Kako sačuvati kontinuitet u poslovanju uprkos cyber incidentima?

MILICA D. ĐEKIĆ, Subotica

Stručni rad
UDC: 005.334:004.6

Savremeni informacioni sistemi su doneli mnoge pogodnosti kada je u pitanju poslovanje preko računara i interneta, ali i kada je reč o automatizaciji procesa u okviru industrije, saobraćaja i drugih vidova klasične i kritične infrastrukture. Međutim, pored svih prednosti koje sa sobom nosi tehnološki napredak, postoje i mnoge opasnosti u vidu cyber rizika, pretnji, ali i realnih hakerskih napada. U ovom radu, analizirane su opasnosti po cyber sisteme, kao i rizicima koje nose IT incidenti i vanredne situacije u slučaju ugrožavanja kontinuiteta poslovanja kako velikih kompanija, tako i malih i srednjih preduzeća.

Ključne reči: *cyber, kontinuitet, poslovanje, privreda, ekonomija, hakovanje*

1. UVOD

Čini se da je u današnje vreme lakše nego ikada počiniti zločin. Preko 2,8 milijarde ljudi širom sveta poseduje priključak za internet, a procenjuje se da će hakerska zajednica do 2020. godine da dobije još milion novih članova. Rizik da privatni ili poslovni računar postane meta cyber napada je iz godine u godinu sve veća. Po nekim procenama, cyber kriminal košta svetsku ekonomiju stotine milijardi dolara godišnje. To su ogromini gubici, ali i razlog više da se ulaže u cyber industriju.

Neretko se dešava da hakeri biraju velike kompanije za svoje ciljeve i tada se dešavaju spektakularne pljačke koje povlače sa sobom štetu od nekoliko desetina ili čak stotina miliona dolara u roku od svega nekoliko trenutaka. Međutim, nisu samo velike kompanije meta hakera i cyber napadača. Najčešći izazov za prosečnog hakera su upravo mala i srednja preduzeća, koja donose prilično dobru zaradu napadačima, a pri tome povlače sa sobom minimum rizika, jer im je nivo cyber zaštite na prilično niskom stepenu.

Osim toga, mala i srednja preduzeća, koja u proseku imaju 30-50 zaposlenih, nisu samo meta zato što se upadom u njihove informacione sisteme može doći do vrednih, ali poverljivih podataka poput brojeva kreditnih kartica, bankovnih podataka zaposlenih i klijenata ili, pak, ličnih podataka nekog trećeg lica, već su i izvor tržišno vrednih informacija kao što su projektna dokumentacija, intelektualna svojina, patenti i slično. Svaki od ovih podataka ima svoju cenu na crnom tržištu i vrlo lako može da donese lepe prihode malicioznim subjektima.

Hakerska zajednica vrlo često komunicira, razmenjuje informacije i deli svoje znanje preko specijalizovanih foruma i diskusionih grupa. U načelu, čitavo podzemlje može da se sretne na takvim mestima, a ono što kriminalcima i teroristima omogućava relativno bezbednu komunikaciju su Darknet mreže ili skriveni slojevi dubokog interneta. Ovaj vid komunikacije otežava istragu i rešavanje slučaja bezbednosnim strukturama, ali treba napomenuti da su u današnje vreme dostupni neki alati pomoću kojih može da se presretne komunikacija čak i u dubokom web-u.

Međutim, ono što je za opstanak i rad biznisa najvažnije je da izbegne, ili, ako već ne može, da nastavi da funkcioniše i uprkos hakerskom napadu koji ga je snašao. Statistika pokazuje da ogroman procenat malih i srednjih preduzeća posle doživljenog upada u svoj sistem prestaje da funkcioniše ili biva izbrisano sa tržišta u roku od najviše 5 godina od prvog cyber napada. Ono što se diskutuje u ovom radu su upravo mere i strategije koje bi trebale da obezbede kontinuirano poslovanje i brz oporavak preduzeća za vreme i nakon hakerskog upada.

2. MALA I SREDNJA PREDUZEĆA KAO MOTOR EKONOMIJE

Interesantan podatak koji postoji u [9] sugeriše da se preko 60% bruto domaćeg proizvoda (BDP) u Srbiji ostvaruje upravo preko malih i srednjih preduzeća i da ona zapošljavaju preko milion ljudi u našoj zemlji. Iz tog razloga je prilično jasno zašto su takva preduzeća

Adresa autora: Milica Đekić, Subotica, Vase Pelagića 39 a

Rad primljen: 12.01.2015.
Rad prihvaćen: 26.01.2015.

od vitalnog, odnosno strateškog značaja za ekonomiju Srbije. Ozbiljni gubici u toj oblasti poslovanja bi mogli ozbiljno da naruše i ekonomiju naše države.

