UDK: 004.6 Stručni rad

DEFINISANJE ADEKVATNIH MERA U FUNKCIJI ZAŠTITE POSLOVNIH INFORMACIONIH SISTEMA

DEFINING ADEQUATE MEASURES IN ORDER TO PROTECT BUSINESS INFORMATION SYSTEMS

Nikola Dragović[1], Mirjana Žilović[1], Nikola Bošković[1]
[1]*Visoka škola strukovnih studija za informacione tehnologije*
nikola.dragovic@its.edu.rs, mirjana.zilovic@its.edu.rs, nikola.boskovic@iths.edu.rs

Apstrakt: *Kompjuterski kriminal, zbog svog specifičnog karaktera, visoke stope rasta i velike društvene opasnosti, u sve većoj meri postaje vrlo ozbiljan društveni problem. U radu je ukazano na značaj definisanja i propisivanja pravila kojima će se zaštititi i osigurati odvijanje vitalnih procesa i funkcija institucije, u kojoj se računarski sistemi koriste.*
Ključne reči: *računarski sistem, ''zlatna pitanja'' zaštite, mere zaštite, politika zaštite.*

Abstract: *Cyber crime, due to its specific character, high rate of growth and big social danger, is increasingly becoming a very serious social problem. The paper puts the emphasis on the importance of defining and prescribing rules to protect and ensure the running of vital processes and functions of the institution, in which the computer systems are used.*
Key words: *Computer system, "golden questions" of protection, protection measures, protection policy.*

1. UVOD

Zaštita poslovnih informacionih sistema (PIS), definisanje i sagledavanje svih faktora koji predstavljaju pretnje za ugrožavanje i urušavanje stabilnosti rada računarskog sistema predstavlja izuzetno složen proces. On se mora posmatrati sa više različitih aspekata u vremenu i prostoru i ne sme se podceniti ni u jednom trenutku i ni u jednoj tački. Razlog za ovakav stav leži u činjenici da opasnosti koje predstavljaju pretnju PIS-u i njegovim objektima, posredno ili neposredno, kontinuirano ili povremeno, u manjoj ili većoj meri, toliko su brojne i međusobno povezane da nad celim informacionim sistemom (IS) formiraju krajnje kompleksnu mrežu opasnosti.

2. ULOGA RAČUNARA U PROBLEMIMA ZAŠTITE PIS-A

Pod pojmom upravljanja zaštitom poslovnih informacionih sistema podrazumeva se:

- identifikacija (računarskih) resursa,
- njihovo vrednovanje,

- procena rizika s obzirom na moguće pretnje,
- izrada odgovarajuće bezbednosne politike i njena implementacija u stvarnom okruženju.

Ulogu računara zavisi od konteksta njegove primene[1]:

- računar - objekt napada
- računar - subjekt napada – sredstvo izvršenja;
- računar - sredstvo za prikrivanje ili planiranje i rukovođenje realizaciom kriminalnih aktivnosti i dela;
- računar - simbol za obmanu;
- računar - sredstvo za sprečavanje, razjašnjavanje i dokazivanje kriminalnih aktivnosti i dela.

Računar - objekat napada

Vrednost hardvera i softvera, kao i najraznovrsniji podaci koji se nalaze u PIS-u, a koji reprezentuju određene poslovne vrednosti (poslovne tajne, projekte, funkcionisanje, način rada, novac, intelektualna dobra, poverljive informacije...), predstavljaju dovoljno jak izazov mnogim pojedincima, organizovanim grupama i kriminalnim organizacijama da do njih dođu na nelegalan način, što predstavlja računar kao objekta napada u PIS.

Računar – ''subjekat'' napada

U ovoj kategoriji računarski procesi su ključni i oni se koriste da bi omogućili, olakšali i/ili ubrzali realizaciju određenih kriminalnih aktivnosti usmerene ka odrđenom informacionom stemu, a upravo računar u PIS kreira jedinstven ambijent u kojem su raznorazne kriminalne aktivnosti realno moguće. Pri tome, kriminalac esencijalno ubacuje nove programske instrukcije u poslovni informacioni sistem da bi manipulisao računarskim procesima ili konvertuje legitimne računarske procese za nelegitimne potrebe.

