"PRISTUP INFORMACIJSKOJ SIGURNOSTI U POSLOVNIM SISTEMIMA - STUDIJ SLUČAJA"

"APPROACH TO INFORMATION SECURITY IN BUSINESS SYSTEMS - CASE STUDY"

Džemal Kulašin, prof.dr.
Fakultet za menadžment i poslovnu ekonomiju
Kiseljak

Nezir Huseinspahić, prof.dr.
Zavod zdravstvenog osiguranja SBK
Travnik

REZIME
Primarni cilj rada je da ukaže na sve izraženiji problem informacijske sigurnosti u poslovnim sistemima, koji postaje uvjetom njihovog uspješnog funkcioniranja. U prvom dijelu rada, elaboriraju se pristupi informacijskoj sigurnosti u poslovnoj praksi, koji se potom grubo distanciraju na tzv. parcijalan i cjelovit pristup. U drugom dijelu rada predstavljaju se rezultati anketiranja jednog poslovnog sistema sa područja SBK, kako bi se jasnije karakterizirao pristup informacijskoj sigurnosti u našoj poslovnoj praksi.

Ključne riječi: informacijska sigurnost, sistem informacijske sigurnosti, poslovni sistemi

SUMMARY
The primary aim of the paper is to point to the increasingly prominent problem of information security in business systems, which becomes a condition for their successful functioning. In the first part of the paper, information security approaches are elaborated, which roughly distance themselves to the so-called partial and complete approach. The second part of the paper presents the results of surveying a business system from the SBK area in intention to better characterize the access to information security in our business practice.

Keywords: information security, information security system, business systems

1. UVOD

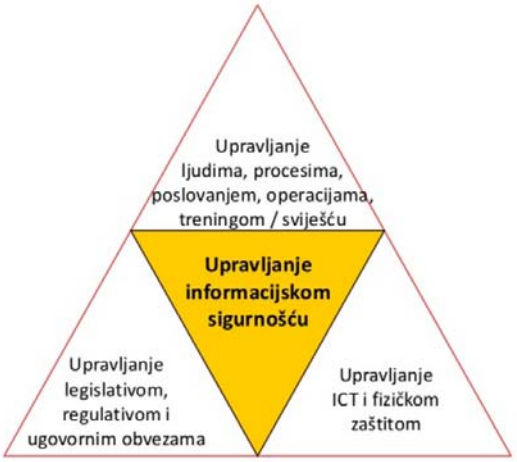
Kako je savremeno poslovanje postalo potpuno ovisno o informacijsko-komunikacijskim tehnologijama, dramatično su porasle i sigurnosne ranjivosti zbog čega se potencijalni korporativni sigurnosni rizici premještaju iz sfere tzv. tradicionalnih rizika (prirodne katastrofe, konkurencija itd.) u sferu tzv. netradicionalnih problematičnih događaja, u prvom redu *cyber incidente*.

Stoga je začuđujuće da još uvijek značajan broj kompanija nema konkretnu strategiju u borbi protiv cyber kriminala, niti odgovarajuće sigurnosne protokole koje treba slijediti. Tako, prema

istraživanju na uzorku od 9500 ispitanika pozicioniranih u IT sektoru različitih kompanija u 122 zemlje svijeta, gotovo polovina svih anketiranih kompanija (44%) nema konkretnu sigurnosnu strategiju, dok čak više od polovine kompanija (54%) nema sigurnosni protokol koji treba slijediti u slučaju da dođe do cyber napada [2].
Ipak, u značajnom broju kompanija porasla je svijest o razmjerama sigurnosnih rizika, gdje implementiraju potrebne i adekvatne mjere kako bi zaštitili obimnu informacijsku infrastrukturu. U tom cilju, implementiraju i sistem upravljanja informacijskom sigurnošću (eng. ISMS - Information Security Management System), mahom na podlogama standarda ISO 27001. Da se zaista radi o veoma znakovitom trendu, potvrđuje činjenica da je ISO 27001 najbrže rastući sistem koji se implementira u svijetu (!), te je prema posljednjem dvogodišnjem oficijelnom *ISO Survey*-u[1] iz 2017. godine broj kompanija sa certifikatom koji normira informacijsku sigurnost u porastu za čak 21% [3].

