Cyber procedure za poslovno okruženje u Srbiji

MILICA D. EKI, Subotica

Stručni rad

UDC: 004.041:005.922.1(497.11)

004.738.5.056

DOI: 10.5937/tehnika1603471D

Na osnovu iskustava iz prakse, postalo je jasno da mala i srednja preduzeća u Srbiji, kao i predstavništva nekih inostranih kompanija pokazuju ogromne nedostatke ili čak potpuno odsustvo procedura kada je cyber bezbednost u pitanju. U poslovnom okruženju naše zemlje se uočava potreba za sveobuhvatnim i sistematizovanim dokumentom koji bi ponudio rešenja za neke situacije iz prakse, a koji bi bio u skladu sa interesima poslodavca i obezbeđivao siguran rad zaposlenih. U ovom pregledu ćemo pokušati da definišemo osnovne smernice kada je reč o cyber proceduri.

Ključne reči: cyber procedura, prevencija, kontrola, zaštita, itd

1. UVOD

Da bi posao u okviru neke radne organizacije bio obezbeđen i da bi rad zaposlenih tekao neometano, u preduzeću ima li je rad vitalno zavisao od različitih unarskih jedinica, potrebno je da se prate određene procedure u radu na različitom internetu. 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 kontrolom.

Ono što treba da bude glavni zahtev za svaku cyber službu je da cyber procedure moraju, pre svega, da budu u skladu sa interesima poslodavca, ali i da imaju sposobnost da ponude bezbedan rad zaposlenih u okviru preduzeća.

U daljem tekstu ćemo pokušati da identifikujemo kritične tačke u cyber okruženju i da damo smernice kako mogući problemi treba da se prevaziđu.

2. IZNOŠENJE POVERLJIVIH INFORMACIJA IZ FIRME

Poverljivi podaci iz preduzeća mogu da se iznesu na više različitih načina. Veliki je problem ako preduzeće nema bezbedonosne provere i ako pušta nepouzdanu ljude u svoj sistem. Takvi maliciozni subjekti mogu da zloupotrebe svoj položaj i da na crno tržište ili konkurenciji iznesu poverljive podatke. Grafički prikaz metoda iznošenja poverljivih podataka je dat na slici 1.

Slika 1 - Iznošenje poverljivih informacija iz firme

U daljem tekstu ćemo navesti na koje iznošenja vrednih informacija iz preduzeća, kao i moguće mere prevencije:

Putem email komunikacije

Nije redak slučaj da zaposleni imaju otvorene naloge na nekom od javnih mail servisa i da na taj način iznose ili primaju razne informacije koje bi mogle da nanese štetu njihovom poslodavcu.

Mera prevencije

Kako baš nije prikladno da poslodavac proverava privatnu email komunikaciju svojih zaposlenih bez nekog posebnog razloga i kako se do informacije o tome ko je maliciozni subjekt u kolektivu dolazi putem neke prijave, jedino što ostaje kao mera prevencije je to da se zaposlenima izda uputstvo kako treba da se ponašaju na radnom mestu u cyber smislu i da se uvedu rutinske kontrole u vidu anketa za prikupljanje inteligencije kojima će se redovno proveravati stanje među zaposlenima.

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

Rad primljen: 27.12.2015.

Rad prihvaćen: 24.02.2016.

Putem chat-a na mail servisu ili društvenoj mreži

Neretko se dešava da zaposleni održavaju privatnu komunikaciju preko nekih od chat-ova koji su dostupni na servisima kao što su Gmail, Facebook i sli. no. Na taj na in mogu da se iznesu poverljivi podaci poput lozinki, trenutne situacije u kolektivu, itd.

Mera prevencije

I ovde, baš kao u prethodnom slučaju, nije moguće tako lako doći do informacije ko to radi, ali se, takođe, preporučuje da se zaposlenima izda upustvo da ne pokušavaju sa takvim aktivnostima i da se, s vremena na vreme, proverava situacija u firmi kroz rutinske kontrole.

Putem privatnih kontakata na Skype-u

esto se dešava da zaposleni imaju privatne kontakte na svom poslovnom Skype nalogu. To može da bude rizik po poslodavca, pogotovo ako su ti kontakti nepouzdati.