U praksi je potrebno razlikovati mala i srednja preduzeća po njihovoj delatnosti, odnosno, ne može isto da se tretira preduzeće koje se bavi trgovinom, kao i ono koje se bavi visokom tehnologijom. Vrlo je čest slučaj da vlasnik firme obavlja i neku od menažerskih funkcija i on tada mora da pokaže visok stepen strateškog razmišljanja kada je posao u pitanju. On pored svoje vlasničke i direktorske funkcije obavlja i mnoge druge poslove kao što su vođenje komunikacije sa partnerima i klijentima, donošenje odluka o poslovanju firme, definisanje strateških ciljeva, postavljenje zahteva koji su u skladu sa trendovima na tržištu, itd.

U stvarnosti to može da se ilustruje na sledeći način. Menadžment preduzeća ne održava baš sve vidove komunikacije sa strankama, ali je upoznat sa svim informacijama koje dođu u preduzeće i na osnovu toga daje zaposlenima zadatke da urade određeni posao, dok on uglavnom probleme rešava preko telefona, e-pošte ili u neposrednom susretu, preko sastanaka u zemlji i inostranstvu. Dalje, pod definisanjem strateških ciljeva podrazumeva se to da menadžment uvek planira unapred i gleda da uloži sredstva u onom pravcu koji bi, prema njegovom dugogodišnjem preduzetničkom iskustvu, trebao da mu donese dobit. Tu postaje jasno zašto je vlasnik sa funkcijom menadžera ključna karika u donošenju odluka kada je poslovanje firme u pitanju. On, takođe, prati zahteve tržišta i na osnovu toga zaposlenima izdaje radne zadatke.

Kao glavni problem u privredi malih i srednjih preduzeća u Srbiji može da se navede to da ne postoji razvijeno istraživanje tržišta i njegovih potreba, već se informacija o tome šta je aktuelno dobija kroz kontakt sa poverljivim izvorima iz vlasnikove mreže saradnika, što može biti predmet napada.

Treba još napomenuti da je u srpskom biznisu vrlo bitno da se prođe proces serifikacije, odnosno da se dobije uverenje da su poslovanje, kao i kvalitet usluga i proizvoda na jednom nivou koji je definisan kao zahtevan za to tržište. Takođe, važno je naglasiti da sertifikacija ne obuhvata sigurnost informacionih sistema.

3. CYBER RIZICI U POSLOVNOM OKRUŽENJU

Ono što se pokazalo kao zabrinjavajuće u poslovnoj praksi Srbije je to što većina malih i srednjih preduzeća beleži potpuno odsutvo cyber procedura. Pod cyber procedurom podrazumevamo sistematizovani skup znanja i iskustva koji ima za cilj da reši neku cyber situaciju, ali i da drži proces rada zaposlenih pod kontinuitetom, dok se stanje ne sanira. Glavna svrha postojanja takve procedure je da zaštiti interese poslodavca, ali i da omogući zaposlenima bezbedan rad na računaru i internetu. Cyber procedura nastaje zbog realnih potreba koje se javljaju u poslu, dok se pod pojmom bezbednost obično podrazumeva proces održavanja prihvatljivog nivoa rizika u nekoj oblasti u praksi, a cyber procedura je upravo dokument koji ima za cilj da taj zahtev sprovede i realno.

Srpsko društvo je u poslednjih nekoliko decenija u priličnoj meri zahvaćeno korupcijom. Taj trend nije zaobišao ni privredu u našoj zemlji. Neretko se dešava da neko od zaposlenih deli poverljive informacije iz firme sa trećim licem i to u cilju sticanja lične koristi. Kao sredstvo komunikacije i razmene informacija u tim slučajevima u praksi se koriste cyber tehnologije. Cyber tehnologija podrazumeva korišćenje interneta, računara i mobilnih uređaja u cilju manipulisanja informacijama. Drugim rečima, validni dokazi da je neko vršio korupciju mogu upravo da se nađu u cyber okruženju. Iz tog razloga se uvođenje cyber procedura u poslovanje može videti kao ključna preventivna mera u borbi protiv korupcije u privredi Srbije.