2. SISTEM UPRAVLJANJA INFORMACIJSKOM SIGURNOŠĆU

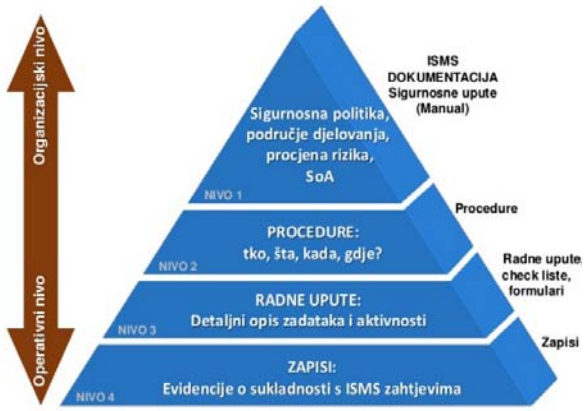
Sistem upravljanja informacijskom sigurnošću karakterizira promatranje organizacije u cjelini, uz sigurnosne mjere koje obuhvataju sve resurse informacionog sistema. Pri tome, izbor sigurnosnih mjera nije proizvoljan i incidentan, već je rezultat procjene rizika kao dijela procesa upravljanja rizikom. Praktično, radi se o procesnom pristupu informacijskoj sigurnosti, gdje se sigurnosnim mjerama obuhvataju tri široka područja, predstavljeno na Slici 1.



Slika 1. Područja upravljanja informacijskom sigurnošću

Treba naglasiti da je projekat implementacije ISMS-a složen i zahtjevan projekat, koji ishodište ima u jasnom i čvrstom opredjeljenju top menadžmenta a potom i na stalnim poboljšavanjima postojećeg sistema. Kao rezultat, uspješnim implementiranjem ISMS-a sigurnosni rizici svode se na projektovani prihvatljivi nivo, jer se harmonizira složeni organizacijski sistem zaštite tajnosti, integriteta i dostupnosti podataka, tzv. C-I-A sigurnosni triangl[2]. Takav sigurnosni sistem je i potpuno dokumentiran shodno zahtjevima standarda ISO 27001 - ako se implementira prema podlogama ovog međunarodnog standarda, pri čemu postoji jasna hijerarhija sigurnosne dokumentacije (Slika 2) [1].

[1] https://www.iso.org/the-iso-survey.html [pristup: 22.03.2019]
[2] C-I-A sigurnosni triangl: Confidentiality (Tajnost), Integrity (Integritet), Availability (Dostupnost)



Slika 2. Nivoi sigurnosne dokumentacije ISMS-a

Prema iskustvima brojnih svjetskih kompanija, krajnjim certificiranjem ISMS-a prema ISO/IEC 27001 stječu se brojne prednosti, kako interne, tako i eksterne, što ne samo da maximalizira nivo sigurnosne zaštite, već poboljšava i ukupnu organizacijsku učinkovitost [5] Na žalost, ovakav cjelovit pristup nije dominantan u našoj poslovnoj praksi, što potvrđuje i broj certifikata ISO 27001 koje imaju kompanije u Bosni i Hercegovini. Naime, zaključno sa 2017. godinom, broj ISO 27001 certifikata iznosio je svega 27, što predstavlja veliki zaostatak u odnosu na druge zemlje; npr. Češka ima 463 kompanije sa certifikatom ISO 27001, Mađarska 472, Italija 958, Njemačka 1.339, Japan 9.161 itd.