Računar - sredstvo za prikrivanje ili planiranje i rukovođenje realizacijom kriminalnih aktivnosti

U ovom slučaju računar pomaže da se kriminalne radnje obavljaju brže, pouzdanije i anonimnije, čineći težim identifikaciju i otkrivanje (dokazivanje) takvih aktivnosti nad IS. Zahvaljujući mogućnostima računari mogu biti korišćeni kao snažan i precizan alat u planiranju, organizovanju ili rukovođenju kriminalnih aktivnosti, bilo od strane pojedinca, organizovanih kriminalnih grupa.

Računar - simbol za obmanu

Ugled koji računar uživa zbog svoje preciznosti, kao i rasprostranjeno shvatanje da i računar može da pogreši, često se koriste kao maska za izvršavanje ili prikrivanje određenih kriminalnih radnji. Bez obzira na činjenicu da je sve više onih za koje računar ne predstavlja nepoznanicu, uvek će biti i onih drugih, naivnih, gramzivih i lakovernih, koji upravo zbog toga predstavljaju veoma zahvalne objekte obmane uz pomoć računara.

Računar - sredstvo za sprečavanje, razjašnjavanje i dokazivanje kriminalnih dela nad PIS

Računar ne predstavlja snažan alat samo u rukama onih koji izvršavaju kriminalno delo nad IS. Predstavlja i veoma snažno sredstvo za sprečavanje, otkrivanje, razjašnjavanje i dokazivanje kriminalnih dela: integracija raspoloživih policijskih podataka, brzina, tačnost, kompletnost i raznovrsnost njihove obrade (selekcija po različitim kriterijumima,

sortiranje, poređenje, ukrštanje, povezivanje, statističko obrađivanje i sl.), kao i njihovo korišćenje u realnom vremenu, omogućavaju policijskim organima da svoju delatnost, pre svega preventivnu, podignu na znatno viši nivo.

3. CILJEVI ZAŠTITE I MOGUĆE PRETNJE

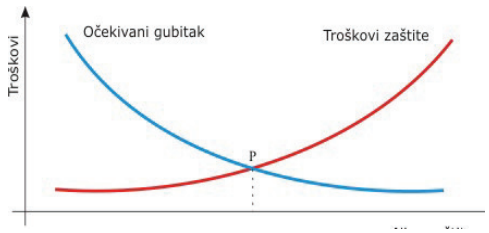
U funkcionisanju jednog PIS-a informacone tehnologije su od velikog značaja za brzinu obrade podataka, dostupnost, preciznost..., zapravo više i nije moguće zamisliti uspešnu kompaniju bez svog IS. Na žalost, primena informacionih tehnologija nisu uvek pozitivne i poželjne, postoji i ona ''druga strana funkcionisanja''. Tu spadaju, pre svega, one promene i pojave koje pogoduju asocijalnim i kriminalnim ponašanjima i aktivnostima i koje podstiču njihovo nastajanje, širenje i intenzitet. Ove promene i pojave predstavljaju u suštini kriminogene faktore koji se moraju imati u vidu kod sagledavanja i razrešavanja zaštite poslovnih informacionih sistema. Analizom nastalih promena, kao i onih koje su u toku, moguće je definisati kriminogene faktore na globalnom nivou: tehnološki razvoj, preuzimanje funkcija, koncentracija podataka, bogatstvo izbora, nove kriminalne metode i tehnike, stabilnost rizika, inženjersko planiranje, povećanje moći pojedinaca, širenje informatičke pismenosti, glorifikacija kompjuterskih kriminalaca, informatička etika, zakonska regulativa, zaštita itd.

U vezi sa navedenim faktorima neophodno je naglasiti značajnu činjenicu, da oni u manjoj ili većoj meri doprinose da se zloupotreba informacione tehnologije može izvršavati lakše, brže, obimnije i anonimnije.

