena pakétna datotéka -e -e -e ž *(angl. configuration batch file)*
paketna datoteka za spreminjanje nastavitev računalniškega programa, sistema, naprave

nastavítveni pripomóček -ega -čka m *(angl. configuration utility)*
program za zapis nastavitev (2) računalniškega programa v konfiguracijsko datoteko; sin. konfiguracijski pripomoček

nastavítveno ôkno -ega -a s *(angl. configuration dialog box)*
pogovorno okno za spreminjanje nastavitev

odkleníti -em dov. *(angl. unlock)*
narediti napravo, program tako, da je ponovno dostopna in odzivna; prim. zakleniti

odklèp -épa m *(angl. unlock)*
postopek, ki omogoči, da je naprava dostopna, da deluje; prim. zaklep

odklépanje -a s *(angl. unlock)*
omogočanje uporabe, dostopa do naprave, programa, ki je bila prej zaklenjena; prim. zaklepanje

osébna nastavítev -e -tve ž *(angl. personalization)*
nastavitev programa glede na osebne potrebe ali želje posameznika; sin. personalizacija, osebna prilagoditev

osébna prilagodítev -e -tve ž *(angl. personalization)*
nastavitev programa glede na osebne potrebe ali želje posameznika; sin. osebna nastavitev, personalizacija

personalizácija -e ž *(angl. personalization)*
gl. osebna nastavitev in osebna prilagoditev

ponôvno namestíti -- -ím dov. *(angl. reinstall)*
ponoviti namestitev programa, dela programa, zaradi vzpostavitve pravilnega delovanja

postavítev -tve ž *(angl. deployment)*
izdaja, namestitev in prilagoditev programske rešitve za delovanje v produkcijskem okolju; prim. uvedba, uvajanje

postáviti -im dov. *(angl. deploy)*
izdati, namestiti in prilagoditi programsko rešitev tako, da deluje v produkcijskem okolju; prim. izvesti

povozíti -im dov. *(angl. override)*
začasno neupoštevati eno ali več obstoječih nastavitev

prédnostna nastavítev -e -tve ž *(angl. preference settings, preferences)*
nabor najpogosteje uporabljenih nastavitev (1)

prilagodítev -tve ž *(angl. customization)*
1. sprememba nastavitve (2) glede na potrebe in želje uporabnika
2. sprememba ali izdelava računalniškega programa glede na zahteve uporabnika

prilagodíti -im dov. *(angl. customize)*
1. spremeniti nastavitev (2) glede na potrebe in želje uporabnika
2. spremeniti ali izdelati računalniški program glede na zahteve uporabnika; prim. konfigurirati

prilagojèni -ênа -o prid. *(angl. customized, custom)*
narejen, spremenjen po meri uporabnika

privzéta nastavítev -e -tve ž *(angl. default setting)*
nastavitev, pri kateri je vrednost parametra vnaprej nastavljena

privzét -a -o prid. *(angl. default)*
ki se nanaša na programsko nastavljeno vrednost

uvájanje -a s *(angl. implementation)*
postavitev programske rešitve, prenos podatkov in usposobitev uporabnikov pri vpeljavi informacijskega sistema v prakso; sin. uvedba; prim. izvedba, postavitev

uvédba -e ž *(angl. implementation)*
postavitev programske rešitve, prenos podatkov in usposobitev uporabnikov pri vpeljavi informacijskega sistema v prakso; sin. uvajanje; prim. izvedba, postavitev

zakleníti zaklénem dov. *(angl. lock)*
narediti napravo, program tako, da ni dostopna ali da se ne odziva; prim. odkleniti

zaklép -épa m *(angl. lock)*
postopek, ki povzroča, da naprava ni dostopna, da ne deluje; prim. odklep

zaklépanje -a m *(angl. lock)*
onemogočanje uporabe, dostopa do naprave, programa, npr. zaklepanje tipkovnice; prim. odklepanje

zapóra tipkóvnice -e -e ž *(angl. keyboard lock)*
fizična prepreka za uporabo tipkovnice

Izbor pripravlja in ureja
Katarina Puc s sodelavci Islovarja.

