INFORMACIJSKA SIGURNOST U BOSNI I HERCEGOVINI

INFORMATION SECURITY IN BOSNIA AND HERZEGOVINA

Branka Mijić
Fakultet za kriminalistiku, kriminologiju i sigurnosne studije, Sarajevo, Bosna i Hercegovina

JEL kategorija: **D82, G32, L86**

Apstrakt

U današnje vrijeme informacijsku sigurnost najčešće povezujemo s raznim internetskim prijetnjama poput hakerskih napada, virusa ili raznih drugih aplikacija koje imaju funkciju da naprave štetu našem računalu, informacijskom sustavu, a samim tim i informacijama. Međutim, informacijsku sigurnost treba promatrati u širem kontekstu. Moguće nekontrolirano „curenje" važnih i vrijednih informacija izvan sustava predstavlja veliku prijetnju organizaciji, kompaniji. Možemo reći da informacije koje često mogu biti vrlo važne ili okarakterizirane kao tajne i povjerljive, nisu uvijek u elektronskom obliku, one mogu biti i u pisanim dokumentima, slikama, tablicama, grafikonima i sl. U današnje vrijeme, velika većina spomenutih informacija je u digitalnom obliku, te se tema ovog rada, odnosi na sigurnost informacija, rizicima, procjeni i upravljanju rizicima i zakonskim regulativama a sve u svrsi zaštite, odnosno, sigurnosti informacije i informacionog sustava, a za sve to je potrebna primjena standarda iz serije ISO27001.

***Ključne riječi**: informacijska sigurnost, procjena rizika, upravljanje rizikom, zakonske regulative i ISO 27001.*

Abstract

At present, information security is most commonly associated with various Internet threats such as hacking attacks, viruses, or various other applications that have the potential to harm our computer, information system, and even information. However, information security should be seen in a wider context. Possible uncontrolled "leak" of important and valuable information outside the system poses a major threat to the organization, the company. We can say that information that can often be very important or characterized as secret and confidential, not always in electronic form, can be in written documents, pictures, tables, charts, etc. Nowadays, most of the information mentioned is in digital form, the subject of this paper relates to the security of information, risks, risk assessment and risk management and legal regulations, all for the

Adresa autora:
Branka Mijić
brankica_mijic@net.hr

purpose of protection, respectively, information security and information system, and for all this it is necessary to apply ISO27001 standards.

***Keywords**: information security, risk assessment, risk management, legal regulations and ISO 27001.*

1 UVOD

U vrijeme snažnog utjecaja globalizacije teško je pronaći područje poslovanja koje nije pod utjecajem informacijskih tehnologija. Sukladno tome, informacijski sustavi postali su nezaobilazni u današnjem visoko integriranom društvu. Visoka razina primijenjenosti, te visoka razina integriranosti informacijskih sustava nameće sve češća pitanja sa aspekta sigurnosti informacija. Informacijski sustav i informacije su postali stalna meta kao unutar organizacije, tako i izvana. Razloga tome je jako mnogo, jedan od tih razloga je to da je cilj napada uništenje ili promjena izvornih podataka ili krađa istih. Od 2000. godine informacijska sigurnost se počela znatnije razvijati, radi zaštite istih. Svjetske organizacije su sve više svjesne činjenice da su informacijski podaci postali nesigurni, te su se počele baviti ovom problematikom.

Najčešći vidovi napada na računarske mreže, Internet, tipa su: prisluškivanje, lažno predstavljanje, napad tipa ukidanje servisa, ponavljanje poslanih poruka, pogađanje lozinke, kripto analiza, napadi tipa Trojanskog konja i virusi. Mogući načini odbrane od navedenih napada su sljedeći: šifriranje, primjena tehnologije digitalnog potpisa, procedura jake autentifikacije, korištenje jakih ključeva i česta izmjena ključeva, zaštita adresa servera, korištenje digitalnih certifikata kao jednoznačnih identificiranih parametara subjekata u komunikaciji, korištenje Smart kartica za generiranje digitalnog potpisa, više-nivovska virusna zaštita. (Sinkovski & Lučić, 2006)