Upravo zbog toga posebno je značajno shvatiti i zapamtiti da u razrešavanju problema zaštite informacionih sistema aktivnosti treba usmeriti ka navedenim faktorima u cilju neutralisanja ili ublažavanja njihovog uticaja na podsticanje, širenje i intenzitet kriminalnih aktivnosti. Međutim, te aktivnosti ne bi mogle biti preduzimane prema svim izloženim faktorima, jer je očigledno da bi šteta bila daleko veća od koristi. Tako, na primer, bilo bi nerazumno i krajnje štetno zbog zaštite informacionih sistema sprečavati ili usporavati tehnološki razvoj, preuzimanje osetljivih funkcija i podataka od strane informacione tehnologije ili širenje informatičke pismenosti. Nasuprot tome, aktivnosti na promovisanju i primeni informatičke etike, adekvatne zakonske regulative i izgradnji celovitih i kvalitetnih sistema zaštite predstavljaju imperativ.

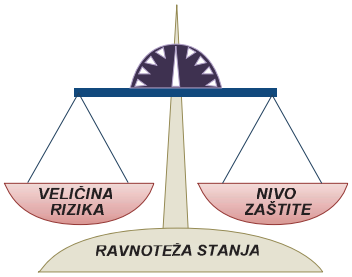
Svaka poslovna organizacija je specifična u pogledu izloženosti rizicima i potrebnim merama zaštite, pa je zbog toga i cena zaštite različita. Najviši nivoi zaštite su izuzetno skupi. Gledajući na odnos cena/kvalitet, može se reći da se bitne mere zaštite mogu realizovati i sa malim troškovima.

Sva ulaganja u zaštitu PIS-a moraju biti u skladu sa vrednošću informacija, podataka, celokupnog sistema koji se štite, tj. da pri izboru adekvatnih mera zaštite u cilju smanjenja ili neutralisanja identifikovanih pretnji, troškovi zaštite ne bi smeli biti ni veći ni jednaki potencijalnom gubitku. Odnos potencijalnog gubitka i troškova zaštite grafički je prikazan na Slici 1. Presek krivih (tačka P) označava optimalni nivo zaštite.



Slika 1. Optimalni nivo zaštite[2]

Prema tome, u realizaciji sistema zaštite treba težiti uspostavljanju ravnotežnog stanja između veličine rizika i ostvarenog nivoa zaštite poslovnih informacionih sistema (Slika 2). Manje od toga bi predstavljalo nedovoljnu zaštitu, a više od toga bi samo iziskivalo dodatne (nepotrebne) troškove.



Slika 2. Ravnotežno stanje veličine rizika i nivoa zaštite

Zaštita poslovnih informacionih sistema je vrlo složen problem, jer uključuje mnogobrojne interakcije između raznih komponenti. Mehanizmi zaštite se stalno razvijaju, jer to zahtevaju novi problemi koji se pojavljuju. Najosetljiviji deo u mehamizmu zaštite je čovek koji radi u datoj poslovnoj organizaciji.

Kada se razmišlja o zaštiti poslovnih informacionih sistema, polazi se od činjenice da bilo koji sistem zaštite ima smisla ako i samo ako njime nešto, od nečega i zbog nečega se štiti, a da bi isti postigao cilj on svoju funkciju mora sa nečim i na neki način izvršavati[2]. Iz ovakve opšte konstatacije nije teško uočiti ''zlatna pitanja''[3] o zaštiti računarskog sistema na koja treba dati što potpunije odgovore (Slika 3):

1. Šta štititi?
2. Od koga ili čega štititi?
3. Zbog čega štititi?
4. Čime štititi?
5. Kako štititi?

Odgovor na prvo pitanje podrazumeva utvrđivanje objekta zaštite, na drugo podrazumeva identifikaciju pretnji (opasnosti) koje, u manjoj ili većoj meri, mogu ugroziti objekte zaštite. Odgovaranje na treće pitanje podrazumeva utvrđivanje posledica koje neka pretnja može izazvati u odnosu na neki objekat, a na četvrto podrazumeva izbor mera koje će se koristiti. Poslednje pitanje podrazumeva definisanje politike zaštite.

