INFORMACIONA SIGURNOST SA PREGLEDOM STANJA U BOSNI I HERCEGOVINI

INFORMATION SECURITY WITH OVERVIEW OF THE SITUATION IN BOSNIA AND HERZEGOVINA

Muharem Redžibašić, Sabahudin Jašarević
Univerzitet u Zenici
Politehnički fakultet
Zenica

REZIME

Svjedoci smo svakodnevne ekspanzije u polju informacionih tehnologija. Bilo da smo stručnjaci iz oblasti informacionih tehnologija (IT) ili da informacione tehnologije koristimo kao olakšicu pri obavljanju svakodnevnih poslovnih zadaka, evidentno je da je tema informacione sigurnosti uvijek aktualna. Razlog tome jeste povećanje sigurnosnih rizika na dnevnoj bazi koji su direktno proporcionalni porastu upotrebe informacionih sistema u poslovanju. Što više težimo „uredima bez papira" to više moramo obratiti pažnju na našu informacionu sigurnost. Iako je prvi motiv pri kreiranju informacionih sistema da se poslovna logika prilagodi i digitalizuje kroz informacioni sistem, nerijetko se desi situacija gdje se zanemari informaciona sigurnost ili izostavi kao bitan faktor poslovanja. U tim situacijama, maliciozni korisnici to mogu da zloupotrijebe i štete koje nastaju mogu da budu izrazito velike. Uslijed novonastalih svjetskih dešavanja po pitanju pandemije, mnogi poslovni procesi su se digitalizovali jako brzo što bi moglo da ima značajne posljedice ukoliko se zanemarila informaciona sigurnost. U ovom radu će biti obrađeni bitni koncepti informacione sigurnosti, sa pregledom stanja u Bosni i Hercegovini, koji mogu poslužiti kao smjernica za daljnji razvoj i unapređenje kvalitete poslovanja.

Ključne riječi: informaciona sigurnost, kvaliteta poslovanja, informacioni sistemi, digitalizacija

ABSTRACT

We are witnessing a daily expansion in the field of information technology. Whether we are experts in the field of information technology (IT) or we use information technology as a tool in performing everyday business tasks, it is evident that the topic of information security is always relevant. The reason for this is increase in security risks on a daily basis that are directly proportional to the increase in use of information systems in business. The more we trend for "paperless offices", the more we must pay attention to our information security. Although the first motive in creating information systems is to adapt and digitize business logic through the information system, there is often a situation where information security is neglected or omitted as an important factor in business. In these situations, malicious users can abuse it and the damage that can occur can be extremely large. Due to the new global developments regarding the pandemic, many business processes have been digitized very quickly, which could have significant consequences if information security is neglected. This paper will discuss important concepts of information security, with an overview of the situation in Bosnia and Herzegovina, which can serve as a guide for further development and improvement of business quality.

Keywords: information security, business quality, information systems, digitalization

1. UVOD

Mnogo puta smo se susreli sa pojmom informacija i u svim definicijama koje možemo pronaći akcenat se stavlja na važnost informacija i njihovu vrijednost koja se posmatra kao veoma značajan resurs bilo da se prenose u pisanom, elektronskom ili nekom drugom obliku. Upravo ispravnost, a u nekim slučajevima i tajnost informacija predstavlja bitan faktor poslovanja institucije ili organizacije. [1]

U ovom radu naglasak će biti na informacijama koje se prenose u digitalnom obliku i na jednom širem konceptu pristupa informacionoj sigurnosti koji se ne odnosi samo na tehničke mjere zaštite, već niz drugih faktora koji čine jedan kompletan pristup zaštiti informacija kroz davanje značaja administrativnim mjerama kao i fizičkim. Prema tome, lahko je doći do zaključka da informaciona sigurnost direktno utječe na kvalitet poslovanja, odnosno, konkuretnost, profitabilnost i sam poslovni ugled ukoliko se radi o organizacijama.