Mera prevencije

I u ovom slučaju je potrebno izdati neku vrstu uputstva, a kontrola bi mogla da se vrši tako što bi se poslodavac, s vremena na vreme, logovao u poslovni Skype zaposlenog i proveravao stanje na istom.

Putem mobilnih uređaja

Poverljive informacije iz firme mogu da se iznesu čak i pomoću mobilnih telefona, PDA uređaja, prenosivih računara i sli. no.

Mera prevencije

Kako u današnje vreme nije baš prikladno da se svakom zaposlenom kontroliše mobilni uređaj koji nosi sa sobom na posao, kao mera prevencije treba uvesti upustvo koje bi bilo usklađeno sa odgovarajućim smernicama. Takođe, situacija na terenu može periodično da se proverava putem rutinskih anketa za prikupljanje inteligencije.

Putem ličnih susreta

Ukoliko je poslodavac primio na posao neproverenu osobu, ona vrlo lako preko svojih privatnih kontakata iz ličnog života može da iznese poverljive podatke na nekom od memorijskih uređaja, hartiji ili putem usmene komunikacije.

Mera prevencije

Ovaj slučaj je u praksi prilično teško proveriti, te se s toga preporučuje da se kao mera prevencije primeni upustvo i da se kroz rutinske kontrole u vidu prikupljanja inteligencije proverava stanje u kolektivu.

3. METODE SPROVOĐENJA CYBER KONTROLE U PREDUZEĆU

Kako bi se rizik u cyber smislu u okviru nekog preduzeća održavao na prihvatljivom nivou, potrebno je,

s vremena na vreme, da se sprovedu cyber kontrole. Cyber kontrola treba da garantuje da se interesi poslodavca budu zaštićeni u svakom trenutku, ali i da se svi zaposleni budu sigurni u cyber smislu.

U daljem pregledu ćemo navesti neke od mogućih mera koje u tom smislu mogu da se primene. Grafički prikaz spomenutih mera je dat na slici 2.

Slika 2 - Metode sprovođenja cyber kontrole u preduzeću

Provera poslovne email komunikacije

U praksi je potrebno, s vremena na vreme ili čak stalno, proveravati poslovne email naloge zaposlenih. Na taj način, ne samo da mogu da se otkriju bezbedonosni rizici, već i da se proverí radna disciplina i na in na koji komuniciraju zaposleni u poslovnom smislu.

Provera komunikacije pomoću Skype-a

Skype neretko može da bude mesto na kome može da se bezbedonosno ugrožavaju zaposleni, ali i mesto raznih zloupotreba kao što je iznošenje poverljivih informacija iz firme. Iz tog razloga, potrebno je uvesti rutinske kontrole Skype naloga zaposlenih kako bi rad zaposlenih, ali i funkcionisanje kompanije bili bezbedni.

Provera zaštitenosti mrežne komunikacije

Neretko se dešava u praksi da mrežna komunikacija ne funkcioniše kako treba, odnosno da podaci sa svih računara u mreži ne idu u centralni sistem, bilo zbog greške na nekoj od računarskih jedinica, bilo zbog namere nekog od zaposlenih da zaštiti svoju privatnost.

U svakom slučaju, to je u sukobu interesa sa poslodavcem kome su potrebni ti podaci kako bi u svakom trenutku mogao da dokaže svoju validnost u legalnom smislu. S tim u vezi, potrebno je vršiti rutinske kontrole rada mreže.

Rutinsko prikupljanje inteligencije

Preporuka je da se periodično sprovedu ankete, ispitivanja ili kvizovi sa pažljivo pripremljenim pitanjima čiji odgovori se tumače po ključu i da se na taj način proverava situacija u okviru kolektiva. Ovim vidom kontrole mogu da se provere razni parametri u poslovanju, a ne samo mogući cyber rizici i brige.

4. METODE PREVENTIVNOG DELOVANJA U PREDUZE U

U cilju sprovođenja mera prevencije potrebno je sprovesti aktivnosti sa slike 3 kako bi se spre ili eventualni cyber problemi.