3. SIGURNOSNI PRISTUP IZ NAŠE POSLOVNE PRAKSE

Ogledni primjer korporativnog pristupa informacijskoj sigurnosti je respektabilan poslovni sistem sa područja Srednjobosanskog kantona[3], anketiran u smislu pristupa informacijskoj sigurnosti. Kompanija je, inače, certificirana prema međunarodnim standardima ISO 9001 i ISO 14001, ali izostaje certifikat informacijske sigurnosti ISO/IEC 27001. Kako anketirana kompanija nema (pod)sistem upravljanja informacijskom sigurnošću, nema niti dokumentiranu sigurnosnu politiku i fokus je na segmentima a) programske zaštite i b) zaštite podataka.

U tom cilju poduzimaju veći niz aktivnosti, odnosno procedura i postupaka kako sigurnosni incidenti ne bi doveli do uništenja i/ili nepravilnog korištenja podataka. Pri tome, mjere zaštite određene su shodno vrsti podataka i informacija koji se žele zaštititi. Pored tehničkih rješenja, najvažnija stvar koju ističu su djelatnici, odnosno ljudski faktor, posebno IT tim koji vrši redovne kontrole i nadzor sistema zaštite.

Prijetnje informacijskoj sigurnosti promatraju iz više izvora, a kao najvažnije ističu:

- Prirodna katastrofa (strujni udar, poplava, požar, zemljotres),
- Fizički kvar opreme zbog dotrajalosti ili neispravnosti neke komponente,
- Kvar opreme zbog nepravilnog održavanja i korištenja,
- Namjeran kvar opreme (sabotaža),
- Namjerno brisanje podataka,
- Nesavjesno i nemarno ponašanje ovlaštenih korisnika,
- Neovlašteno korištenje podataka, tj. zloupotreba podataka.

Shodno prijetnjama, zaštitu podataka dijele u dvije osnovne grupe:

a) Zaštita podataka od slučajnog/(ne)namjernog uništenja podataka, i

[3] Economic, Vitez

b) Zaštita/kontrola pristupa podacima od mogućeg neovlaštenog korištenja i zloupotrebe odnosno namjernog uništenja.
Daljnju vrstu i načine zaštite podataka definiraju prema glavnim parametrima, svrstanim u sljedeće grupe:

- Grupa I. Postavljanje **cilja i vrste** zaštite podataka: S obzirom na vrstu i djelatnost organizacije postavlja se i ciljna vrsta zaštite. Ona je različita po više osnova ovisno o vrsti subjekta kojem je potrebna. Naime, nije isto izvršiti zaštitu podataka vezanih za spisak knjiga neke biblioteke i osobnih podataka iz zdravstvenog kartona pacijenata bolnice, na primjer.
- Grupa II. Postavljanje potrebnog **stepena sigurnosti** zaštite podataka: Prema vrsti subjekta za kojeg se pravi zaštita podataka, postavlja se i nivo sigurnosti zaštite. Vrši se procjena koliko su podaci važni pa prema izvršenoj procjeni određuje se i postavlja potreban stepen sigurnosti zaštite.
- Grupa III. Određivanje **veličine i obima** zaštite podataka: Prema procijenjenoj količini podataka određuje se i odgovarajuća vrsta zaštite, odnosno koliko i kakvih resursa je potrebno da bi se izvršila potrebna zaštita. Nakon što se odrede glavni parametri zaštite, u okviru osnovne podjele podataka određuju se daljnji načini i vrsta zaštite podataka. Redovna zaštita se vrši u unaprijed određenim vremenskim terminima. Povremena i vanredna zaštita se radi po potrebi, gdje su glavni razlozi ovih mjera migracija podataka sa jednog na drugi server, fizičko premještanje informatičke opreme odnosno servera te razni godišnji obračuni i sravnjivanja stanja.

