Analiza varnostne ogroženosti

Matjaž Jaušovec, Boštjan Brumen, Tatjana Welzer - Družovec
Fakulteta za elektrotehniko, računalništvo in informatiko Univerze v Mariboru
Matjaz_Jausovec@hotmail.com

Izvleček

Podjetja, ki pri svojem poslovanju ne uporablja računalniškega sistema, si ne moremo več predstavljati. Med uporabo računalniškega sistema lahko pride do neželenega izpada ali nepravilnega delovanja strojne ali programske opreme, večkrat tudi zaradi nepravilne uporabe. Podjetja zaradi tega izgubljajo denar, stranke, naročila in ugled. Zato je smiselno, da izračunajo stroške neželenih dogodkov in da z določenimi tehnikami preprečijo take dogodke.

V prvem delu članka predstavljamo tehniko analize ogroženosti, s katero lahko ugotovimo in zmanjšamo ranljivost računalniškega sistema. V drugem delu članka pa predstavljamo analizo ogroženosti v enem izmed slovenskih podjetij.

Abstract

Analysis of Security Risk

It is beyond our comprehension to imagine a company operating without the use of the information technology. However, the use of computer system involves unforeseen events, such as irregular operation of the hardware and software equipment, mostly as the consequence of inappropriate handling. In such cases a company loses its money, clients, placed orders, its reputation, to mention just a few. Therefore it is highly recommended to estimate the consequences. In such a way a company adopts a technique by which the occurence of the unforeseen events is prevented.

The first part of the article describes a technique called »Analysis Of Security Risk«, which helps to establish and decrease the sensitivity factor of computer system. The second part of the article presents the actual analysis of the security risks, carried out in one of the Slovene companies.

1 Analiza ogroženosti

Načrtovanje varnosti računalniških sistemov se začne z analizo ogroženosti. To je postopek, s katerim določimo izpostavljenost računalniškega sistema in izgubo denarja, ki jo lahko povzroči neželeni dogodek. Prvi korak analize je določitev in opis vseh oblik izpostavljenosti računalniškega sistema, ki se kažejo kot izpad ali nepravilno delovanje strojne ali programske opreme, kar je večkrat tudi posledica nepravilne uporabe, nato pa za vsako od njih določitev ravnanja, ki ga je treba tudi ovrednotiti. Pri tem je vsekakor pomembno tudi dejstvo, da imajo prednost tiste rešitve, ki prinašajo največ koristi (primerjava stroškov in koristi za vse rešitve). Zadnja stopnja analize je torej analiza stroškov in koristi (angl. cost-benefit), ki nam pove, ali se srečamo z nižjimi stroški, če ukrepamo, ali pa je morda ceneje sprejeti pričakovano izgubo. [1]

Ustrezno ravnanje lahko zmanjšajo ogroženost in posredno izgubo. Smiselno je na primer shraniti pomembnejše podatke z diskov, da zaradi okvare ne ostanemo povsem brez njih [3]. Osebno shranjevanje podatkov v večjih podjetjih ni najprimernejše, treba je uvesti ukrepe, ki bi ta problem rešili na ravni podjetja. Z analizo ogroženosti na primer lahko odgovorimo na vprašanje, ali so stroški ob izgubi podatkovnih vsebin zaradi okvare diska večji od stroškov, namenjenih za ukrepe, ki bi to izpostavljenost reševali drugače.

V nadaljevanju predstavljamo razloge za analizo ogroženosti in korake te analize.

1.1 Razlogi za analizo ogroženosti

Nekateri razlogi za analizo ogroženosti so:

1. *Pozornost.* Seznanitev uporabnikov s pomembnostjo varnosti lahko poveča zanimanje in odgovornost zaposlenih.
2. *Ugotavljanje prednosti, pomanjkljivosti in ukrepanja.* Veliko podjetij se ne zaveda svojih prednosti in pomanjkljivosti. S sistematično analizo pridobimo razumljivo predstavo [5].
3. *Dvig osnove za odločanje.* Ukrepi preprečujejo ustvarjalnost uporabnikov, večkrat neupravičeno. Velikokrat pa zaradi pomanjkanja ukrepov zaznamo večjo ustvarjalnost, ki lahko poveča stopnjo tveganja. Da bi izbrali primerne ukrepe, moramo zelo dobro poznati ali oceniti stopnjo tveganja.
4. *Upravičenost izdatkov za varnost.* Nekateri varnostni ukrepi so zelo dragi in nimajo posebne prednosti. Prikazati moramo, koliko stane ukrep in za koliko se zmanjša tveganje, če ukrepamo.