Ukoliko govorimo na državnom nivou, upravo, razvoj sistema informacione sigurnosti jedne države je važna pretpostavka za stvaranje informacionog društva (državna uprava, privredni subjekti i stanovništvo), što je jako bitno i postavlja se kao uslov za međunarodne integracione procese.[7]

2. ZAKONSKA REGULATIVA

Povodom prethodno navedenog, Vijeće ministara Bosne i Hercegovine je na 22. sjednici, održanoj u martu 2017. godine donijelo *Odluku o usvajanju politike upravljanja informacionom sigurnošću u institucijama Bosne i Hercegovine* za period od 2017. do 2022. godine kojom je najavljen *Zakon o informacionoj sigurnosti i sigurnosti mrežnih i informacionih sistema*, a isti je u oktobru 2020. godine objavljen na zvaničnoj web stranici Federalnog ministarstva prometa i komunikacija i trenutno se nalazi u fazi prednacrta.[3]

Prema tom prednacrtu, pojam informaciona sigurnost je definisan kao *„stanje povjerljivosti, cjelovitosti i dostupnosti podataka, koje se postiže primjenom propisanih mjera i standarda informacione sigurnosti te organizacijskom podrškom za poslove planiranja, provođenja, provjera i dorade mjera i standarda.“[4]*

Bitno je spomenuti da u zemljama okruženja već postoje ovakvi Zakoni i to u Republici Srbiji. *„Zakon o informacionoj bezbednosti“* - ("Sl. glasnik RS", br. 6/2016, 94/2017 i 77/2019) [8] i Republici Hrvatskoj *„Zakon o informacijskoj sigurnosti“* (NN 79/07) – RH. [6]
Evidentna je velika sličnost sa spomenutim Zakonom iz RH, a isti je dosta star ukoliko uzmemo u obzir brzinu napredovanja informacionih tehnologija, moglo bi se reći da prednacrt *Zakona o informacionoj sigurnosti i sigurnosti mrežnih i informacionih sistema* ne sadrži sve bitne pojmove koji su relevantni za sigurnost infromacionih sistema.
Po uzoru na Zakon iz Republike Srbije bilo bi dobro uvesti još neke pojmove i definisati njima pripadajuće članove kao sto su: kripto bezbjednost, osnovne mjere zaštite IKT sistema, uvođenje inspekcije za informacionu bezbjednost i članova koji definišu zaštitu djece pri korištenju informaciono-komunikacionih tehnologija.
U prednacrtu najavljeno je i formiraje CERT-a[1] u roku od 12 mjeseci od dana stupanja na snagu ovog Zakona. Ranije po pitanju CERT-a urađena je *Strategija uspostave CERT-a u BIH* 2011. Godine [9] i Odluka iz 2017. godine kojom se određuje Tim za odgovor na računarske incidente za institucije Bosne i Hercegovine (CERT). Na državnoj razini još nije formiran CERT, dok je isti formiram u Republici Srpskoj još 2015. godine,

[1] Tim za odgovor na računarske incidente - **C**omputer **E**mergency **R**esponse **T**eam

Također je bitno naglasiti da se očekuje i novi *Zakon o elektronskoj identifikaciji i uslugama povjerenja za elektronske transakcije* čiji je prijedlog Zakona donio Savjet ministara u tehničkom mandatu u mjesecu februaru 2019. godine, a čiji je predlagač Ministarstvo komunikacija i prometa BIH. [10]

Ovaj Zakon treba riješiti bitne stvari oko sigurnosti povezivanja informacionih sistema, kako bi se olakšao promet elektronskih dokumenata u javnoj upravi. Nažalost, ovaj Zakon je povučen iz parlamentarne procedure zbog negodovanja institucija Republike Srpske.
Jedan od uslova za pristupanje Bosne i Hercegovine Evropskoj uniji jeste usvajanje, između ostalog, ovog a i sličnih Zakona.

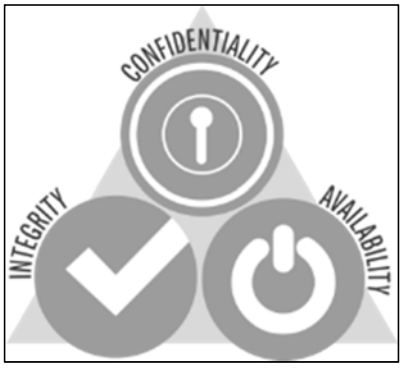
Bito je uskladiti ovaj prednacrt *Zakon o informacionoj sigurnosti i sigurnosti mrežnih i informacionih sistema* sa prijedlogom *Zakon o elektronskoj identifikaciji i uslugama povjerenja za elektronske transakcije* koji treba biti nasljednik *Zakona o elektronskom potpisu iz 2006.* godine koji više nije usklađen sa direktivama Evropske unije i zato se isti mijenja.