U daljem tekstu se navode realni problemi koji se javljaju u poslu upravo zbog nedostatka dokumenta koji bi na sistematičan i sveobuhvatan način predstavio kako održavati rizik na prihvatljivom nivou. U praksi je cyber sistem često sredstvo rada od vitalnog značaja za funkcionisanje preduzeća i svaki gubitak ili zloupotreba informacija donosi štetu firmi. U društvu sa povećanim stepenom korupcije je čest i očekivan slučaj da delovanje nekoga od zaposlenih bude maliciozne prirode u odnosu na poslodavca. Neretko se dešava da zaposleni putem privatne pošte, privatnih kontakata na Skajpu, mobilnih uređaja ili prilikom ličnih susreta iznose poverljive informacije iz firme, čineći iste dostupnim konkurenciji ili na crnom tržištu. Da bi se stepen rizika u odnosu na ove situacije držao na prihvatljivom nivou, odnosno da bi se zaštitili interesi poslodavca i obezbedio proces rada zaposlenih, potrebno je preduzeti odgovarajuće preventivne i kontrolne mere.

Tu se, u okviru preduzća, podrazumeva provera rada komunikacionih linija svih zaposlenih, periodično prikupljanje podataka od zaposlenih za poslovnu inteligenciju, edukacije radnika, pažljiva selekcija novih kadrova, itd. Posebno je interesantno objasniti pojam prikupljanja podataka za poslovnu inteligencije. U bezbednonosnim krugovima se pod inteligencijom podrazumeva informacija na koju je primenjena određena analiza. U ovom primeru se sugeriše da se periodično proverava stanje među zaposlenima pomoću vešto kreiranih upitnika, kvizova ili testova kako bi se proverilo kako funkcionišu u datom aspektu posla, kao što je budnost u cyber smislu. Samo na ovaj način cyber

rizik u poslovanju može da se održava na kontolisanom nivou.

4. ZNAČAJ DOBRE STRATEGIJE KONTINUIRANOG POSLOVANJA

Kako se u poslovnoj praksi malih i srednjih preduzeća Srbije neretko dešavaju cyber incidenti [6, 11], potrebno je i uprkos poteškoćama obezbediti da poslovanje firme teče bez zastoja, odnosno da vremenski gubici budu što manji. To se postiže primenom dobre strategije kontinuiranog poslovanja. Kontinuirano poslovanje se odnosi na svaku operaciju ili funkciju koja se izvršava sa ciljem da se podrže aktivnosti vezane za prevenciju gubitka, odgovora na krizu, oporavka od tehničke katastrofe, itd. To je sposobnost da organizacija obezbedi proizvode i usluge svojoj zajednici i da održava svoje poslovanje pre, za vreme i posle ometajućeg događaja.

Poznato je da u poslovnom svetu vreme znači novac, te je, stoga, u praksi potrebno potrošiti što manje vremena na otklanjanje eventualnih problema u funkcionisanju informacionih sistema. Plan oporavka treba da ponudi optimalno rešenje koje bi bilo prihvatljivo i sa tehničke i sa ekonomske tačke gledišta. S druge strane, strategija kontinuiranog poslovanja treba da se oslanja na plan oporavka i da obezbedi da se radni proces obavi uz minimum zastoja, jer veći zastoj znači veće finansijske gubitke za to preduzeće.

Idealan slučaj bi bio kada bi se cyber incident izbegao u potpunosti, ali to je u praksi teško izvodljivo ako su napadači posebno motivisani da napadnu i izvuku informacije iz malog ili srednjeg preduzeća i time ostvare određenu korist za sebe. Drugim rečima, kako je cyber napad postao nešto što može svakoga da zadesi, potrebno je razmišljati o merama koje bi omogućile da firma to preživi. Cyber procedura je dobra mera, ali u preventivnom smislu, jer smanjuje stepen rizika da do incidenta uopšte dođe. Međutim, ako se ipak i desi nešto neplanirano, tada se primenjuje plan oporavka i strategija kontinuiranog poslovanja čiji značaj i vidimo u takvim situacijama.

5. MERE SPAŠAVANJA PODATAKA ZA VREME I POSLE INCIDENTA

Kada se u praksi desi cyber incident, potrebno je postupiti po nekom planu koji bi obezbedio da se data situacija reši na što racionalniji način. Ono što se prvo uočava kada poslovna mreža postane zatrpana malicioznim softverom je da je potrebno (1) očistiti dati sistem od malicioznog softvera koji, u tehničkom smislu, preuzima kontrolu nad slabostima u aplikacijama i operativnom sistemu i tako nanosi štetu sistemu, a zatim i (2) reinstalirati operativne sisteme i softver na svim računarskim jedinicama, da bi se (3) na kraju informacije povratile iz nekog od *back up* izvora pomoću kojih se periodično i vrši čuvanje važnih podataka iz firme.