Slika 3 - Metode preventivnog delovanja u preduze u
Pravne preporuke o cyber zaštiti

Kao osnovni vid preventivne zaštite u cyber smislu može da se izdvoji davanje i pravne preporuke koje treba da obezbede pravilno poslovanje i smanjen nivo rizika koji može da bude posledica nepažljivog rada zaposlenih.

Preporuke se u praksi odnose na sledeće elemente cyber zaštite:

Preporuka o odabiru lozinke

U praksi se pokazalo da je jedan od ključnih uslova dobre cyber zaštite upravo pametan odabir lozinke. Lozinka ne treba da bude slabog tipa i pogodna za upad raznih hakera, već mora da bude jaka i da se ažurira periodično.

Drugi rešenje ima, treba da sadrži kombinaciju raznih znakova, da ne uključuje podatke kao što su ime zaposlenog ili njegov datum rođenja i da se menja u određenim vremenskim intervalima, kako bi se obezbedila što pouzdanija zaštita.

Preporuka o ne stupanju u kontakt sa neproverenim licem

esto se dešava da su zaposleni u nekoj firmi meta kompromitovanja od strane raznih malicioznih subjekata i tada te osobe pokušavaju da zloupotrebe njihovo ime i reputaciju u cyber smislu i tako steknu određenu prednost u svoju korist. Jasno se preporučuje zaposlenima da svaki kontakt sa neproverenom osobom odbiju.

Preporuka o prijavljivanju incidenta nadležnom licu

Ukoliko dođe do cyber incidenta, jasno se preporučuje da zaposleni prijavi isti nadležnom licu, a ono dalje da istraži taj slučaj.

Poštovanje zabrana vezanih za cyber okruženje

Pored ovoga, potrebno je uvesti i neke od zabrana u svakodnevnu poslovnu praksu. Data mera ima za cilj sprečavanje svakog vida zloupotrebe na radnom mestu i ugrožavanja interesa poslodavca, ali i bezbednosti ostalih zaposlenih.

Zabrana o deljenju poverljivih informacija sa trećim licem

Veliki problem za svakog poslodavca može da predstavlja zloupotreba poverljivih informacija od strane njihovih zaposlenih, jer se tako vrši korupcija i moguće curenje podataka na crno tržište. U ovaj vid zaštite mogu da se uključe sledeće vrste zabrana:

- Zabrana o zloupotrebi mobilnih uređaja,
- Zabrana o zloupotrebi komunikacionog softvera,
- Zabrana o svakom vidu zloupotrebe prilikom ličnog susreta, itd.

Edukacija zaposlenih u cyber smislu

Kako bi budnost zaposlenih u firmi bila na što višem nivou, potrebno je da poslodavac kontinuirano organizuje razne vidove obuka, seminara i edukacija o cyber zaštiti.

Prevencija u vidu anti-malware zaštite

Bezbedonosno stanje u cyber prostoru svakog radnog unara i aktivne mreže se najbolje kontoliše tako što svaka radna unarska jedinica mora da ima anti-malware program koji je u današnje vreme prilično dobar na in prevencije u cyber smislu.

Sprečavanje ulaska malicioznog zaposlenog u sistem poslodavca

Kao poslednja mera preventivnog delovanja u okviru firme, može da se vidi sprečavanje poslodavca da zasnuje radni odnos sa licem koje bi moglo da bude bezbedonosni problem i da kompromituje to preduzeće. S tim u vezi, predlaže se pažljivo osmišljavanje sistema selekcije koji ne bi dozvolio da neprovereno lice uopšte uđe u kolektiv i dobije pristup poverljivim podacima.

5. OBEZBEĐIVANJE POVERLJIVOSTI MAKAR JEDNE KOMUNIKACIONE LINIJE

U praksi je esto potrebno da makar jedna od korišćenih linija poseduje određeni stepen poverljivosti. Pojam komunikacione linije se odnosi na e-poštu, Skype, mobilne uređaje i slično. Kao najbolji primer za poverljivu komunikacionu liniju se navodi korišćenje email naloga na principu Gmail-a kod kojih je vrlo jednostavno podesiti bezbednost e-pošte.