Koledar prireditev

Conferences & Seminars APF'2012 – Annual Privacy Forum	10.–11. oktober 2012	Lemesos (Limassol), Ciper	www.privacyforum.eu
Mednarodna konferenca Nova evropska perspektiva: pomen e-znanj za vključenost in zaposlovanje	15. oktober 2012	Ljubljana, Slovenija	http://simbioza.eu/about/konferenca.html
3rd Worldwide Cybersecurity Summit: The Next Billion Netizens Safely Connect	30.–31. oktober 2012	New Delhi, Indija	http://cybersummit2012.com
2nd European Cybercrime Expert Forum Fighting Cybercrime: How Best to Cope with Current Cyber Threats	8.–9. november 2012	Berlin, Nemčija	http://www.euroacad.eu
The 4th Annual Internet of Things Europe Shaping Europe's Future Internet Policy – The road to Horizon 2020	12.–13. november 2012	Bruselj, Belgija	www.IoTConference.eu
The 3rd Annual European Data Protection and Privacy Conference	4. december 2012	Bruselj, Belgija	www.dataprotection2012.eu

Pomembni spletni naslovi

→ IFIP News: **http://www.ifip.org/images/stories/ifip/public/Newsletter/news ali www.ifip.org → Newsletter**

→ IT Star Newsletter: **www.itstar.eu**

→ ECDL: **www.ecdl.com**

→ CEPIS: **www.cepis.com**

Dostop do dveh tujih strokovnih revij

→ Revija **Upgrade** (CEPIS) v angleščini (ISSN 1684-5285) je dostopna na spletnem naslovu: **http://www.upgrade-cepis.org/issues/2008/4/upgrade-vol-IX-4.html**.

→ Revija **Novática** (CEPIS) v španščini (ISSN 0211-2124) je dostopna na spletnem naslovu: **http://www.ati.es/novatica/**.

Najava konference

DNEVI SLOVENSKE INFORMATIKE 2013

Spoštovani,

obveščamo vas, da bo **od 15. do 17. aprila 2013** v Kongresnem centru Grand hotela Bernardin v Portorožu potekala že 20. konferenca

Dnevi slovenske informatike.

Prireditelj konference je Slovensko društvo Informatika.

Vabimo vas k **oddaji prispevkov** za konferenco.
Več informacij o konferenci (in oddaji prispevkov)
bo v kratkem na voljo na spletni strani www.dsi2013.si.

Slovensko društvo Informatika

Včlanite se v Slovensko društvo INFORMATIKA

Pristopna izjava

za članstvo v Slovenskem društvu INFORMATIKA

Pravne osebe izpolnijo samo drugi del razpredelnice

Ime in priimek	
Datum rojstva	
Stopnja izobrazbe	srednja, višja, visoka
Naziv	prof., doc., spec., mag., dr.
Domači naslov	
Poštna št. in kraj	
Ulica in hišna številka	
Telefon (stacionarni/mobilni)	

Zaposlitev člana oz. člana - pravna oseba	
Podjetje, organizacija	
Kontaktna oseba	
Davčna številka	
Poštna št. in kraj	
Ulica in hišna številka**	
Telefon	
Faks	
E-pošta	

Zanimajo me naslednja področja/sekcije*

- ☐ jezik
- ☐ informacijski sistemi
- ☐ operacijske raziskave
- ☐ seniorji
- ☐ zgodovina informatike
- ☐ poslovna informatika
- ☐ poslovne storitve
- ☐ informacijske storitve
- ☐ komunikacije in omrežja
- ☐ softver
- ☐ hardver
- ☐ upravna informatika
- ☐ geoinformatika
- ☐ izobraževanje

podpis _____ kraj, datum _____

Pošto društva želim prejemati na domači naslov / v službo.

Članarina znaša: 18,00 € - redna
7,20 € - za dodiplomske študente in seniorje (ob predložitvi dokazila o statusu)
120,00 € - za pravne osebe

Članarino, ki vključuje glasilo društva – revijo **Uporabna informatika**, bom poravnal sam / jo bo poravnal delodajalec.

DDV je vključen v članarino.

Naročilnica na revijo UPORABNA INFORMATIKA

Naročnina znaša: 35,00 € za fizične osebe
85,00 € za pravne osebe – prvi izvod
60,00 € za pravne osebe – vsak naslednji izvod
15,00 € za študente in seniorje (ob predložitvi dokazila o statusu)

DDV je vključen v naročnino.

_____
ime in priimek ali naziv pravne osebe in ime kontaktne osebe

_____
davčna številka, transakcijski račun

_____
naslov plačnika

_____
naslov, na katerega želite prejemati revijo (če je drugačen od naslova plačnika)

telefon/telefaks _____ elektronska pošta _____

Podpis _____ Datum _____

Znanstveni prispevki

Strokovni prispevki

Informacije

ISSN 1318-1882
9 771318 188001