Zbog toga mnoge tvrtke u svijetu posvećuju veliku pažnju zaštiti svojih informacija i informacijskoj sigurnosti primjenjujući ISO/IEC standard kao ključni element u upravljanju informacijskom sigurnošću. Informacijska sigurnost uključuje kako zaštitu informacijskog sustava, tako i samih informacija, bez obzira u kakvom obliku bile. Koncept informacijske zaštite je izuzetno širok, od tehničke mjere zaštite obuhvata i fizičku zaštitu, programske, logičke i administrativne mjere zaštite. Sve te mjere su propisane normama iz serije standarda ISO/IEC 27000.

Informacijska sigurnost je jako važna javnim i privatnim organizacija. Povezanost javnih i privatnih računalnih mreža i dijeljenje informacija otežava kontrolu pristupa informacijama. Upravljanje informacijskom sigurnošću zahtijeva sudjelovanje svih zaposlenika organizacije, a često je potrebna pomoć konzultanta izvan organizacije.

2 INFORMACIJSKA SIGURNOST

2.1 Pojam sigurnosti

Pleskonjić i dr. (Pleskonjić, Maček, Đorđević, & Carić, 2007) sigurnost definiraju kao proces održavanja prihvatljive razine, dok Hadjina (2013) i Krapac (1992) sigurnost opisuju kao proces smanjenja rizika ili vjerojatnosti nastajanja štete.

Sigurnost je osjećaj pojedinca da je zaštićen (*engl. safe, protected, secure, franc. sauf, njem. sicher, gesch tzt, gefahrlos*) od fizičke, društvene, duhovne, novčane, političke, ekonomske, osjećajne, profesionalne, psihološke, odgojne ili bilo koje druge prijetnje, ugroze, opasnosti, štete, povrede ili bilo kakvog događaja koji se može tumačiti kao neželjen. Isto tako, navodi da je sigurnost kontrola neizvjesnosti pri čemu se prepoznata opasnost svodi u granice prihvatljivog rizika. (Cingula, 2016)

Kada se govori o sigurnosti i zaštiti informacijskih sustava i mreža, nekoliko principa danas vrijede kao osnovni postulati:

1. Sigurnost je proces. Sigurnost nije gotov proizvod, usluga ili procedura, već skup koji ih sadržava, i još mnogo elemenata i mjera koje se stalno provode.
2. Ne postoji apsolutna sigurnost.
3. Uz različite metode tehničke zaštite, treba imati u vidu i ljudski faktor, sa svim slabostima.

2.2 Informacijska sigurnost

Informacijska sigurnost je disciplina kojoj je osnovni cilj osigurati zaštitu informacija i informacijskih sustava od neovlaštenog pristupa, korištenja, primjene ili uništavanja. (Antoliš, i

drugi, 2010) Informacija je jako važan resurs i kao takav je potrebno zaštiti, a to je iznimno zahtijevan posao s obzirom da su informacije izložene velikom broju prijetnji.

Cilj informacijske sigurnosti je zaštita informacija od velikog broja prijetnji u svrhu smanjenja poslovnih rizika, osiguranja poslovnog kontinuiteta, te povećanja broja poslovnih prilika i povrat od investicija. Važno je naglasiti da se informacijska sigurnost postiže primjenom raznih kontrola kao što je sigurnosna politika, razni procesi i procedure.

Danas se sve češće upotrebljava termin osiguranje informacija, kao zamjenski za pojam informacijska sigurnost, a sve zbog širokog značenja sigurnosti.

Osiguranje informacija predstavlja međudjelovanje tehnologije koja osigurava uvjete sigurnosti, procesa koji osnažuju djelovanje tehnologije i ljudi koji omogućavaju rad tehnologije u operativnoj uporabi. (Klaić, 2010)

Sustav informacijske sigurnosti se sastoji od uravnoteženog skupa sigurnosnih mjera, fizičke sigurnosti, sigurnosti podataka, sigurnosti informacijskih sustava, koordiniranog uvođenja formalnih procedura, kao što su procjene rizika, certificiranje uređaja i akreditacije tehničkih sustava za primjenu u određenim segmentima poslovnih procesa u institucijama. Uravnoteženost i koordiniranje mjera i postupaka treba da se postiže organizacijom i upravljanjem sustavom informacijske sigurnosti.