Ovo sve navedeno povodom zakona na državnoj razini itekako je važno jer se radi o informacionim sistemima i uvođenju elektronske Uprave. Pojam sigurnosti informacionih sistema vežemo za pojam umrežavanja informacionih sistema, moglo bi se reći, koliko nam je sigurna veza kojom osiguravamo protok podataka, toliko će nam biti siguran i sam informacioni sistem sa pripadajućim podacima.
Ovdje se također kriju odgovori na mnoga pitanja gdje smo svjedoci digitalizacije poslovnih procesa. Bez primjene savremenih IT rješenja i uz adekvatnu Zakonsku regulativu mi ne dobivamo urede bez papira, već ostaju nam uredi sa papirima i dvostruke evidencije (elektronski i papirni oblik), a da ne spominjemo deficit po pitanju informacione sigurnosti.

3. INFORMACIONA SIGURNOST

3.1. Zaštita informacija

Ukoliko pogledamo definiciju informacione sigurnosti, uglavnom se svaka interpretira kroz tri aspekta, a to su povjerljivost, intergritet i dostupnost podataka. To nije slučajno jer upravo ta tri aspekta čine sigurnosni trougao (eng. C-I-A triad).



Slika 1. CIA trougao [12]

Ova tri aspekta trebaju da budu temeljni ciljevi ka postizanju informacione sigurnosti budući da se svaki poslovni proces bazira na protoku podataka. Kada kažemo informaciona sigurnost pri tome se ne misli isključivo na IT sigurnost, kao i kada govorimo o informacionom sistemu analogno tome možemo reći da neki IT sistem čini samo dio informacionog sistema.

Povjerljivost predstavlja zaštitu podataka od neovlaštenog pristupa, odnosno sprječavanje neovlaštenog otkrivanja podataka. Ukoliko govorimo o tehničkoj implementaciji ovoga aspekta onda su to uglavnom metode koje su usmjerene prema korisničkoj autorizaciji i autentifikaciji. Svakako je preporučljivo koristiti dvo-faktorsku autentifikaciju (2FA).
Integritet podataka predstavlja dosljednost podataka uslijed skladištenja, prijenosa, arhiviranja, itd. Ovo je jako bitna činjenica jer u elektronskom poslovanju trebaju biti osigurani mehanizmi zaštite integriteta podataka. Često se putem informacionih sistema prenose jako bitne stvari i njihov integritet nekada određuje uspješnost poslovanja. Za osiguranje integriteta podataka svakako je bitno spomenuti *blockchain*[2] tehnologiju koja je sa aspekta sigurnosti donijela jedan novi pristup skladištenja podataka.
Dostupnost podataka predstavlja aspekt gdje je fokus na dostupnosti podataka onima koji imaju pravo pristupa istim. Ovaj aspekt je sa sigurnosne tačke gledišta prvi vrhu prioriteta i napadi koji se dešavaju na razne profitabilne organizacije su usmjereni upravo da naruše ovaj aspekt poslovanja. Mnogim organizacijama koje posluju on-line dostupnost je direktno vezana za profitabilnost, tako da ako imamo situaciju da neki server iz oblasti *e-commerc* nije dostupan određeno vrijeme, uz manju jednostavniju analizu mogu se izračunati gubitci koji su nastali tom radnjom. [13]

3.2. Sistemi upravljanja sigurnošću informacija (ISMS)

Svim problemima u bilo kojoj sferi poslovanja treba da se pristupa sistematski, sa uređenim skupom pravila. Tako da sistemi za upravljanje sigurnošću informacija (ISMS) predstavljaju jedan sistemski pristup za očuvanje aspekata ka postizanju informacione sigurnosti (C-I-A) koji imaju za cilj uspješnu zaštitu informacione imovine.[5]

Za postavljanje temelja i okvira informacione sigurnosti, između ostalog, koriste se standardi, odnosno norme. Upravo slijedeći te standarde, odnosno norme, možemo biti sigurni da smo kvalitetno uspostavili sigurnosne kontrole. U tu svrhu postojani su međunarodni standardi, koji se odnose na informacionu sigurnost i koji pomažu institucijama ili organizacijama da uspostave sistem upravljanja informacionom sigurnošću.