Slika 3. ''Zlatna pitanja" zaštite računarskih sistema

4. OBJEKTI ZAŠTITE

Nalaženje odgovora na pitanje *Šta štititi* je prvi ključni korak u izučavanju i razrešavanju problema zaštite u poslovnim informacionim sistemima. Jer, ukoliko je skup odgovora na postavljeno pitanje prazan skup, otpada i svaka potreba preduzimanja bilo kakvih aktivnosti na ovom planu. Međutim, kako je jedan od osnovnih kriterijuma kod utvrđivanja objekata zaštite njihova vrednost za onog kome pripadaju, jasno je da taj skup sigurno neće biti prazan. Pri tome, u praktičnom razrešavanju ovog pitanja, ne bi se trebala gubiti iz vida opštost datog skupa, koji isključivo može da posluži samo kao polazna osnova koja bi se, zavisno od konkretnog stanja, uslova i specifičnosti, ili suzila ili proširila, tj. razradila do željenog nivoa detaljizacije. Drugim rečima, dok za neke informacione sisteme navedeni broj objekata može biti prevelik, za druge sigurno nije konačan, a uz to svaki od tih objekata može se posmatrati i kao složen objekt koji se, po raznim kriterijumima, zavisno od potreba, može razložiti na elemente – objekte nižeg nivoa.

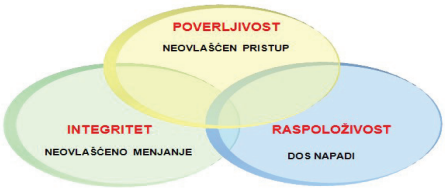
Ukoliko su utvrđeni objekti zaštite onda se zna i šta treba štititi, pa je logično da sledeći korak, identifikacija pretnji i opasnosti koje mogu posredno ili neposredno, u manjoj ili većoj meri ugroziti objekte zaštite.

Sledeći korak je definisanje potrebe *zbog čega* se štiti, a nalaženje ovog odgovora predstavlja ustvari utvrđivanje negativnih (štetnih) posledica koje identifikovane pretnje mogu izazvati delovanjem na objekte zaštite. Globalno gledajući posledice bi se uopšteno mogle iskazati kroz narušavanje: integriteta, poverljivosti i raspoloživosti.

Integritet mora osigurati konzistentnost informacija i onemogućiti bilo kakve neovlaštene promene sadržaja. Koristi se u kontekstu tačnosti i kompletnosti informacija koje se nalaze u sistemu u njegovoj celosti, uključujući i procese koji se obavljaju.

Poverljivost se odnosi na zaštitu određenih sadržaja, odnosno informacija od bilo kakvog namernog ili nenamernog otkrivanja neovlašćenim osobama[4]. Koristi se u kontekstu osetljivosti na otkrivanje (obelodanjivanje) podataka i informacija. Na primer, neko

istraživanje je osetljivo dok se podaci prikupljaju i obrađuju. Ali kada se jednom objave, dobijaju javni karakter i gube prethodni stepen poverljivosti.
Konačno, pojam *raspoloživost* podrazumeva da su sve relevantne informacije na mestu i upotrebljive za obavljanje namenjenih funkcija u vremenski prihvatljivom terminu. U tom kontekstu termin ''raspoloživost'' povezan je sa kontinuitetom usluga[5].
Bilo koji od ovih zahteva može biti kompromitovan na razne načine, bilo namernom ili nenamernom ljudskom greškom, bilo zbog nedostataka i kvarova opreme i aplikacija ili zbog drugih izvanrednih događaja (slika 4).



Slika 4. Osnovni elementi informacione bezbednosti po ISO 17799:2000 i njihove moguće pretnje

Osim ova tri osnovna zahteva treba spomenuti i pojmove koji su usko vezani uz implementaciju bezbednosnih kontrola, a to su:

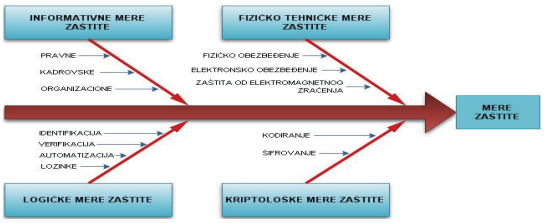
1. Pouzdanost je sposobnost komponente, uređaja ili sistema da obavlja svoju zadatu funkciju u određenim uslovima eksploatacije i da zadržava svoje parametre (osobine) u datim tolerancijama.
2. Neporicljivost je stanje sistema takvo da strane u transakciji ne mogu naknadno da poriču učestvovanje u svim ili delovima transakcije.
3. Proverenost je kao atribut bezbednosti računarskog sistema stanje u kome je omogućena provera rada svih komponenti računarskog sistema u svrhu pravovremenog otkrivanja eventualne povrede njegove bezbednosti.