1.2 Koraki opravljanja analize ogroženosti

Proces analize ogroženosti je prevzet iz upravljanja (angl. management). Vsebine, ki jih obravnavamo, se nanašajo na računalniški sistem. Temeljni koraki analize ogroženosti so [1]:

1. Ugotavljanje sredstev (angl. assets).
2. Določitev možne ranljivosti sredstev.
3. Ocena verjetnosti izrabe (angl. exploitation) sredstev. Ocenimo verjetnost nastopa situacij, v katerih je sredstvo ranljivo.
4. Izračun pričakovane letne škode.
5. Pregled primernih ukrepov za preprečevanje nastajanja škode in stroškov uporabe.
6. Načrtovanje letnega prihranka ob uveljavitvi novih ukrepov.

1.2.1 Ugotavljanje sredstev

Prvi korak analize ogroženosti je popis sredstev. Sredstva lahko razdelimo v kategorije. Prve tri so povsem računalniške, preostale tri pa niso nujno del računalniškega sistema, vendar so pogoj za primerno delovanje [2].

1. *Strojna oprema*: računalniki, monitorji, terminali, delovne postaje, tračne enote, tiskalniki, diski, kabli, povezave, komunikacijski vmesniki.
2. *Programska oprema*: izvorna koda, objektni programi, kupljeni programi, programi v hiši, aplikacijski programi, operacijski sistemi, sistemski programi (prevajalniki) in vzdrževalno-diagnostični programi.
3. *Podatki*: podatki, ki jih uporabljajo programi, podatki, shranjeni na magnetnih nosilcih, arhivirani podatki, tiskani podatki in poročila o osveževanju podatkov.
4. *Zaposleni*: potrebni za delovanje računalniškega sistema ali programov.
5. *Dokumentacija*: za programske in strojno ter administrativno proceduro.
6. *Dobava pisarniškega materiala*: papir, kartuše, nosilci za shranjevanje podatkov.

Z izdelavo takega seznama smo pravzaprav opravili inventuro informacijskih sredstev.

1.2.2 Določitev ranljivosti sredstev

Ugotavljanje sredstev je preprost postopek, ker so sredstva večinoma opredmetena. Ugotavljanje ranljivosti sredstev zahteva veliko več predvidevanj, če hočemo ugotoviti, kolikšno škodo lahko utrpijo sredstva in kateri vir jo povzroči.

Trije temeljni cilji varnega računalniškega sistema so:

- tajnost, zaupnost (angl. secrecy),
- popolnost, neokrnjenost, celovitost, povezljivost (angl. integrity),
- razpoložljivost (angl. availability).

Ranljivost je vsaka situacija, ki lahko povzroči izgubo katerekoli od teh treh lastnosti.

Smiselno je narediti primerjavo med sredstvom in njegovo ranljivostjo. Ta primerjava je razvidna iz naslednje tabele:

Sredstva	Tajnost/ zaupnost	Popolnost/ neokrnjenost/ celovitost/ povezljivost	Razpoložljivost
Strojna oprema			
Programska oprema			
Podatki			
Zaposleni			
Dokumentacija			
Dobava pisarniškega materiala			

Za vsako kombinacijo sredstva in njegove ranljivosti moramo ugotoviti, kaj neželenega se lahko zgodi. Pomagamo si lahko z naslednjimi vprašanji:

- Kakšne so posledice nenamernih napak?
- Kakšne posledice lahko povzročijo namerno narejene napake zaposlenih?
- Kako na sistem vplivajo zunanji dejavniki?
- Kakšne so posledice naravnih nesreč in fizičnih okvar?