Informacijska sigurnost uključuje:
1. oporavak informacijskih sustava
2. detekciju i odvraćanje napada
3. primjenu zakonski propisa koji se odnose na privatnost, računalni kriminal, računalnu forenziku i slično.

2.3 Sustav upravljanja informacijskom sigurnošću (ISMS)

Sustav upravljanja informacijskom sigurnošću (ISMS, *engl. Information Security Managment System*) dio je sveukupnog sustava upravljanja, utemeljen na pristupu upravljanju rizicima, u cilju uspostavljanja, provođenja, praćenja, revidiranja, održavanja i unapređenja informacijske sigurnosti. (ISO/IEC, HRN ISO/IEC 27001:2005, 2005)

Da bi organizacija dobila certifikat koji potvrđuje upravljanje informacijskom sigurnošću organizacije moraju ispuniti skup zahtjeva koje definira standard ISO 27001. Osnovni koraci u implementaciji standarda ISO 27001 su početak projekta, definiranje ISMS-a, procjena rizika, upravljanje rizikom, obuka, priprema za reviziju, revizija i kontinuirano unaprjeđenje.

Uspostava ISMS-a je važan zbog zaštite informacijske imovine što omogućuje organizaciji da postigne veću garanciju sigurnosti u zaštiti informacija i imovine od informacijskih rizika na kontinuiranoj osnovi, održava strukturiran sveobuhvatan radni okvir, identifikaciju i procjeni rizika informacijske sigurnosti, odabir i primjenu odgovarajući sigurnosni mjera (kontrola), te mjerenje i poboljšanje njihove učinkovitosti kao i da kontinuirano poboljšava kontroliranu okolinu, te da djelotvorno postiže zakonsku i regulatornu usklađenost.

Da bi se postavio temelj informacijske sigurnosti i odredio njezin okviri, te omogućilo razumijevanje sigurnosnih zahtjeva organizacije i potrebu za uspostavu ciljeva na području informacijske sigurnosti, upotrebljavaju se ISO standardi.

2.4 Definiranje sigurnosnih zahtjeva

Najvažnije za organizaciju je da identificiraju svoje sigurnosne zahtjeve, a to su: procjena rizika, izbor odgovarajućih kontrola i zakonske regulative (Hamidović, 2010):

- Procjena organizacijskih sigurnosnih rizika. Kroz procjenu rizika identificiraju se prijetnje imovini, ranjivosti, te procjena vjerojatnosti incidentne pojave i njenog potencijalnog utjecaja
- Kako bi rizik sveli na prihvatljiv nivo nakon identificiranja sigurnosnih zahtjeva i izrade procjene rizika, potrebno je izabrati i implementirati adekvatne kontrole. Izbor kontrola ovisi o instituciji, odnosno prihvatljivosti rizika i načinu upravljanja rizikom, ali i o državnim i međunarodnim zakonskim pravima i obvezama.
- Zakonom regulirane kontrole presudne za instituciju odnose se na zaštitu tajnosti osobnih podataka i informacija, čuvanje institucijskih izvješća i poštivanje prava intelektualnog vlasništva.

Proces upravljanja rizikom informacijske sigurnosti može se primijeniti na organizaciju kao cjelinu, ili na dio organizacije, bilo koji informacijski sistem.

2.5 Procjena rizika

ISO 27005:2018 (ISO, 2018) definira rizik informacijske sigurnosti kao potencijal da će prijetnja iskoristiti ranjivosti imovine i time uzrokovati štetu za organizaciju.