5. MERE I POLITIKA ZAŠTITE

Odgovor na pitanje *Čime štiti* podrazumeva identifikaciju svih mera koje stoje na raspolaganju u izgradnji celovitog i pouzdanog sistema zaštite. Sve te mere, po svojim prirodnim svojstvima koja ih karakterišu (Slika 5), mogu se razvrstati na sledeći način: normativne, fizičko-tehničke, logičke i kriptološke.
Mere *normativnog* karaktera, u koje spadaju pravne, organizacione i kadrovske mere, pripadaju kategoriji netehničkih mera. Osnovna karakteristika ovih mera je da ne degradiraju rad poslovnih sistema, već naprotiv, znatno doprinose povećanju njegove raspoloživosti i produktivnosti, a istovremeno značajno utiču na efikasnost sistema zaštite. Ovim merama se utvrđuje politika zaštite, koja određuje šta se smatra prihvatljivim i kakve su sankcije za neprihvatljivo ponašanje – što im daje karakter samostalnog i delotvornog instrumenta u pravcu preventivnog odvraćanja od nedozvoljenih aktivnosti, a istovremeno predstavljaju najjeftinije i najefikasnije sredstvo u

u sprečavanju i otkrivanju brojnih nedozvoljenih ponašanja i aktivnosti.
Fizičko-tehničke mere mogu biti vrlo efikasne za određene probleme zaštite, ali isto tako povlače za sobom i znatne troškove. Njihova zajednička karakteristika je da uslovljavaju finansijske investicije pre nego što počnu da dejstvuju, znači unapred, plus troškove njihovog tekućeg održavanja. Pozitivna strana se ogleda u činjenici da se svi ovakvi troškovi mogu tačno proceniti i izbor planski podesiti raspoloživim finansijskim mogućnostima. Ono što svakako treba imati u vidu je činjenica da efikasnost ovih mera značajno opada u ambijentu u kojem normativne mere nisu primenjene na adekvatan način.
Logičke mere za ne mali broj problema zaštite posovnih informacionih sistema predstavljaju jedino, ali i vrlo snažno sredstvo. Visok stepen efikasnosti se prvenstveno postiže korišćenjem logičkih mera ''u paketu''. S druge strane, ove mere povlače za sobom tzv. ''nevidljive'' (prikrivene) troškove, jer direktno utiču na smanjenje raspoloživosti i efikasnosti računarskog sistema, a to je dovoljan razlog da se njihovoj primeni pristupi krajnje odgovorno, osmišljeno i racionalno. I u ovom, kao i u prethodnom slučaju, važi konstatacija da je efikasnost ovih mera uslovljena, ne samo njihovim sopstvenim kvalitetom, već i adekvatnom primenom mera normativnog karaktera.