1.2.3 Ocena verjetnosti izrabe sredstev

V tem koraku analize ogroženosti podajamo svoja pričakovanja o pogostosti pojava neželenega stanja. Upoštevamo naslednje:

- Verjetnost dogodkov pri splošni populaciji. Največ teh podatkov imajo zavarovalnice.
- Verjetnost dogodkov, ki se nanašajo na opazovanje posameznega sistema.
- Ocenitev števila dogodkov v določenem času.
- Ocenitev verjetnosti iz tabele (navedeni sta pogostost pojavljanja in ocena).
- Delfi raziskava. Med strokovnjaki obravnavanega področja poskušamo ugotoviti splošno mnenje.

1.2.4 Izračun pričakovane letne škode

Določiti moramo pričakovane stroške vseh neželenih dogodkov. Stroške menjave strojne opreme določimo hitro, medtem ko je težje določiti stroške menjave dela programa. Stroške drugih področij večinoma lahko ocenimo na podlagi izkušenj.

Pravna pravila določajo, katere podatke je treba zaščititi zaradi tajnosti oziroma zaupnosti poslovanja podjetja. Stroške, ki bi nastali ob nedovoljeni objavi takih podatkov, je težko določiti.

Neprijetne posledice lahko nastanejo, če računalniški sistem ali programska oprema ne deluje ali če manjka ključna oseba.

Višino stroškov lahko določimo z naslednjimi vprašanji:

- Kakšne so pravne obveznosti do popolnosti, celovitosti, povezljivosti in tajnosti oziroma zaupnosti podatkov?
- Ali bi objava podatkov povzročila škodo posamezniko m ali podjetjem? So pravne posledice predvidljive?
- Ali lahko nedovoljen dostop do podatkov povzroči izgubo poslovnih priložnosti? Ima konkurent zaradi tega prednost? Kakšna je izguba pri prodaji?
- Kakšen je psihološki učinek na delovanje računalniškega sistema? Lahko povzroči zadrego, izgubo verodostojnost in posla? Koliko strank bo oškodovanih? Kakšna vrednost je povezana s temi strankami?
- Koliko nam pomeni dostop do podatkov? Lahko obdelavo podatkov (angl. computation) preložimo za časovno predvidljivo obdobje? Jo lahko opravimo kje drugje? Koliko bi to stalo?
- Kakšno vrednost vidi konkurent v naših podatkih? Koliko sredstev je pripravljen vložiti, da pridobi te podatke?
- Kakšne težave povzroči izguba podatkov? Lahko podatke nadomestimo ali obnovimo in koliko dela moramo v to vložiti?

Tovrstne stroške je težko oceniti. Ogroženost računalniškega sistema je večinoma veliko večja, kot jo pričakuje vodstvo.

Vrednost neželenega dogodka določimo na opisani način. Pomnožimo jo s pričakovanim številom ponovitev dogodka v enem letu. Tako ovrednotimo pričakovane letne stroške (angl. annual loss expectancy).

1.2.5 Pregled primernih ukrepov za preprečevanje nastajanja škode in stroškov uporabe

Za trenutno znane in veljavne ukrepe za preprečevanje nastajanja škode poznamo pričakovane stroške. Če so stroški nesprejemljivo visoki, moramo poiskati nove ukrepe, s katerimi jih bomo znižali.

Eden izmed načinov identifikacije dodatnih ukrepov temelji na izpostavljenosti. Pred izgubo podatkov se lahko zavarujemo z varnostnimi kopijami, s podvajanjem, z nadzorom dostopa, ki preprečuje brisanje, s fizično zaščito, ki preprečuje krajo diska, ali s programi, ki preprečujejo dostop do podatkov. [3]

Drugi načini se nanašajo na pregled poznanih ukrepov za preprečevanje nastajanja škode [1]:

- vtajnopisje (angl. cryptographic controls),
- varni protokoli,
- nadzor pri razvoju programov,
- nadzor okolja pri izvajanju programov,
- uporaba varnostnih ukrepov operacijskega sistema,
- identifikacija,
- verodostojnost,
- načrtovanje in razvoj varnega operacijskega sistema,
- nadzor dostopa do baze podatkov [3],
- zanesljivost dostopa do baze podatkov,
- uporaba večplastnih varnostnih ukrepov za podatke, podatkovne baze in operacijske sisteme,
- varnost osebnih računalnikov,
- varnostni ukrepi za dostop in uporabo računalniške mreže,
- varnost fizičnih dostopov.