Rizik informatičko/internetske tehnologije je opasnost da njezina primjena dovede do neželjenih posljedica (šteta) u organizacijskom sustavu i/ili njegovoj okolini. Do zlouporabe uglavnom dolazi zbog dva razloga, i to radi ostvarivanja neopravdanih ili protupravnih koristi od strane pojedinaca ili organiziranih skupina ili radi nanošenja materijalne ili nematerijalne štete pojedincu, skupini ili zajednici. Najugroženiji su informacijski sustavi iz koji se može pristupiti Internetu, jer je i sam Internet izuzetno ugrožen. (Klasić & Klarić, 2009, str. 160)

Rizici kojima su tvrtke izložene u svom poslovanju i za koje minimalno moraju biti propisani postupci mjerenja, procjene i upravljanja uključuju i rizik koji proizlazi iz neadekvatnog upravljanja informacijskim i pridruženim tehnologijama. Upravljanje rizikom informacijskog sustava obuhvaća postupke procjene rizika te poduzimanja radnji za smanjenje rizika na prihvatljivu razinu i održavanje prihvatljive razine rizika. Tvrtke danas moraju obavljati mjerenje, procjenu i upravljanje svim rizicima kojima su u svom poslovanju izložene.

Rizik se uglavnom smanjuje na jedan od tri moguća načina (Uremović, 2009):

- Smanjivanje, provođenjem sigurnosnih kontrola – ovim se načinom primjenjuju sigurnosne kontrole koje smanjuju vjerojatnost ostvarivanja prijetnje ili smanjuju njezin utjecaj,
- Izbjegavanje rizika – bilo koja akcija kod koje se mijenjaju poslovne aktivnosti ili način vođenja poslovanja kako bi se spriječila pojava rizika, primjerice nekorištenjem e-trgovine ili Interneta za određene poslovne aktivnosti, izbjegava se čitav niz prijetnji koje vrebaju uslijed ovakvoga načina poslovanja,
- Prenošenje rizika – ovim se načinom uglavnom pokrivaju rizici kod kojih bi primjena sigurnosnih kontrola bila neekonomična, pa se pribjegava prenošenju rizika na drugu organizaciju, primjerice ugovaranjem polica osiguranja i sl.

3 UPRAVLJANJE INFORMACIJSKOM SIGURNOŠĆU

3.1 Upravljanje i procjena rizika

Upravljati rizicima općenito, znači baviti se pojmom vjerojatnosti. Svaki događaj koji se dogodi i koji za posljedicu ima određeni učinak nosi određenu vjerojatnost, te su vjerojatnosti podaci koji se najčešće izračunavaju naknadno i koji služe za retroaktivnu analizu u procesima upravljanja rizicima.

Upravljanje rizicima može se općenito definirati kao identifikacija, procjena i prioritizacija rizika, nakon kojih slijedi koordinirana i ekonomična uporaba sredstava kako bi se smanjila, nadzirala i bolje kontrolirala vjerojatnost i/ili utjecaj neželjenih događaja.

Upravljanje rizicima možemo istaći u dvije faze i to:

- procjena rizika,
- obrada rizika

Procjena rizika u oblasti sigurnosti informacija, podrazumijeva prepoznavanje uzroka koji bi mogli dovesti do neželjenih ishoda, tj. proučavanje vjerojatnoće pojavljivanja i težine posljedica koje oni izazivaju. U okviru tog procesa potrebno je uzeti u obzir sve raspoložive informacije, kao i sve ostale potrebne resurse. Konkretnije, procjena rizika u oblasti sigurnosti informacija podrazumijeva procjenu vjerojatnoće pojavljivanja i težine posljedica neželjenih događaja koji narušavaju sigurnost informacija, tj. njihovu povjerljivost, cjelovitost i raspoloživost.

Prilikom procjene rizika dodjeljuju se vrijednosti vjerojatnosti i posljedici rizika. Ove vrijednosti mogu biti kvantitativne ili kvalitativne. Tako možemo reći da se procjena rizika temelji se na procjeni posljedica i vjerojatnosti.

Nakon procjene slijedi korak koji je izbor i provođenje mjera zaštite kako bi se rizici umanjili, odnosno njihove posljedice izbjegle ili barem ublažile.

Nakon provođenja koraka koji obuhvaćaju praćenje, mjerenje i izvještavanje o riziku može se

govoriti o upravljanju rizikom u oblasti sigurnosti informacija koje je potrebno utemeljiti na detaljno razrađenim planovima.