3.1. Osnovni načini i postupci zaštite podataka

U anketiranom poslovnom sistemu provode se određeni osnovni načini i postupci zaštite podataka. Osnovni načini i postupci zaštite koje ističu su:

- Redovno kopiranje važnih podataka od strane korisnika na externi medij za pohranu podataka (npr. snimanje podataka na stick odnosno optički medij DVD/CD);
- Redovno kopiranje važnih podataka od strane korisnika na externi medij za pohranu podataka koji se nalazi na izdvojenoj lokaciji; prenos podataka se vrši kroz mrežu, npr. na mrežni disk koji se nalazi na drugoj lokaciji korisnik snima podatke u prostor (folder) koji mu je unaprijed određen od strane IT administratora;
- Snimanje baze podataka na principu "otac-sin"; metoda koja se koristi jako dugo u velikim centrima za obrade podataka; svaki dan se snima baza podataka i odlaže na određeno mjesto; npr. “današnja” zaštita se odlaže na sigurnoj lokaciji i to na mjesto "sin", dok se “jučerašnja” zaštita premješta na lokaciju "otac"; na taj način ima se slijed punih zaštita u zadnja dva dana;
- Zaštita/backup baze podataka se automatski vrši svaki dan na drugi elektronički medij - (data centar); procedure koje vrše kontrolu rada servera i centralne baze podataka u unaprijed zadanom terminu vrše automatski backup/zaštitu baze;
- Normalan i redovan rad centralne baze podataka se odvija u ″mirror″ modu; na taj način istovremeno se podaci nalaze i obrađuju na dva ili više fizičkih jedinica, i ako jedna jedinica otkaže u slučaju kvara, redovan rad se nastavlja sa drugom kao da se ništa nije desilo;
- Povremeno/periodično pravi se backup podataka i arhiviraju i snimaju na optički ili externi magnetni medij; fizički mediji se sklanjaju na izdvojenu lokaciju kako bi se zaštitili od mogućih posljedica prirodne nesreće i katastrofe (požar, poplava, zemljotres);
- Ukoliko se planira vršiti migracija podataka (prenos na novi server) ili značajniji unos/izmjena podataka (npr. razlličiti popisi) vrši se vanredna zaštita podataka; tbog

važnosti podataka, višestruko se zaštićuju podaci kako na medije u lokalnoj mreži, tako i na izdvojenim lokacijama;
- Ograničen i kontroliran pristup centralnoj bazi podataka kroz dodjelu privilegija; na temelju dodijeljene šifre, korisnik ima pravo pristupa određenim podacima, opcijama (modulima i dijelovima programa) i manipulaciji s podacima (pregled, unos, izmjena, brisanje);
- Podjela prostora za podatke zajednički folder koji služe za razmjenu podataka (fajlova) podijeljeni su po interesnim grupama tako da grupi osjetljivih podataka pristupaju samo osobe koje imaju pravo pristupa tim podacima (npr. podacima vazanih za plaću mogu pristupati samo osobe koje imaju pravo pristupa jer su oni poslovna tajna);
- Automatska/manualna sinhronizacija podataka; provodi se redovno ili periodično, ovisno o potrebama.

3.2. Napredni načini i postupci zaštite podataka

U anketiranom poslovnom sistemu provode se određeni napredni načini i postupci zaštite podataka. Ovaj nivo zaštite odnosi se na podatke klasificirane u *strogo poslovna tajna* (financijske transakcije u bankama, poslovni i drugi ugovori u sudovima, osobni podaci građana u MUP-u). Napredni načini i postupci zaštite koje ističu su:

- Informatička oprema na kojoj se vrši obrada osjetljivih podataka nalazi se u zasebnim prostorijama koje su fizički kvalitetno i dobro osigurane.
- Ulaz u prostorije gdje se može izvršiti pristup podacima i njihova obrada imaju samo osobe sa posebnim ovlaštenjima i dozvolama za pristup;
- Sigurnosne kartice i ključevi koji omogućavaju pristup prostorijama, odnosno terminalima se nalaze pod kontrolom sigurnosnih službi. One vrše provjeru i identitet osoba koje mogu pristupiti povjerljivim podacima;
- Posebne intranet linije (lokalna mreža) koja ograničava vanjski pristup, ali osigurava pristup podacima više osoba (sve koje imaju dozvole i privilegije pristupa podacima);
- Posebne iznajmljene linije za komunikaciju i pristup.