Poznavanje mehanizmov in primernost za uporabo sta ob določeni nevarnosti temeljna pogoja za pravilno izbiro oziroma odločanje o uporabi. S tem zmanjšamo tudi stroške odločanja in druge stroške, ki bi lahko nastali v povezavi z omenjenim področjem.

1.2.6 Načrtovanje letnega prihranka ob uveljavitvi novih mehanizmov upravljanja

Naslednji korak v procesu opravljanja analize ogroženosti je izračun, ali smo z novimi ukrepi za preprečevanje nastajanja škode in njihovimi stroški v boljšem položaju kot v sedanjem stanju. Po izračunu pridemo do enega izmed treh odgovorov:

1. Novi mehanizmi upravljanja povečajo varnost, vendar so stroški višji kot izguba neželenega dogodka.
2. Novi mehanizmi upravljanja povečajo varnost, stroški pa so manjši, kot izguba zaradi neželenega dogodka.
3. Novi mehanizmi upravljanja ne povečajo varnosti.

2 Analiza ogroženosti v enem izmed slovenskih podjetij

Podjetje, ki smo ga analizirali, je eno iz skupine sorodnih podjetij na slovenskem področju. Omenjena skupina je ustanovila hčerinsko podjetje, ki opravlja del informacijskih storitev (pretežno prek integriranega informacijskega sistema), drugi del informacijskih storitev, ki so povezana s posebnostmi poslovanja teh podjetij, pa podjetja opravljajo sama.

Analizirano podjetje ima upravo in devet poslovnih enot na področjih, ki jih podjetje pokriva s svojim poslovanjem. Analizo ogroženosti smo opravili s stališča službe za informatiko.

Ker bi iz nadaljevanja lahko razbrali, za katero podjetje gre, smo navedene številske vrednosti prilagodili. Navajanje dejanskih vrednosti bi namreč pomenilo izdajanje poslovne skrivnosti podjetja.

V nadaljevanju podrobneje opisujemo naslednje korake:

1. Ugotavljanje sredstev.
2. Določitev ogroženosti sredstev.
3. Ocena verjetnosti izrabe sredstev.
4. Izračun pričakovane letne škode.
5. Pregled primernih ukrepov za preprečevanje nastajanja škode in stroškov uporabe.
6. Načrtovanje letnega prihranka ob uveljavitvi novih ukrepov.

2.1 Ugotavljanje sredstev

Prvi korak pri izvajanju analize ogroženosti je popis sredstev.

1. Strojna oprema:

Oprema	Število
TERMINAL	14
MONITOR	414
RAČUNALNIK	448
OPTIČNI BRALNIK	22
TISKALNIK	222
ROUTER	13
PREKLOPNIK	11
MODEM	3
STREŽNIK	11

Pri računalnikih in monitorjih prihaja do večje razlike, ker so k računalnikom prišteti tudi tanki odjemalci [2].

2. Programska oprema

Programska oprema	Število
WINDOWS 95	130
WINDOWS 98	190
WINDOWS NT	17
WINDOWS 2000	25
OFFICE 97 (Word, Excel, Access, Outlook)	350
PERSONAL COMMUNICATION	350
DB/2	110
FOREST&TREES	110
VISIO TECHNICAL	35
NORTON (protivirusni program)	350
ON DEMAND	65
AUTOCAD	18
ARCVIEW	2
MS PROJECT	3
LOTUS NOTES	150
APPS – pošiljanje in spremljanje transakcij na APP (Agencija za plačilni promet)	1
Elmark – trgovanje	10

3. Podatki

Za podatke po pogodbi o opravljanju storitev skrbi drugo podjetje. Obravnavamo jih zato, ker bi odtujitev podatkov povzročila velike finančne posledice. Mislimo na vrednost informacije, ki se skriva za podatki.

4. Zaposleni

Za nemoteno delovanje računalniškega sistema skrbi služba za informatiko. V njej je zaposlenih sedem ljudi. Stopnja izobrazbe uporabnikov informacijskih storitev v podjetju (tj. zaposlenih) je taka:

Izobrazba	Število uporabnikov
POLKVALIFICIRAN	6
KVALIFICIRAN	20
SREDNJA IZOBRAZBA	162
VIŠJA IZOBRAZBA	103
VISOKA in več	72

5. Dokumentacija

Dokumentacijo strojne in programske opreme hrani služba za informatiko. Dokumentacija IIS (Integrirani IS) je v domeni drugega podjetja.

