

POSLOVNA POLITIKA U FUNKCIJI ZAŠTITE INFORMACIONIH SISTEMA

Dragutin Bjelovuk

Visoka škola poslovnog menadžmenta "PRIMUS" Gradiška
Dositejeva bb, Gradiška 78400, RS/BiH
Tel: +387 (0)65/321-932
Fax: +387 (0)51/816-213
E-mail: drago_b@msn.com

Boško Rodić

Visoka škola poslovnog menadžmenta "PRIMUS" Gradiška
Dositejeva bb, Gradiška 78400, RS/BiH
Tel: +387 (0)66/296-678
E-mail: bosko.rodic@gmail.com

Milica Tepšić

Ministarstvo uprave i lokalne samouprave Republike Srpske
Banja Luka, Trg Republike Srpske 1
Tel: +387 (0)65/561-695
E-mail: milica.tepsic@gmail.com

Sažetak

Sve veći problem i ograničavajući faktor razvoja i primjene računarskih sistema postaje bezbjednost poslovnih informacionih sistema. Sa povećanjem broja napada na poslovne informacione sisteme, i to ne samo na one koji sadrže povjerljive i/ili osjetljive podatke sve više raste potreba za propisivanjem pravila kojima će se zaštititi materijalne i intelektualne vrijednosti organizacije. Zbog toga je veoma važno da pravila obuhvate sva područja na kojima je moguće izvršiti neku vrstu napada. Jasno je da napade nije moguće predvidjeti, a ponekad niti spriječiti, ali moguće je preduzeti sve mjere opreza kako bi se šteta koju je napad prouzrokovao smanjila na najmanji mogući nivo.

Ključne riječi: *poslovna politika, poslovni informacioni sistem, informacija, informaciona bezbjednost*

Abstract

A growing problem and limiting factor for the development and application of computer systems becomes security of business information systems. With increasing number of attacks on business information systems, not only those that contain confidential and/or sensitive data growing need for issuing rules that would protect the material and intellectual values of the organization. It is therefore very important that the rules include all areas where it is possible to make some kind of attack. It is clear that the attack is not possible to predict, and sometimes not prevent, but it is possible to take all precautionary measures in order to damage the attack caused decreased to the lowest possible level.

Key words: *business policy, business information systems, information, information security*

1. UVOD

Prema riječnicima stranih riječi politika (u užem smislu), kao prilog, je „mudro, pametno, razumno, oprezno, lukavo, razborito, promišljeno, smišljeno... i/ili mudrost i vještina ophođenja sa ljudima i snalaženje u životu...“. Sa druge strane „politika“ podrazumijeva rukovođenje – upravljanje, djelatnosti u nadležnosti top menadžmenta.

Poslovnu politiku čine poslovne odluke kojima se definišu načela, principi i kriterijumi kojima se usmjerava odlučivanje u poslovanju preduzeća. Postupkom formulisanja poslovne politike stvara se polazna osnova za donošenje odluka kojima se usmjeravaju aktivnosti na ostvarenju ciljeva.

Prema tome, poslovna politika osnovni je okvir za upravljanje bezbjednošću poslovnih informacionih sistema. Politika bezbjednosti poslovnih informacionih sistema trebala bih da sadrži načela i principe upravljanja bezbjednošću resursa, te odgovornosti koje se odnose na bezbjednost. Cilj donošenja poslovne politike je obezbjeđenje adekvatnog nivoa bezbjednosti poslovnog informacionog sistema. Poslovna politika treba da obuhvati područja upravljanja, logičke i fizičke zaštite resursa u zavisnosti od veličine i složenosti samog informacionog sistema [3].

Izrada kvalitetne poslovne politike trebala bi da obuhvata utvrđivanje resursa, detaljnu procjenu eventualnih rizika, definisanje prijetnji i procjenu „ranjivosti“. Pomoću navedenih komponenti organi upravljanja mogu shvatiti protiv čega se bore i kako mogu ostvariti ciljeve, uz minimalne troškove.

BSP (*Bussines Systems Planning*) metodologija obavezuje top menadžment da preuzme na sebe odgovornost za razvoj informacionog sistema. Samim tim se podrazumijeva da top menadžment vodeći poslovnu politiku vodi računa i o informacionoj bezbjednosti. Ovo, prije svega, zbog strateškog značaja informacija za poslovni sistem.