Kriptološke mere zaštite, posebno u kooperaciji sa merama zaštite od kompromitujućeg elektro-magnetnog zračenja, omogućavaju ostvarivanje najvišeg mogućeg nivoa zaštite. Međutim, ove mere, kao i bilo koje druge, jesu potrebne, ali i pored mogućnosti zadovoljenja širokog spektra zahteva za zaštitom informacionih sistema, one nisu i dovoljne da samostalno obezbede potrebnu zaštitu. Razlog je u činjenici da efikasnost i ovih mera značajno opada u ambijentu u kojem normativne mere nisu primenjene na adekvatan način, jer: ''Ne postoji ni Faradejev kavez, ni kriptouređaj, ni dovoljno pouzdana lozinka koji mogu zaštititi računarski sistem u ambijentu u kojem se ne zna ko, šta, kako i kada treba, može i mora da radi.''[7]
Definisanje politike zaštite koja će se sprovoditi u konkretnom ambijentu predstavlja odgovor na peto pitanje *Kako štititi*. Pri tome bi trebalo imati u vidu da je cilj nalaženja odgovora na ovo pitanje ustvari utvrđivanje svih relevantnih faktora i njihovih međusobnih veza, neophodnih za jedan, zbog njihove promenljivosti u vremenu i prostoru, ciklični proces poznat pod nazivom upravljanje rizikom , koji podrazumeva spektar aktivnosti (uključujući normativne, fizičko-tehničke i logičke kontrole i procedure) i kojim se savlađuje ranjivost informacionih sistema.
Sam rizik rezultira iz kombinacije vrednosti nekog objekta sa posledicom koju materijalizuje bilo koja pretnja koja deluje na objekat. Zbog vrlo kompleksne prirode informacionih sistema za koje se rizik razmatra, u većini slučajeva nije realno da se na postojanje i otkrivanje rizika odgovori pokušajima njegove potpune eliminacije. Izvori rizika su često smešteni van dohvata, tako da oni ne mogu biti jednostavno odstranjeni. Takođe, složeni sistemi su obično izloženi širokom i raznovrsnom spektru potencijalnih pretnji, pa bi njihova totalna eliminacija zahtevala angažovanje neodređenog obima resursa, ali i pored toga sa neizvesnim rizikom[8].



Slika 5. ''Riblja kost'' osnovnih mera zaštite[6]

6. ZAKLJUČAK

Usmeravanje pažnje na faktore koji su pretnja za ugrožavanje rada i stabilnost jednog poslovnog informacionog sistema je prvi korak za uspešnu implemantaciju odgovarajućih bezbednosnih mera, a radi odvijanja i osiguranja vitalnih procesa i funkcija institucije (poslovne kompanije), u kojoj se sistem koristi. Predložene bezbednosne mere povećanju zadovoljstvo u radu, unapređenje i poboljšanje uslova rada svih korisnika PIS-a, kroz njihovo upoznavanje i deklarisanje informacionog sistema. Ukupna bezbednost celokupnog sistema je onolika kolika je bezbednost najslabije karike, pri tome se učestalo misli na ljudske resurse organizacije, koji najčešće predstavljaju najveću pretnju računarskoj bezbednosti, bez obzira da li se radi o namernim pokušajima neovlašćenog pristupa ili o slučajnim greškama.
Podizanje svesti o računarskoj bezbednosti ima za cilj podići svestnost svih zaposlenih o bezbednosti na svim hijerarhijskim nivoima, a efikasno je, samo ako je planirano, sprovedeno, evaluirano i unapređeno prema određenim organizacionim smernicama prikazanim u ovom radu.

LITERATURA

[1] Petrović, S., *Kompjuterski kriminal*, Vojnoizdavački zavod, Beograd, 2004.
[2] NIST: National Institute of Standards and Technology Special publication 800-30: *Risk management guide for Information Technology Systems*
[3] Anđelić, S., Dragović, N. i Obradović S., *Kriptologija i kriptosistemi*, naučno-stručni simpozijum INFOTEH 2008, Jahorina, Republika Srpska, CD izdanje, ISBN 99938-624-2-8
[4] Đapić, M., i Lukić, Lj., *Standardi serije ISO/IEC 27000 najbolja poslovna praksa za sigurnost informacija*, 34. Nacionalna konferencija o kvalitetu, Kragujevac, 2007
[5] Rodić, B., *Da li ste sigurni da ste bezbedni*, CIP – Beograd, 2004.
[6] Milanović, Z., *Organizacija zaštite računarskih sistema*, magistarski rad, odbranjen na Mašinskom fakultetu, Univerzitet u Beogradu, 2006.
[7] Grubor, G., *Razvoj i upravljanje programom zaštite zasnovanim na modelu sazrevanja procesa*, doktorska disertacija, odbranjena na Fakultetu za poslovnu informatiku, Univerzitet Singidunum, Beograd, 2007.