6. Dobava pisarniškega materiala

Dobavitelja pisarniškega materiala v podjetju izbirajo enkrat na leto na podlagi javnega razpisa. Predstavnik službe za informatiko sodeluje ob pripravi razpisne dokumentacije. Izkušnje kažejo, da je dobavitelj pripravljen upoštevati morebitne spremembe in želje naročnika, saj se zaveda, da se izbor oz. javni razpis ponavlja vsako leto.

2.2 Določitev ranljivosti sredstev

Glej tabelo 1.

2.3 Ocena verjetnosti izrabe sredstev

Za razumevanje postopka ocene verjetnosti izrabe sredstev je dovolj, da predstavimo tabelo strojne opreme. Druge tabele izdelujemo po podobni shemi. Vsekakor pa za nadaljevanje postopkov potrebujemo še preostale tabele, ki jih ne prikazujemo (programska oprema, podatki, zaposleni, dokumentacija, dobava pisarniškega materiala).

Pri oceni verjetnosti izrabe smo se odločili za naslednje vrednotenje: številka v razpredelnici označuje število ponovitev pojava (frekvenco) v enem letu. Glej tabelo 2.

2.4 Izračun pričakovane letne škode

Kot v prejšnji točki tudi tukaj predstavljamo tabelo strojne opreme. Tabela 3 na naslednji strani.

Podatke o vrednotenju posameznega izrednega dogodka navajamo v tabeli. Številska vrednost v tabeli pomeni vrednost v evrih, ki jo izgubljamo ob enkratnem izrednem dogodku.

Tabela 1

Sredstva	Tajnost / zaupnost	Popolnost/neokrnjenost/ celovitost/povezljivost	Razpoložljivost
Strojna oprema		Preobremenjena/uničena	Nepravilno delovanje/ukradena/okvara/nedostopna
Programska oprema	Ukradena/prekopirana/ zlorabljena	Nepravilno delovanje/ nedovoljeno nadzorovana (angl. trojan)	Izbrisana/ni na pravem mestu/pretek licenc
Podatki	Objava/ dostop nepooblaščenim	Spremenjeni zaradi napake strojne ali programske opreme in uporabnika	Izbrisani/niso na pravem mestu/uničeni
Zaposleni bolniška		Bolniška	Prenehajo z delom/so upokojeni/na dopustu/
Dokumentacija			Izgubljena/ukradena/uničena
Dobava pisarniškega materiala			Izgubimo/ukradeno/uničeno

Tabela 2

Oprema	Preobremenjena	Uničena	Nepravilno deluje	Ukradena	Nedostopna	Število
TERMINAL	3	0,5	2	0,1	5	14
MONITOR	2	0,5	5	0,1	10	414
RAČUNALNIK	100	1	120	0,1	50	448
OPTIČNI BRALNIK	30	0,2	12	0	5	22
TISKALNIK	70	1	60	0,1	120	222
ROUTER	1	0,5	5	0,1	5	13
PREKLOPNIK	10	0,5	30	0,05	20	11
MODEM	5	0,1	2	0,1	4	3
STREŽNIK	10	0,1	20	0,01	20	11

V tabeli 4 je predstavljena dejanska vrednost, ki jo izgubljamo glede na pričakovano število ponovitev izjeme. Dobimo jo tako, da pomnožimo vrednosti iz tabele, ki prikazuje oceno verjetnosti izrabe sredstva, z vrednostmi iz tabele, ki prikazuje vrednotenje posameznega izrednega dogodka.

V tabeli 5 smo zbrali rezultate prikazanih in neprikazanih tabel. Izračun kaže, da pri posamezni vrsti sredstva izgubljamo naslednje zneske:

Iz tabele je razvidno, da je znesek za strojno opremo zelo visok. Ugotovimo, da k temu precej prispeva nepravilno delovanje računalnikov in preklopnikov.