U ovom radu ćemo objasniti različite zahtjeve poslovnog procesa koje treba imati u vidu pri dizajniranju sistema zaštite. Zanimarivanje bilo kojeg od navedenih aspekata može dovesti do problematičnog i neefikasnog dizajna.

2. UTVRĐIVANJE RESURSA

Jedan od uslova za uspješno upravljanje bezbjednošću informacionog sistema jeste identifikacija resursa koji su dio tog sistema. Bez precizne identifikacije resursa nije moguće sprovesti njegovu kvalitetnu zaštitu.

Svaki poslovni informacioni sistem posjeduje resurse na koje se mora računati, kako u fizičkom, tako i u funkcionalnom smislu. Utvrđivanje resursa predstavlja proces u kome „kompanija procjenjuje“ vrijednost podataka i sistema kojima raspolaže. Ponekad je to jednostavan proces koji se svodi na obično prebrojavanje sistema i softverskih licenci. Takvo fizičko utvrđivanje resursa je uobičajeni dio standardne računovodstvene procedure, koju organizacije moraju redovno sprovoditi.

Proces identifikacije resursa i utvrđivanje njihove važnosti i vrijednosti može se obaviti na najvišem nivou i ne mora da uključuje skupe, detaljne i vremenski zahtjevne analize. Ovo je posebno važno za male firme i organizacije sa ograničenim resursima. Činjenica je da sve organizacije imaju ograničene resurse i rizik nikada ne može biti sveden na nulu. Kvalitet analize utvrđuje se na osnovu postavljenih funkcionalnih i bezbjednosnih ciljeva, te bi se

moralo mjeriti u kontekstu utrošenog vremena i nastalih troškova u odnosu na važnost i vrijednost samih resursa.

Obilježja resursa koja pritom treba uzeti u obzir jesu njihova važnost i osjetljivost, te eventualna inherentna zaštita. Funkcionalne i bezbjednosne potrebe resursa zavise od njihove ranjivosti i prisutnosti određene prijetnje [2].

Procjena vrijednosti podataka predstavlja znatno složeniji dio procesa utvrđivanja resursa. U nekim slučajevima može se utvrditi samo šteta koja bi nastala zbog nedostupnosti ili gubitka podataka. Ukoliko bi gubitak podataka blokirao čitav posao, njihova cijena je nemjerljiva. Takva vrsta podataka pojednostavljuje proces definisanja metoda i pristupa za njihovu zaštitu.

Formula za Coca-Colu i recept za piletinu sa pirinčem svakako nemaju istu vrijednost. Coke formula može da vrijedi čitavo bogatstvo za onoga ko je ukrade; kradljivac je može prodati konkurenciji i mirno otići u penziju. Recept za pile može poslužiti za spremanje divne večere, ali nema nikakvu vrijednost sa finansijske tačke gledišta.

3. PROCJENA RIZIKA

Procjena rizika je veoma važan faktor pri uspostavi poslovne politike. Bez procjene rizika organizacija može uvesti poslovnu politiku sa sasvim opštim pravilima, koji ne uzimaju u obzir moguće rizike specifične za područje djelatnosti. Međutim, organizacija može definisati poslovnu politiku detaljno ili manje detaljno, samo je pitanje na koji će se nivo bezbjednosti odlučiti. Procjena rizika se sastoji se od: otkrivanja opštih prijetnji, otkrivanja specifičnih prijetnji, otkrivanja potrebnog nivoa zaštite i usklađivanja potrebnog nivoa zaštite sa mogućnostima [5].

Postoji nekoliko načina za procjenu rizika, od naučnih metoda, zasnovanih na formulama, do običnog razgovora sa korisnicima. U principu, u procjeni rizika treba identifikovati troškove zamjene ukradenih podataka ili sistema, troškove usljed nefunkcionalnosti sistema i sve druge faktore koji su važni za poslovni informacioni sistem. Procjenu rizika je moguće izvršiti tek nakon utvrđivanja resursa. Tek kada se utvrde svi resursi jednog poslovnog informacionog sistema može se početi sa procjenom eventualnih troškova [4].