Drugim rečima, da bi se što racionalnije sproveo plan oporavka i omogućio kontinuitet u poslovanju malog i srednjeg preduzeća, potrebno je da firma raspolaže (1) tehnologijom koja će da garantuje izvršenje mera spašavanja, (2) ljudima koji će da sprovedu date mere i (3) procesom koji će da obezbedi kontrolisano sprovođenje mera.

Pod tehnologijom se u ovom slučaju podrazumeva softver za uklanjanje malware-a, instalacioni diskovi, alat za back up-ovanje i slično. Dalje, ljudski resursi su ti koji treba da imaju znanje i veštine i da osiguraju da će data tehnologija biti pravilno upotrebljena, dok sam proces može da bude vešto napisan plan ili procedura po kojoj će se spašavanje podataka i organizovati.

U praksi je potrebno do detalja razraditi plan zaštite podataka, kao i sve neophodne mere, jer samo tako će stepen improvizacije u rešavanju te realne situacije biti minimalan, a samim tim će se izbeći bilo kakva greška koja može još više finansijski da ugrozi malo i srednje preduzeće.

6. ZAKLJUČAK

Svrha ovog rada je da bude korisna dopuna već postojećoj literaturi iz cyber bezbednosti i time obezbedi pregled iz prakse stručnjacima iz Srbije. U ovom radu su ilustrovani problemi koji se javljaju u cyber okruženju, posebno bitni za mala i srednja preduzeća u Srbiji. Interesantno je napomenuti da su mere zaštite računara i mreže u našoj zemlji još uvek slabo razvijene, te stoga vidimo ovaj rad kao nastojanje da se učini korak napred u tom smislu.

LITERATURA

[1] Lillian Ablon, Martin C. Libicki, Andrea A. Golay, Markets for Cybercrime Tools and Stolen Data, RAND Corporation, 2014

[2] B. Burr, J. S. Hash, Techniques for System and Data Recovery, ITL Bulletin, 2002

[3] Booz Allen Hamilton, Cyber Operations Maturity Framework: A Model for Collaborative, Dynamic Cybersecurity, 2011

[4] Scott Charney, Rethinking the Cyber Threat: A Framework and Path Forward, Microsoft, 2009

[5] H. Hoang Ngo, X. Wu, P. Dung Le, C. Wilson, and B. Srinivasan, Dynamic Key Cryptography and Applications, International Journal of Network Security, 2010

[6] S. Nikić, Njačešće metode napada cyber kriminalaca i kako se odbraniti, ZITEH '10, 2010

[7] Juniper Networks Perspectives on RAND Corporation's Report, From Underground City to Thriving Metropolis: An Economic Analysis of the Cyber Black Markets, 2014

[8] A. Omari, B. Al-Kasasbeh, R. Al-Qutaish and M. Muhairat, DEA-RTA: A Dynamic Encryption Algorithm for the Real-Time Applications, INTERNATIONAL JOURNAL OF COMPUTERS, 2009

[9] L. Ožegović, N. Pavlović, Menadžment malih i srednjih preduzeća nosilac razvoja privrede, Škola biznisa, 2012

[10] H. Hoang Ngo, X. Wu, P. Dung Le, C. Wilson, and B. Srinivasan, Dynamic Key Cryptography and Applications, International Journal of Network Security, 2010

[11] V. Urošević, S. Uljanov. R. Vuković, Policija i visokotehnološki kriminal - primeri iz prakse i problemi u radu MUP-a Republike Srbije, ZITEH '10, 2010

[12] Gregory B. White, The Community Cyber Security Maturity Model, Proceedings of the 40th Hawaii International Conference on System Sciences, 2007

SUMMARY

HOW TO MAINTAIN A BUSINESS CONTINUITY DESPITE CYBER INCIDENTS?

Modern IT systems can bring a lot of advantages in terms of electronic commerce and governance as well as an automatic process control within industry, traffic and the other ways of classical and critical infrastructure. However, beside many advantages regarding technological development, there are also some drawbacks in sense of cyber risks, threats and the real hacker's attacks. In this article, we plan to deal with all these cyber risks caused by IT incidents and emergency situations that are capable to threaten a business continuity within big companies as well as medium and small enterprises.

Key words: *cyber, continuity, business, industry, economy, hacking, etc.*