Tabela 5

Strojna oprema	**10.900.519 EUR**
Programska oprema	8.627.000 EUR
Podatki	6.760.000 EUR
Zaposleni	483.000 EUR
Dokumentacija	128.000 EUR
Dobavljeno	3.000 EUR
Skupaj	26.901.519 EUR

Tabela 3

Oprema	**Preobremenjena**	**Uničena**	**Nepravilno deluje**	**Ukradena**	**Nedostopna**
TERMINAL	2.000 EUR	120.000 EUR	5.000 EUR	120 EUR	5.000 EUR
MONITOR	1.000 EUR	70.000 EUR	5.000 EUR	70 EUR	1.000 EUR
RAČUNALNIK	5.000 EUR	210.000 EUR	10.000 EUR	300.000 EUR	10.000 EUR
OPTIČNI BRALNIK	1.000 EUR	60.000 EUR	4.000 EUR	65.000 EUR	2.000 EUR
TISKALNIK	5.000 EUR	70.000 EUR	6.000 EUR	80.000 EUR	3.000 EUR
ROUTER	50.000 EUR	1.500.000 EUR	70.000 EUR	1.700.000 EUR	70.000 EUR
PREKLOPNIK	30.000 EUR	1.000.000 EUR	40.000 EUR	1.050.000 EUR	40.000 EUR
MODEM	20.000 EUR	50.000 EUR	20.000 EUR	70.000 EUR	20.000 EUR
STREŽNIK	40.000 EUR	700.000 EUR	40.000 EUR	1.500.000 EUR	50.000 EUR

Tabela 4

Oprema	**Preobremenjena**	**Uničena**	**Nepravilno deluje**	**Ukradena**	**Nedostopna**
TERMINAL	6.000 EUR	60.000 EUR	10.000 EUR	12 EUR	25.000 EUR
MONITOR	2.000 EUR	35.000 EUR	25.000 EUR	7 EUR	10.000 EUR
RAČUNALNIK	500.000 EUR	210.000 EUR	1.200.000 EUR	30.000 EUR	500.000 EUR
OPTIČNI BRALNIK	30.000 EUR	12.000 EUR	48.000 EUR	0 EUR	10.000 EUR
TISKALNIK	350.000 EUR	70.000 EUR	360.000 EUR	8.000 EUR	360.000 EUR
ROUTER	50.000 EUR	750.000 EUR	350.000 EUR	170.000 EUR	350.000 EUR
PREKLOPNIK	300.000 EUR	500.000 EUR	1.200.000 EUR	52.500 EUR	800.000 EUR
MODEM	100.000 EUR	5.000 EUR	40.000 EUR	7.000 EUR	80.000 EUR
STREŽNIK	400.000 EUR	70.000 EUR	800.000 EUR	15.000 EUR	1.000.000 EUR
Vsota	1.738.000 EUR	1.712.000 EUR	4.033.000 EUR	282.519 EUR	3.135.000 EUR 10.900.519 EUR

2.5 Pregled primernih ukrepov za preprečevanje nastajanja škode in stroškov uporabe

Na dveh stroškovno največjih težavah prikazujemo možnost vpeljave nove kontrole.

1. Nepravilno delovanje računalnikov = 1.200.000 evrov.

Ugotovimo, da je vpisana sorazmerno visoka številka ponavljanja problema 120. Ocenjena vrednost ob nastopu pojava je 10.000 evrov. Zakaj nastajajo težave? Ugotovili smo, da se večkrat pojavljajo problemi v računalnikih, čeprav so ti menjali lokacijo in uporabnika. Poskusi odprave »čudnega delovanja« na servisu niso obrodili sadov.

Predlog: Dogovor z dobaviteljem, da zamenja opremo. Tako bi se v prihodnje zmanjšalo število ponavljanj za polovico.

2. Nepravilno delovanje preklopnikov = 1.200.000 evrov.

Težava se pojavi 30-krat na leto, kar stane pa 40.000 evrov. Do problema prihaja zaradi nejasne odpovedi strojne opreme na prehodu iz mreže token-ring v mrežo ethernet in med povezavo med preklopniki.

Prvi del problema je nastajal zaradi globalnosti sistema, ko strojna oprema ni bila združljiva z drugo strojno opremo na povsem drugem mestu. Problem je mogoče rešiti s podrobnim pregledom nastavitev naprav.