Nakon utvrđivanja troškova, moguće je proračunati i vjerovatnoću pojave određenih događaja i njihov najverovatniji ishod. Ako se poslovni informacioni sistem nalazi u SAD-u, koja je vjerovatnoća da će biti ugrožen zemljotresom? Da li će procjena rizika ukazati na listi glavnih uzročnika problema na visoku vjerovatnoću pojave zemljotresa?

Proces procjene rizika započinje identifikacijom prijetnji i ranjivosti, zatim određivanjem vjerovatnoće i uticaja na svaki rizik. Procjena rizika je težak i kompleksan posao, a donosi se obično na osnovu nepotpunih informacija. Postoji dosta metoda za procjenu rizika, koje manje - više daju dobre rezultate.

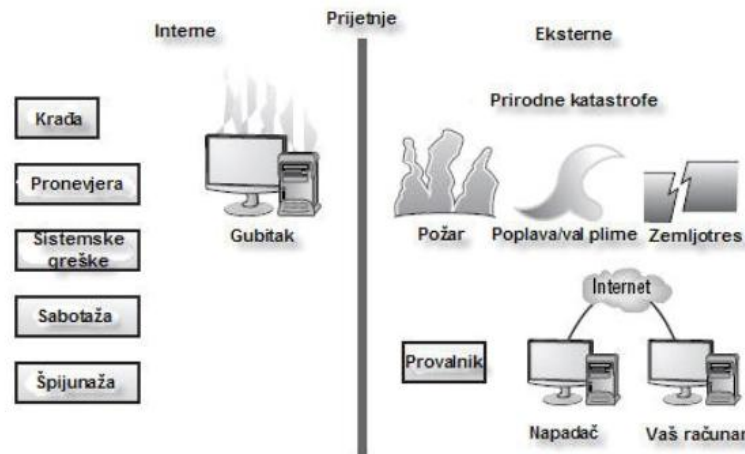
Svrha procjene rizika je da ukaže na slabe tačke informacionog sistema, te davanje smjernica gdje usmjeriti resurse. Postoje četiri osnovne strategije za upravljanje rizikom: ublažavanje, prenošenje, primanje i izbjegavanje. Za svaki rizik u izvještaju procjene rizika mora da se osmisli strategija za upravljanje rizicima. Cilj strategije za upravljanje rizicima je da smanji rizik na prihvatljiv nivo uz prihvatljiv trošak [3].

4. DEFINISANJE PRIJETNJI

Izuzetno je teško znati koje i kakve prijetnje stvarno stoje pred informacionim sistemom i još je teže znati u kom pravcu će se kretati razvoj takvih prijetnji. Utvrđivanje bezbjednosne politike obavezno uključuje i procjenu rizika od internih i eksternih prijetnji kojima resursi

organizacije mogu biti izloženi. Kreiranje zaštićenog okruženja koje sprječava sve napade spolja neće imati nikakvu vrijednost ukoliko prijetnje uglavnom potiču iznutra. Ukoliko član tima donese u kancelariju disk "zaražen" virusom i učita njegov sadržaj na računar, virus se može proširiti preko čitave mreže, zbog toga što je potpuno imun na mjere zaštite koje su usmjerene ka spoljašnjem svijetu [3].

To je uobičajeni problem u organizacijama u kojima korisnici obično rade sa djeljivim resursima. Ako su u organizaciji instalirani računari za javnu upotrebu, koji su povezani na mrežu, virus može "inficirati" sve sisteme u mreži. Eksterne mjere zaštite u takvim uslovima neće spriječiti oštećenje ili gubitak podataka.



Slika 1. Pregled internih i eksternih prijetnji

4.1. Interne prijetnje

Većina dokumentovanih internih prijetnji spada u grupu finansijskih zloupotreba, koje se javljaju u vidu prevara ili krađa. Takve prijetnje, posebno u okruženjima sa intenzivnom primjenom računara, teško se otkrivaju i istražuju. One su dugotrajne i obično se javljaju u obliku malih transakcija u dužem vremenskom periodu.

U jednoj takvoj prevari nosilac je bio profesionalni računovođa, koji je pravio lažne račune za fiktivne poslove koji nikada nisu obavljani. Za nekoliko mjeseci on je zaradio više od 100.000 dolara isplatama kompanijama koje su osnovali on i njegovi rođaci. Prevara je otkrivena tek nakon složene istrage, u koju su bili uključeni stručnjaci iz oblasti finansija i računara. Sa stanovišta zaštite računara, riječ je o internoj prijetnji koja je bila rezultat propusta u kontroli finansijskih, operativnih i računarskih mjera zaštite. Takvih incidenata ima znatno više nego što su objekti prevare spremni da priznaju, čak i znatno više u odnosu na broj detektovanih slučajeva.