Poslije procjene rizika, slijedi obrada rizika. Obrada rizika uključuje određivanje prioriteta, procjenu, odabir i provođenje sigurnosnih kontrola za smanjivanje rizika. Prilikom pravljena plana za obradu rizika, prvo se pristupa opisu kako se procijenjeni rizici trebaju tretirati, da bi zadovoljili kriterije prihvatljivosti. Da bi plan bio prihvaćen potrebno je da rukovodstvo organizacije pregleda i odobri predložene planove obrade rizika i rezultirajuće zaostale rizike, te da se dokumentiraju uvjeti povezani s takvim odobrenjem.

Kriteriji prihvatljivosti rizika mogu biti složeniji od pukog utvrđivanja da li se ili ne preostali rizik nalazi iznad ili ispod praga prihvatljivosti. Prihvaćanjem rizika potrebno je osigurati da su preostali rizici izričito prihvaćeni od rukovodstva organizacije.

3.2 Analiza rizika

Analiza rizika je postupak kojem je cilj da se ustanove ranjivosti sustava, uoče potencijalne prijetnje (rizici), te da na odgovarajući način kvantificirati moguće posljedice kako bi se mogao odabrati najprimjereniji način zaštite, odnosno procijeniti opravdanost uvođenja dodanih protumjera. Analiza rizika se sastoji od identifikacije rizika, opisa rizika i procjenjivanju rizika. Rezultati analize rizika se mogu koristiti za dobivanje profila rizika koji daje ocjenu značajnosti za svaki rizik i osiguranje instrumentarija za definiranje prioriteta u reguliranju rizika.

Postoje dva temeljna pristupa analizi rizika: kvantitativna i kvalitativna analiza. Kvantitativna analiza podrazumijeva iskazivanje rizika u očekivanim novčanim troškovima na godišnjoj razini, dok rezultat kvalitativne analize iskazuje samo relativan odnos vrijednosti šteta nastalih djelovanjem neke prijetnje i uvođenja protumjera.

Nakon završetka procesa analize rizika, potrebno je usporediti procijenjeni rizik sa kriterijima rizika koje je organizacija ustanovila.

3.3 Standardi informacijske sigurnosti

Da bi se postavio temelj informacijske sigurnosti, odredili njeni okviri, te omogućilo razumijevanje sigurnosnih zahtjeva organizacija, kompanija, te potreba za uspostavom ciljeva na području informacijske sigurnosti, upotrebljavaju se standardi (ISO).

Slijed standarda ISO27000 (Rječnik termina koji se koriste unutar ISO 2700 serije standarda) sadrži set smjernica i specifikacija za pomoć organizacijama u razvoju sustava upravljanja informacijskom sigurnošću.

Standardi su od velike važnosti za sigurnost informacijskog sustava su:

- ISO 27001 (ISO/IEC, HRN ISO/IEC 27001:2005, 2005), zamjena za BS7799-2 – predstavlja sustav za upravljanje informacijskom sigurnošću, temeljni standard ISO 27000 serije standarda, a definira zahtjeve za uspostavu, implementaciju, rad, nadzor, reviziju, održavanje i poboljšanje dokumentiranog sustava upravljanja informacijskim sustavom;
- ISO 27002 (2013) – Zbirka pravila, odnosno postupaka za upravljanje informacijskom sigurnošću.

Da bi se uspostavio kvalitetan sustav za upravljanje sigurnošću informacijama, potrebno je uvesti u upotrebu oba standarda. Oba ova standarda glavni su međunarodni standardi informacijske sigurnosti koje je objavila Internacionalna organizacija za standardizaciju (ISO). Ovi standardi su važni zahvaljujući činjenici da ih je moguće primjenjivati skoro u svim organizacijama jer osiguravaju fleksibilnost, definiraju upravljački okvir, a pri tom ne ulaze u konkretnu tehničku implementaciju.