„ISMS je važan i za javni i za privatni poslovni sektor. U bilo kojoj industriji ISMS omogućava podršku za e-poslovanje i osnova je za upravljanje rizicima. Povezanost javnih i privatnih mreža i dijeljenje informacione imovine usložnjava kontrolu pristupima informacijama i njihovo rukovanje.“ [5]

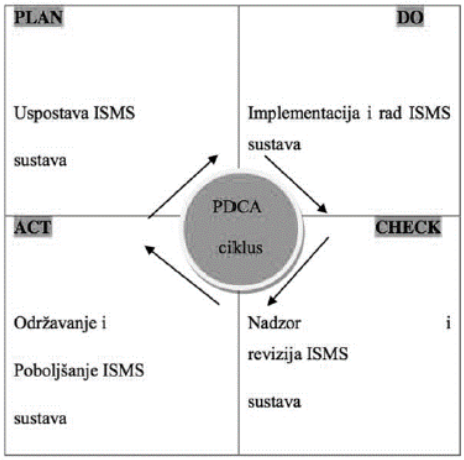
ISMS su nedvojbeno istaknuti kao faktori unapređenja poslovanja jer kada neka institucija ili organizacija usvoji ISMS familiju standarda to je dobar pokazatelj povjerenja potencijalnim i trenutnim poslovnim saradnicima.

Informacionu sigurnost definiše standard ISO/IEC[3] 27001. To je skupina smjernica i pravila koja bilo kojoj organizaciji, bez obzira na veličinu i djelatnost, može pružiti metodologiju za uspostavljanje sistema za upravljanje informacionom sigurnošću.

Osim ISO/IEC 27001 standarda koji definiše *Zahtjeve za informacionu sigurnost*, bitno je pomenuti i ISO/IEC 27003 koji predstavlja *smjernice za implementaciju sistema za upravljanje sigurnošću informacija*.

[2] Blockchain predstavlja distribuiranu repliciranu bazu podataka. Organizovana je u formi jednostruko spregnute liste (lanac), gde su čvorovi blokovi sa podacima o transakcijama, koji se poslije grupisanja štite kriptografskim metodama. [2]
[3] Internacionalna organizacija za standardizaciju

Metodologija izgradnje sistema za informacionu sigurnost temelji se na standardnom PDCA (engl. *Plan-Do-Check-Act*)[4] ciklusu i čine je 4 faze: planiranje, implementacija, nadzor, poboljšavanje.



Slika 2. Faze PDCA ciklusa (modela) [1, str. 28]

PCDA predstavlja jedan neprekidan ciklus promjena u cilju poboljšanja i trajne upotrebe. Može da se primjeni u svim sferama poslovanja pa čak i života. Jasno je zašto se baš jedna od najzahtjevniji metodologija, a to jeste metodologija izgradnje sistema za informacioni sigurnost, temelji baš na ovom ciklusu.

4. ZAKLJUČAK

Kroz ovaj rad mogli smo da dobijemo bolju percepciju pojma informacione sigurnosti i nekih jako bitnih stvari koje istu definišu. Poglavlje broj 2 upravo je posvećeno zakonskoj regulativi jer bez obzira na tehničke predispozicije ovaj dio mora biti riješen za uspješnu uspostavu informacione sigurnosti u cilju kvalitetne digitalizacije poslovnih procesa. Nedvojbeno je da država Bosna i Hercegovina tek treba da usvoji važne zakone koji regulišu sferu elektronskog poslovanja kao i da se formira CERT, a važnost istog nije potrebno mnogo naglašavati. Do tada, da bi zadržali povjerenje klijenata, institucije i organizacije mogu da pristupe certificiranju za neki od međunarodno priznatih standarda kako bi zadobili povjerenje klijenata i eventualno odbacili nelojalnu konkurenciju. Implementacija bilo kojeg međunarodno priznatog standarda, u ovom slučaju ISO/IEC 27001, ne predstavlja kraj razvoja sistema informacione sigurnosti, naprotiv, koristeći PDCA ciklus ulazimo u jedan neprekidan proces poboljšanja gdje se završetak jednog ciklusa može smatrati ulaznim parametrima za započinjanje novog, složenijeg i kvalitetnijeg, ciklusa.

Da bi zadovoljili aspekte informacione sigurnosti (C-I-A) predstavljeni su i sistemi za upravljanje sigurnošću informacija(ISMS) gdje je evidentno da se metodologija izgradnje pomenutih sistema upravo temelji na PDCA ciklusu. Donosimo zaključak da se svi zahtjevi za poboljšanje kvalitete poslovanja trebaju rješavati sistematski kako bismo izbjegli da previdimo neke osnovne stvari, a ujedno i postigli željeni cilj.