U drugom primjeru nosilac je bio jedan zaposleni koji je koristio računarske resurse organizacije za svoje finansijske transakcije. Prevara je trajala nekoliko godina. Kada je otkrivena, zaposleni je dobio automatski otkaz, uz zaplijenu svih njegovih podataka. Tokom istrage, međutim, došlo je do nenamjernog oštećenja zaplijenjenih podataka, čime su uništeni i dokazni materijali. Kada je došlo do suđenja, na zahtjev advokata optuženog sud je odbacio prikupljene dokaze. Iako je bilo očigledno da je optuženi kriv, sudija je obustavio čitav slučaj - zbog nedostatka nepobitnih dokaza. Zaposleni je, nakon toga, tužio firmu, zbog netačnih optužbi, uznemiravanja i sličnih razloga. On je čak i dobio taj sudski spor, pa je vraćen na stari posao.

U navedenom primjeru do problema je došlo zbog grešaka u internoj politici u pogledu zaštite, zbog grešaka u funkcionisanju sistema koji su angažovani za detekciju, istraživanje i otklanjanje posljedica problema. Čitav slučaj je organizaciji donio velike novčane gubitke, dok je prevarant vraćen na posao [1].

4.2. Eksterne prijetnje

Veliki broj internih prijetnji sa kojima se organizacije bore uključuju i primjenu procedura i metoda koje su postale industrijski standard. Eksterne prijetnje, sa druge strane, imaju porast koji je već na granici dramatičnosti. Prije nekoliko godina većinu incidenata u vezi sa računarima izazivala su lica koja su to radila iz hobija i radi zabave. U najvećem broju slučajeva ti incidenti nisu bili zlonamjerne prirode; samo mali broj je dovodio do izmjene ili uništenja podataka i slogova u bazama.

Većina kompanija danas koristi *online* baze podataka, interaktivne narudžbine, plaćanja, isporuke, *online* popis i administriranje ključnih podataka pomoću složenih sistema. Takvi sistemi su povezani sa drugim sistemima na kojima su smješteni povjerljivi korporativni podaci, poslovne tajne, stratejski planovi i drugi oblici vrijednih podataka.

Prilikom kompromitovanja takvih sistema obično dolazi i do kompromitacije kompletnog poslovnog procesa. Evidentirani su čak i takvi incidenti u kojima je "rupa" u bezbjednosnom sistemu ostajala otvorena više godina, pri čemu ugrožena kompanija nije imala nikakvih saznanja o kompromitovanju. Eksploatacija takvih propusta u bezbjednosnim sistemima predstavljaju najveće zadovoljstvo za profesionalne kriminalce.

Prvobitni metodi za "provaljivanje" u računarske sisteme su bili primitivni i zahtjevali su dosta rada. Danas, međutim, postoje takvi softverski paketi koji automatski pronalaze cilj, nakon čega preduzimaju sistematski napad na njega radi pronalaženja osjetljivih mjesta. Većina tih alati posjeduje grafički korisnički interfejs, koji zahtjeva minimum tehničkog znanja od hakera-početnika. Veliki broj računarskih sistema je neprekidno izložen metodičnim napadima znatiželjnika i kriminalaca koji pokušavaju da ostvare svoje kriminalne ciljeve [1].

5. PROCJENA "RANJIVOSTI"

Da bi poslovna politika bila potpuna potrebno je izvršiti i procjena ranjivosti. Cilj ovog koraka je da razvije spisak ranjivosti sistema (slabosti ili nedostataka) koji bi mogao biti iskorišten od strane potencijalnih prijetnji izvora [4].