Pored ova dva standarda postoje i upotrebljavaju se još i standardi i to:

- ISO 27003 – Vodič za implementaciju ISMS (ISO/IEC 27003, 2017);
- ISO 27004 – Mjerenje i metrika efikasnosti informacijske sigurnosti (ISO/IEC 27004, 2016);
- ISO 27005 – Upravljanje rizicima informacijske sigurnosti (ISO/IEC 27005:2018, 2018);
- ISO 27006 – Zahtjevi za postupkom analize i certificiranja standarda (ISO/IEC 27006, 2015);

Najnovija inačica ovog standarda je objavljena 2013. godine, te je sadašnji puni naziv ISO/IEC 27001:2013. Najvažnije izmjene u verziji 2013. se odnose na strukturu glavnog dijela standarda, zainteresirane strane, ciljeve, praćenje i mjerenje. Međutim, sve te izmjene nisu zapravo mnogo promijenile standard u cjelini – njegova temeljna filozofija se i dalje bazira na procjeni i obradi rizika, a zadržane su iste faze uspostave, primjene, pregledavanja i poboljšavanja. Ova nova verzija standarda je lakša za čitanje i razumijevanje, te je mnogo jednostavnija za integriranje s drugim standardima upravljanja kao što su ISO 9001, ISO 22301, itd. (ISO/IEC, ISO/IEC 27000 family - Information security management systems, 2018)

3.4 Zakonska regulativa - Sigurnost informacijskog sustava u BiH

Bosna i Hercegovina je zemlja koja je ne tako davno izašla iz ratnog perioda, a i složenog je državnog ustroja sa dva entiteta (Entitet Federacije BiH i Entitet Republike Srpske) i Brčko Distrikt. Ekonomski i socijalni uvjeti u Bosni i Hercegovini su loši, što je i rezultat sporijeg razvoja informacijskih sustava kako u organizacijama tako i u državnim tijelima, tj. danas su na dosta nižoj razini nego u ostalim razvijenim zemljama u okruženju.

Zakonske regulative po pitanju informacijske sigurnosti u Bosni i Hercegovini doneseni su samo par okvirnih zakona koji pokrivaju ovu oblast, sam zakon, kao „Zakon o informacijskoj sigurnosti“ ne postoji, mada je za njega urađen nacrt, a bilo je i nekoliko prijedloga ali do dan danas nije usvojen.

Dok se čeka usvajanje ovog zakona, po pitanju informacijske sigurnosti u Bosni i Hercegovini, postoje zakoni koji su izuzetno značajni po ovom pitanju, a to su:

- Zakon o zaštiti tajnih podataka (Službeni glasnik BiH br. 54/05. i prečišćeni 12/09.;
- Zakon o zaštiti osobnih/ličnih podataka (Službeni glasnik BiH br.32/01, 49/06, 76/11. i prečišćeni 89/11.;
- Zakon o centralnoj evidenciji i razmjeni podataka (Službeni glasnik br.32/01, 16/02, 32/07. i 44/07 (prečišćeni));
- Zakon o komunikacijama (Službeni glasnik BiH br. 31/03, 75/06, 32/10 i 98/12. ;
- Odluka - Politika upravljanja informacijskom sigurnošću u institucijama Bosne i Hercegovine, za razdoblje 2017 - 2022. godine (Službeni glasnik BiH br.38/17.),

U Parlamentu BiH je u proceduri Zakon o Agenciji za razvoj informacijskog društva (ZARID) od listopada 2008.godine, ali do danas nije donesen. Za razliko od ovoga, formirana je Agencija za zaštitu osobnih podataka, prema preporukama Europske unije (EU) koja jednim dijelom radi i na zaštiti informacijskih sustava institucija BiH, ali samo u segmentu administracije i upravljanja /radio-relejnom mrežom putem koje su povezane sve institucije BiH).

U Entitetu Republike Srpske formirana je Agencija za informacijsko društvo koji se bavi stanjem informacijskog sustava (AIDRS- koje je počelo sa radom 01.07.2015.godine, Službeni glasnik RS br.70/11.) što nažalost, ista nije usvojena i na državnoj razini.