Za drugi del problema je kriva različna verzija biosa enakih naprav, kupljenih v obdobju šestih mesecev. Problem odpravimo s posodobitvijo biosa.

Znesek, ki ga ob nastopu problema izgubljamo, je ocenjen na 40.000 evrov. Ker je posredno prizadetih veliko računalnikov z velikim številom procesov, je znesek temu primerno visok. Ob odpravi napak pričakujemo znižanje števila pojavljanj na 3. Znesek ob enkratnem pojavu neželenega dogodka se ne zmanjša.

2.6 Načrtovanje letnega prihranka ob uveljavitvi novih mehanizmov upravljanja

Izračunajmo zmanjšanje ovrednotenega tveganja ob upoštevanju teh dveh rešitev.

Ovrednotenje rešitve prvega problema: glede na to, da nas dogovor z dobaviteljem (morda zapisan v razpisnih pogojih) ne bo stal nič, je ovrednoteno tveganje 60 ponavljanj x 10.000 evrov = 600.000 evrov. Od prvotnega zneska 1.200.000 evrov odštejemo novi znesek 600.000 evrov in dobimo razliko 600.000 evrov, ki pomeni prihranek.

Rešitev drugega primera nam ovrednoteno pomeni še več. Rešitev nas stane 3 x 40.000 evrov = 120.000 evrov. Brez rešitve 1.200.000 evrov – rešitev 120.000 evrov = prihranek 1.080.000 evrov.

Ugotovimo, da smo z rešitvama dveh težav prihranili 1.680.000 evrov.

Mogoča izguba se je s 26.901.519 evrov zmanjšala na 25.221.519 evrov.

3 Ugotovitve

Ugotavljamo, da je tehnika uporabna in da odgovarja na vprašanje, kje je računalniški sistem glede varnosti najbolj ranljiv.

Med opravljanjem analize ogroženosti smo si zastavili naslednja vprašanja. Analiza pogosto sloni na ocenah. Je rezultat, ki je zmnožek ocen, pravilen? Ugotovili smo, da imamo raje rezultate, ki temeljijo na teoretskih predpostavkah, kot pa da jih sploh ni. Pozitivna lastnost tehnike je, da razbija problem na posamezne dele, ki jih lahko rešujemo posamično in neodvisno od drugih.

Brez zadržka bi tehniko priporočili vsem, ki želijo ugotoviti in izboljšati varnost računalniškega sistema; ocenjujemo jo kot zelo uporabno predvsem v okolju z velikimi tveganji.

Literatura

[1] Pfleeger, C. P.: (1996): Security in computing, Prentice-Hall, Inc., Upper Saddle River, New Jersey.

[2] EMRIS – Enotna metodologija razvoja informacijskih sistemov, Vlada Republike Slovenije, Center za informatiko, Ljubljana.

[3] Ozsu, M. T., Valduriez, P.: Priciples of Distributed Database Systems, Prentice-Hall PTR, Upper Saddle River, New Jersey.

[4] Subrahmanian, V. S.: Principles of Multimedia Database Systems, Morgan Kaufmann Publishers, Inc, San Francisco, California.

[5] Adriaans, P., Zantinge, D.: Data Mining, Addison Wesley Longman Limited, Harlow, England.

Matjaž Jaušovec je diplomiral leta 1996 na Fakulteti za elektrotehniko, računalništvo in informatiko Univerze v Mariboru. Je študent magistrskega študija na omenjeni fakulteti. Pri raziskovalnem delu se ukvarja predvsem z vrednotenjem podatkov.

Boštjan Brumen je doktorski študent na Fakulteti za elektrotehniko, računalništvo in informatiko v Mariboru, kjer je zaposlen kot asistent za področje informatika. Raziskovalno se ukvarja s podatkovnimi bazami in podatkovnim rudarjenjem.

Tatjana Welzer - Družovec je izredna profesorica na Fakulteti za elektrotehniko, računalništvo in informatiko v Mariboru, kjer predava na dodiplomski in podiplomski stopnji in vodi laboratorij za podatkovne tehnologije. Raziskovalno se ukvarja predvsem s podatkovnimi bazami, kakovostjo podatkov in podatkovnim modeliranjem.