Zaštita softvera i sistema koji se koriste u poslovanju je osnovna preokupacija u oblasti računarske zaštite. Veliki broj proizvođača operativnih sistema je u bliskoj prošlosti pitanjima zaštite poklanjao samo deklarativnu pažnju. Jedan od popularnih operativnih sistema je u cilju zaštite koristio tehniku prijave korisnika uz odgovarajuću lozinku. Nakon pojave dijaloga za prijavu na ekranu, korisnik je jednostavno mogao da pritisne dugme *Cancel*, nakon čega je imao pristup većini mrežnih i kompletnim lokalnim resursima. Ukoliko je zaštita ekrana (*screensaver*) bila zaštićena lozinkom, ponovni pristup sistemu je bio moguć unosom lozinke, ali i prostim resetovanjem sistema. Takva rješenja su bila opasnija od onih bez ikakve zaštite. Veliki broj korisnika je smatrao da je njihov sistem zaštićen, mada u suštini zaštite nije bilo - rezultat su bile brojne krađe podataka koje su vršile kolege na poslu.

Operativni sistemi i aplikativni programi su bili i još uvijek su osjetljivi na razne vrste eksternih i internih napada. Softverske kompanije žele da kreiraju programe koji su jednostavni za upotrebu, sa grafičkim dizajnom i olakšanom konfiguracijom. Želje korisnika

se poklapaju sa njihovim namjerama. Na taj način se, međutim, nameću novi problemi zaštite podataka u velikom broju mreža.

Brojni proizvođači operativnih sistema danas u cijelosti preispituju mjere zaštite svojih proizvoda. Oni su shvatili da ranije verzije njihovih proizvoda ne mogu zaštititi kompanije-korisnike od gubitka ili zloupotrebe podataka. Problem zaštite je postao osnovna preokupacija većine korisnika, tako da je danas "pokriven" u većini operativnih sistema i ostalih softverskih mrežnih proizvoda. Proizvođači softvera su ranije krili eventualne sigurnosne propuste u svojim proizvodima; danas se te slabosti javno objavljuju, pri čemu se odmah nakon njihovog otkrivanja pojavljuju i rješenja problema. Takva politika, međutim, pomaže i hakerima, koji su svjesni da veliki broj kompanija neće odmah primijeniti rješenja na svojim računarima [1].

6. ZAKLJUČAK

Osnovni razlog definisanja poslovne politike je zaštita imovine i misije same organizacije. Na osnovu poslovne politike svaka organizacija bi trebala propisati i primjenjivati detaljna interna akta, koja se odnose na sve aspekte bezbjednosti informacionog sistema. Politiku bezbjednosti informacionih sistema potrebno je uskladiti sa promjenama u informacionom sistemu i u njegovoj okolini, u slučajevima narušavanja bezbjednosti informacionih sistema, te zavisno od rezultata procjene rizika.

Sam razvoj poslovne politike u određenom poslovnom informacionom sistemu trebao bi da obuhvati sve zaposlene, čime bi se obezbjedila izgradnja uspješnog sistema zaštite. Većina bezbjednosnih incidenata su sve češće uzrokovali zaposleni što ukazuje da je potrebno uvesti niz efikasnih i jasno određenih pravila koja će obezbjediti i zaštititi materijalne i intelektualne vrijednosti organizacije od krađe, uništavanja i falsifikovanja. Potrebno je obratiti pažnju na svaki dio zaštite poslovnog informacionog sistema. Poslovna politika mora biti dokument prilagođen specifičnim potrebama organizacije.

Zbog strateškog značaja informacija informaciona bezbjednost mora biti predmet poslovne politike. Međutim, uvođenje poslovne politike može biti skup i dugotrajan proces u kojem je potrebno prilagoditi sve dijelove organizacije da rade sinhronizovano. Poređenjem uloženog i dobijenog, rezultat je sasvim jasan, poslovna politika je dobro ulaganje. Organizacijama i institucijama preporučujemo uvođenje poslovne politike radi podizanja nivoa bezbjednosti kako informacionog sistema, tako i korisnika istog.

LITERATURA

- [1.] Mike Pastore, Emmett Dulaney, *Security*, Sybex, 2007.
- [2.] Steve Elky, *An introduction to information system risk management*, SANS Institute, 2006.
- [3.] Boško Rodić, Goran Đorđević, *Da li ste sigurni da ste bezbedni*, Produktivnost AD, Beograd, 2004.
- [4.] Gary Stoneburner, Alice Goguen, Alexis Feringa, *Risk Management Guide for Information Technology Systems*, National Institute of Standards and Technology, Gaithersburg, 2002.
- [5.] Damir Kovačević, *Sigurnosna politika*, diplomski rad, Zagreb, 2008.