Za razliku od Bosne i Hercegovine kao države koja nema CERT *(Computer Energency Response Team*) koja bi se bavila koordinacijom i suradnjom u rješavanju sigurnosnih incidenata između zemalja, radili na edukaciji korisnika Interneta i državne mreže na prevenciji sigurnosnih incidenata, Entitet Republike Srpske ima oformljeno „Odjeljenje za informacijsku bezbjednost“ (OIB) koji vrši funkciju CERT-a Republike Srpske. OIB – CERT Republike Srpske je za sada jedini organ ove vrste u Entitetu Republike Srpske i Bosne i Hercegovine. (CERT RS, 2019)

4 ZAKLJUČAK

Suvremena poslovna praksa pokazuje da se, danas, sigurnost informacija ne tiče samo sektora informacijskog sistema već se tiče cjelokupnog poslovanja jer se sve odluke i rješavanja problema na nivou organizacije se moraju temeljiti na informacijama. Primjene novih tehnologija, organizacije sve teže mogu da prežive na tržištu koje se sve više globalizira. Svjedoci smo da su, informacije i informacioni resursi (hardverski i softverski) danas mnogo više izloženi brojnim prijetnjama po sigurnost, te se koncept zaštite, odnosno sigurnosti informacija nameće kao jedan od prioriteta poslovanja.

Unutar organizacijskih informacijskih sistema sve više se prikupljaju, obrađuju, pohranjuju i razmjenjuju podaci i informacije od vitalnog

interesa za organizaciju, a nerijetko i od društvenog interesa, njihov neometan rad postaje preduvjetom, ne samo njihovog funkcioniranja već sve više i cijelog društva, koje se na njih sve više oslanja. Budući da je to moguće postići samo ako postoji zadovoljavajući stepen njihove sigurnosti, načelo sigurnosti je jedan od temelja njihovog rada.

Organizacije bi prilikom zaštite svojih informacija i svoga informacijskog sustava trebale prvo da obave analizu rizika informacijske sigurnosti, zatim da dokumentiraju rezultate analize, zatim da implementiraju odgovarajuće sigurnosne mjere. Procjenom rizika određuje se vrijednost informacijske imovine, identificiraju primjenjive prijetnje i ranjivosti, identificiraju postojeće sigurnosne kontrole i njihov utjecaj na identificirane rizike, određuju potencijalne posljedice i konačno određuje prioritet identificiranih rizika.

Rizici su dinamični. Prijetnje, ranjivosti, vjerojatnosti ili posljedice mogu se promijeniti naglo bez nagovještaja o promjeni.

Upravljanje informacijskom sigurnošću i kontinuitetom poslovanja, te upravljanje rizicima informacijske sigurnosti zakonska je, moralna i poslovna obaveza svake organizacije i društva, te se stoga treba stalno pratiti, pregledati i poboljšavati, te bi trebalo postati obvezna i razumna aktivnost svake organizacije. Uspostava normi i standarda zahtijeva razumijevanje i iskustvo u uspostavi odredbi iste. Standard ISO 27001 se može promatrati kao model tj. dobra praksa u obliku smjernica i preporuka za osiguranje djelotvornog sistema sigurnosti informacija. Primjenom standarda se stvara sistem koji je fokusiran na poboljšavanja i smanjenje incidenata, a što je najvažnije je eliminiranje uzročnika grešaka i incidenata u samom sistemu.

Iz navedenog je vidljivo da je informacijska sigurnost u Bosni i Hercegovini još uvijek na niskoj razini, a za to je najveći krivac nedostatak zakonskih regulativa koje država iz samo njoj poznatih razloga do sada nije usvojila, te zanemarivanje informacijske tehnologije (IT) od strane države. Ne postoji Agencija na državnom nivou koja bi se bavila ovom problematikom, kao što ne postoji ni okvirni zakon. Pozitivno je jedino to što je sve veći broj organizacija i institucija koji su svjesni vrijednosti informacija, te je sve veće interesiranje organizacija za ovu oblast i porast broja certifikata izdanih po ovim standardima, a i zbog zahtjeva EU, te Agende za Jugoistočnu Europu.

CITIRANA DELA

Antoliš, K., Ždrnja, B., Pakšić, I., Vugrek, A., Pavliček, J., Marijenović, I., . . . Jušić, S. (2010). *Sigurnost informacijskih sustava.* Zagreb: Algebra d.o.o.