3.3. Zaštita od zloupotrebe Interneta

U anketiranom poslovnom sistemu provode se i određene mjere zaštite od zloupotrebe Interneta. Mjere zaštite u ovom kontekstu koje ističu su:

- Pristup Internetu je ograničen i kontroliran korištenjem odgovarajućeg softvera za nadzor i kontrolu; konkretno, u funkciji je ZoneAlarm koji kroz sistem filtera vrši blokadu i zabranu pristupa podacima, kao i ograničenje pristupa samo određenim web lokacijama;
- Zaštita pristupa Internetu kroz firewall hardware;
- Uređaji za pristup Internetu (router-i) imaju kroz svoj sistem kontrolu pristupa i mogućnost zabrane/dopuštenja općeg pristupa Internetu te određenim stranicama;
- Antivirusni i antispam programi koji uključuju mnogobrojne filtere i zaštitu od nedozvoljenog pristupa;
- Blokada nepoželjne elektronske pošte koja inicijalno sadrži maliciozni software.

4. ZAKLJUČAK

Analizirajući teoriju i praksu u pristupu informacijskoj sigurnosti, u poslovnim sistemima općenito se determiniraju dva pristupa, parcijalan i cjelovit. Prvi pristup - **parcijalan**, karakterizira promatranje samo određenih resursa informacionog sistema, prema kojima se ustrojavaju i sigurnosne mjere. Drugi pristup - **cjelovit**, karakterizira proces i sistematičnost, gdje se organizacija promatra u cjelini, uz sigurnosne mjere koje obuhvataju sve resurse

informacionog sistema. Pritom, izbor sigurnosnih mjera nije proizvoljan i incidentan, već rezultat procjene rizika u procesu upravljanja sigurnosnim rizikom.
Kada je naša zemlja u pitanju, u praksi se susreću oba pristupa, parcijalan i cjelovit. Ipak, sudeći po malom broju certifikata ISO 27001 naših kompanija (prema posljednjem oficijelnom *ISO pregledu* - ukupno 27!), nije teško zaključiti da je prevaga na parcijalnom pristupu. Doduše, ovakav pristup donekle je i "iznuđen" kako skromnijim finansijskim mogućnostima naših firmi, tako i nepostojanjem odgovarajuće zakonske regulative na državnom nivou. Naime, treba naglasiti da je BiH jedna od rijetkih zemalja u kojima nije usvojen krovni Zakon o informacijskoj sigurnosti niti postoji tzv. CERT na nivou države kao najviši tim za borbu protiv cyber kriminala.

5. LITERATURA

[1] Adelsberger, Z. 2015, *Implementacija ISMS prema ISO /IEC 27001/2013*, ICT Security Kladovo, 14.-16.maj 2015, dostupno na: http://www.slideshare.net/dejanjeremich/adelsberger-zdenko-implementacija-iso27001-2013 [Pristup: 30.05.2018]

[2] ALLIANZ Zagreb d.d. za osiguranje, 2016, *Allianzov barometar rizika za 2016*, dostupno na https://www.allianz.hr/privatni-korisnici/press/objave-za-medije/allianzov-barometar-rizika-za-2016-godinu/ [pristup: 12.11.2017]

[3] Charlet, L., 2019, *ISO Survey*, dostupno na: https://www.iso.org/the-iso-survey.html [pristup: 22.03.2019]

[4] Deželić, V., 2017, *Velike tvrtke, organizacije iinstitucije neuspjevaju se pripremiti za cybernapade*, dostupno na: http://www.ictbusiness.info/internet/velike-tvrtke-organizacije-i-institucije-ne-uspjevaju-se-pripremiti-za-cyber-napade [pristup: 11.11.2017]

[5] IT Governance, 2016, *ISO 27001 Global report - 2016*, dostupno na: https://www.itgovernance.co.uk /download/ISO27001-Global-Report-2016.pdf [Pristup: 28.03.2019]