Ono što je potrebno uraditi u tom slučaju je da se definiše kao jedini poverljiv, odnosno da se samo sa tog radnog unara u korisni kom smislu može

proveravati dati email nalog, dok opcija da neko može da skida poštu sa tog naloga treba da bude onesposobljena. Grafički prikaz ovog procesa je dat na slici 4.

Slika 4 - Obezbeđivanje poverljivosti komunikacione linije

Ako se poslovni email definiše kao poverljiv samo za računarsku jedinicu u kancelariji i ako se u radnom okruženju uvede pravilo da poslovna pošta može da se proverava samo na poslu, dok je, zabranjeno raditi bilo šta od kuće, jasno je da kontrola za ovu meru može da se vrši tako što bi telefonska poruka o svakom neovlašćenom logovanju u e-nalog van firme stizala nadležnom licu, koje je pre toga izdalo odgovorajuću zabranu.

6. DISKUSIJA

Treba napomenuti da je svrha ovog rada da kroz praktične primere ilustruje kako cyber situacije izgledaju u praksi, ali i da sa smernice kako sva ta znanja i iskustva da se sistematizuju u smislu kreiranja cyber procedure koja bi našla svoje primene u poslovnom svetu Srbije. Iskreno se nadamo da će ovaj dobitnik i na odziv stručne javnosti u našoj zemlji i da će istim biti u njen korak napred u pristupu praktičnim problemima.

7. ZAKLJUČAK

Ovaj stručni rad predstavlja nastojanje da se na što jasniji i sveobuhvatniji način da pregled iz prakse

vezan za bezbednost računara i interneta, kao i da se sugeriše značaj i potreba za cyber procedurama u poslovnom okruženju Srbije.

LITERATURA

- [1] Lillian Ablon, Martin C. Libicki, Andrea A. Golay, Markets for Cybercrime Tools and Stolen Data, Sponsored by Juniper Networks, 2014.
- [2] B. Burr, J. S. Hash, Techniques for System and Data Recovery, ITL Bulletin, 2002.
- [3] Scott Charney, Rethinking the Cyber Threat: A Framework and Path Forward, Microsoft, 2009.
- [4] Stephen Cobb, Four basic and effective defensive measures against cybercrime, Tech Brief, ESET Business Solutions, 2014.
- [5] Sam Curry, Engin Kirda, Eddie Schwartz, William H. Stewart, Amit Yoran, Big Data Fuels Intelligence-driven Systems, RSA Security Brief, EMC, 2013.
- [6] T. Mahmood, U. Afzal, Security Analytics: Big Data Analytics for Cybersecurity, 2013 2nd National Conference on Information Assurance (NCIA), 2013.
- [7] Mark Mateski, Cassandra M. Trevino, Cynthia K. Veitch, John Michalski, J. Mark Harris, Scott Maruoka, Jason Frye, Cyber Threat Metrics, Sandia National Laboratories, 2012.
- [8] R. Schell, Security – A Big Question for Big Data, 2013 IEEE International Conference on Big Data, 2013.
- [9] Shirley C. Payne, A Guide to Security Metrics, SANS Institute, 2007.
- [10] Moira J. West-Brown, Don Stikvoort, Klaus-Peter Kossakowski, Georgia Killcrece, Robin Ruefle, Mark Zajicek, Handbook for Computer Security Incident Response Teams (CSIRTs), U.S. National Science Foundation (NSF), 2003.

SUMMARY

CYBER PROCEDURES FOR A BUSINESS ENVIRONMENT IN SERBIA

Through a practical experience, it is getting clear that medium and small enterprises as well as some foreign companies in Serbia suffer the serious lack of cyber security procedures. In a business environment of our country, there is a strong need for a comprehensive and systematized document that would suggest how to resolve any cyber situation from the practice. The document would comply with employer's interests and assure a secure working process of employees, at same glance. In this overview, we will attempt to define basic guidelines in sense of cyber procedures.

Key words: cyber procedure, prevention, control, protection, etc