[4] "PDCA (ili PDSA) ciklus je originalno opisao Walter Shewhart tijekom 1930-tih, a kasnije ga je prihvatio W. Edwards Deming. Model osigurava okvir za poboljšavanje procesa ili sistema". [11]

5. REFERENCE

[1] B. Vukelić (2016.) – Sigurnost informacijskih sustava; Veleučilište u Rijeci; ISBN: 978-953-6911-84-4

[2] Miroslav M. (2017.), „Blockchain tehnologija: mogućnost upotrebe izvan kripto valuta“, INFOTEH 2017, Srbija, https://www.researchgate.net/publication/318722738_BLOCKCHAIN_TEHNOLOGIJA_MOGUCNOSTI_UPOTREBE_IZVAN_KRIPTO_VALUTA, pristupljeno 09.05.2021.godine

[3] Službena web stranica Federalnog ministarstva prometa i komunikacija (2021.), Poziv za dostavljanje primjedbi, prijedloga i komantara na Zakon o informacionoj sigurnosti i sigurnosti mrežnih i informacionih sistema; http://fmpik.gov.ba/bh/aktuelnosti/obavje%C5%A1tenja/308-poziv-za-dostavljanje-primjedbi,-prijedloga-i-komantara-na-zakon-o-informacionoj-sigurnosti-i-sigurnosti-mre%C5%BEnih-i-informacionih-sistema.html , pristupljeno 10.04.2021. godine

[4] Službena web stranica Federalnog ministarstva prometa i komunikacija (2021.), Prednacrt Zakona o informacionoj sigurnosti i sigurnosti mrežnih i informacionih sistema; http://fmpik.gov.ba/bh/dokumenti/prijedlozi-i-nacrti.html?task=document.viewdoc&id=1094 , pristupljeno 10.04.2021.

[5] Službena web stranica instituta za standardizaciju Bosne i Hercegovine (2021), Sistemi upravljanja sigurnošću informacija, https://isbih.gov.ba/p/sistemi-upravljanja-sigurnoscu-informacija, pristupljeno 09.05.2021.

[6] Službena web stranica Internet projekta za prikupljanje svih zakona Republike Hrvatske (2021.); „Zakon o informacijskoj sigurnosti“ (NN 79/07) – RH; https://www.zakon.hr/z/218/Zakon-o-informacijskoj-sigurnosti , pristupljeno 10.04.2021.

[7] Službena web stranica JP NIO Službeni list BIH (2021.), Odluka o usvajanju Politike upravljanja informacionom sigurnošću u institucijama Bosne i Hercegovine, za period 2017-2022. Godine; http://www.sluzbenilist.ba/page/akt/bM0k8gNBNCU= , pristupljeno 10.04.2021. godine)

[8] Službena web stranica kompanije PARAGRAF (2021.), Zakon o informacionoj bezbednosti - ("Sl. glasnik RS", br. 6/2016, 94/2017 i 77/2019); https://www.paragraf.rs/propisi/zakon_o_informacionoj_bezbednosti.html, prisupljeno 10.04.2021. godine

[9] Službena web stranica Ministarstva sigurnosti Bosne i Hercegovine (2021.), Strategija upostave CERT-a u Bosni i Hercegovini; http://www.msb.gov.ba/dokumenti/strateski/default.aspx?id=6248&langTag=bs-BA , pristupljeno 10.04.2021. godine

[10] Web platorma javnarasprava.ba (2021.), Prijedlog Zakona o elektronskoj identifikaciji i uslugama povjerenja za elektronske transakcije; https://javnarasprava.blob.core.windows.net/content/LawText/UKWVADF6.pdf , pristupljeno 11.04.2021.

[11] Web stranica Ekonomskog fakulteta u Osjeku (2021.), PDCA Ciklus, http://www.efos.unios.hr/upravljanje-marketingom/wp-content/uploads/sites/151/2014/01/PDCA-ciklus.pdf , pristupljeno 09.05.2021.

[12] Web stranica kompanije Falcongaze (IT security) (2021.), CIA triad: history and modernity; https://falcongaze.com/en/pressroom/publications/articles/cia-triad.html , pristupljeno 09.05.2021.

[13] Web stranica online organizacije Panmore Institute (2021.), The CIA Triad: Confidentiality, Integrity, Availability; A.Henderson (2019.); http://panmore.com/the-cia-triad-confidentiality-integrity-availability , pristupljeno 09.05.2021.