CERT RS. (2019). *CERT RS Odjeljenje za informacionu bezbjednost*. Preuzeto sa https://oib.aidrs.org/

Cingula, M. (2016). KORPORATIVNA SIGURNOST - Pojam sigurnosti i temeljni srodni pojmovi. U B. Vukelić, *Sigurnost informacijskih sustava* (str. 6). Rijeka: Veleučilište u Rijeci.

Hajdina, N. (2013). *Osnove informacijske sigurnosti.* Zagreb: FER - Zavod za primijenjeno računarstvo.

Hamidović, H. (2010). Upravljanje rizikom informacijske sigurnosti. *Telekomunikacije*, 33-37.

ISO. (2018). *ISO 27005:2018 Information technology -- Security techniques -- Information security risk management.* Preuzeto sa ISO: https://www.iso.org/standard/75281.html

ISO/IEC. (2005, 10 27). *HRN ISO/IEC 27001:2005.* Preuzeto sa Hrvatski zavod za norme: https://www.iso.org/news/2005/10/Ref976.html

ISO/IEC. (2018). *ISO/IEC 27000 family - Information security management systems.* Preuzeto sa ISO: https://www.iso.org/isoiec-27001-information-security.html

ISO/IEC 27002. (2013, 10). *Information technology -- Security techniques -- Code of practice for information security controls.* Preuzeto sa ISO: https://www.iso.org/standard/54533.html?browse=tc

ISO/IEC 27003. (2017, 03). *Information security management systems — Guidance.* Preuzeto sa ISO: http://www.iso27001security.com/html/27003.html

ISO/IEC 27004. (2016, 12). *Information security management — Monitoring, measurement, analysis and evaluation.* Preuzeto sa ISO: https://www.iso.org/standard/64120.html?browse=tc

ISO/IEC 27005:2018. (2018, 07). *Information technology -- Security techniques -- Information security risk management.* Preuzeto sa ISO: https://www.iso.org/standard/75281.html?browse=tc

ISO/IEC 27006. (2015, 10). *Requirements for bodies providing audit and certification of information security management systems.* Preuzeto sa ISO: https://www.iso.org/standard/62313.html?browse=tc

Klaić, A. (2010, 02 08). *Pregled stanja i trendova u suvremenoj politici informacijske sigurnosti i metodologijama upravljanja informacijskom sigurnošću.* Preuzeto sa FER - Fakultet elektrotehnike i računarstva: https://www.fer.hr/_download/repository

Klasić, K., & Klarić, K. (2009). *Informacijski sustavi.* Zagreb: Intus informatika.

Krapac, D. (1992). *Kompjuterski kriminalitet.* Zagreb: Pravni fakultet.

Pleskonjić, D., Maček, N., Đorđević, B., & Carić, M. (2007). *Sigurnost računarskih sistema i mreža.* Beograd: Mikro knjiga.

Sinkovski, S., & Lučić, B. (2006). Informaciona bezbednost i kriptografija. *ZITEH 2006* (str. R25 1-16). Beograd: IT Veštak. Preuzeto sa http://www.itvestak.org.rs/media/biblioteka/zbornik-radova-ZITEH-06.zip

Uremović, D. (2009). Kako upravljati IT rizicima. *InfoTrend*(5), 42-47.

ZAKONI:

- Zakon o zaštiti tajnih podataka (Službeni glasnik BiH br. 54/05. i prečišćeni 12/09.;
- Zakon o zaštiti osobnih/ličnih podataka (Službeni glasnik BiH br.32/01, 49/06, 76/11. i prečišćeni 89/11.;
- Zakon o centralnoj evidenciji i razmjeni podataka (Službeni glasnik br.32/01, 16/02, 32/07. i 44/07 (prečišćeni));
- Zakon o komunikacijama (Službeni glasnik BiH br. 31/03, 75/06, 32/10 i 98/12. ;
- Službeni glasnik BiH, broj 38/17 Odluka - Politika upravljanja informacijskom sigurnošću u institucijama Bosne i Hercegovine, za razdoblje 2017 - 2022. godine