PREGLEDNI RAD
REVIEW PAPER

BOSNIACA 2018; 23: 95-98
UDK/UDC 02:004.738.5]:006.3

Primljeno/Received 03. 11. 2018.
Prihvaćeno/Accepted 24. 12. 2018.

UNAPREĐENJE BEZBEDNOSTI BIBLIOTEČKO-INFORMACIONOG SISTEMA PRIMENOM STANDARDA ISO 27001

IMPROVING THE SECURITY OF LIBRARY-INFORMATION SYSTEM BY APPLYING STANDARD ISO 27001

Stefan Jamandilović[1]
stefan.jamandilovic@nb.rs

Miroljub Stojanović[1]
misa.stojanovic@nb.rs

[1] Narodna biblioteka Srbije, Beograd, Srbija

Sažetak

U ovom članku će biti opisane stavke koje je potrebno ispuniti kako bi se podigao nivo bezbednosti prema standardu ISO 27001. Pored toga, opisani su slojevi na koje je neophodno obratiti pažnju kada je u pitanju postizanje maksimalne zaštite sistema. Na osnovu ISO 27001 standarda i zakona o IKT (Informaciono-komunikacionih tehnologija) bezbednosti, donesen je dokument "Pravilnik o bezbednosti informaciono-komunikacionih sistema Narodne biblioteke Srbije".

Ključne reči: ISO 27001, zaštita, bezbednost, informacija, standard

Abstract

This article will describe the items that need to be fulfilled in order to raise the level of security according to the ISO 27001 standard. Additionally, layers are described which need to be considered when it comes to achieving maximum protection of the system. Based on ISO27001 and ICT (Information and Communications Technologies) laws, the document "Information and Communications Technologies security rule book of the National Library of Serbia" was adopted.

Key words: ISO 27001, protection, security, information, standard

Uvod

ISO 27001 (zvanični naziv ISO/IEC 27001:2013, u Srbiji je zvanični naziv SRPS ISO/IEC 27001:2014), predstavlja međunarodni standard. Ovaj standard se odnosi na zaštitu i bezbednost informacija. Razlog za primenu standarda ISO 27001 se ogleda u organizaciji, identifikaciji i analizi rizika bezbednosti informacija, kao i njihovom adresiranju. Cilj primene standarda ISO 27001 je da pruži sveobuhvatnu bezbednost, kao i da vodi računa o ranjivosti, pretnjama i uticajima na poslovanje u okviru informacionog sistema kompanije.

Koraci u uvođenju standarda

Kako bi započeli proces uspostavljanja bezbednijeg poslovanja po standardu ISO 27001, potrebno je izvršiti određene radnje u cilju zadovoljavanja propisanih ovim standardom.

Prvi korak se ogleda u GAP (pregled sadašnjeg stanja sastava i upoređivanje s "idealnim stanjem" u odnosu na nove zahteve koji će biti sadržani u normama) analizi trenutnog stanja sistema ISMS (sistem menadžmenta bezbednosti informacija) na osnovu smernica GDPR (General Data Protection Regulation).

GDPR predstavlja opštu uredbu o zaštiti podataka o ličnosti usvojenu na nivou Evropske unije. Cilj njenog donošenja je unificirana zaštita podataka o ličnosti na tlu EU, kao i u zemljama koje obrađuju podatke o ličnosti državljana EU.

Rezultat analize GAP-a je lista aktivnosti koje je neophodno realizovati da bi se postojeći poslovni sistem organizacije usaglasio sa standardom. GAP analiza obuhvata:

- Snimanje i analizu stanja prostora, opreme, dokumenata, organizacija, radne prakse i sl.;
- Izradu izveštaja gde su naznačena svi delovi organizacije u kojima su potrebne promene, prilagođavanja i poboljšanja, kao i davanje smernica kako ta prilagođavanja i poboljšanja implementirati u sistem poslovanja.

Potom je potrebno uraditi analizu rizika koji se odnose na bezbednosti informatičkih resursa. Pod tim se podrazumeva kreiranje planova koji se sprovede u stacionarnom režimu, u režimu pripravnosti, kao i polazna varijanta. Veoma je važno imati sanacioni plan ako dođe do nepredviđenih okolnosti i koji predstavlja preventivni strateški plan u incidentnim situacijama.

U sledećem koraku se obrađuje politika bezbednosti informacija. Tokom ove faze se izrađuju i priručnici o bezbednosti informacija. Od strane organizacije takođe se mora uspostaviti sistem za upravljanje incidentima. Klijenti potpisuju dva sporazuma – prvi se odnosi na izjavu o primenljivosti 114 (kontrola za bezbednost informacija), koja se odnosi na kontrolu bezbednosti utvrđeno standardom ISO 27001:2013, kao i sporazum o poverljivosti informacija.

U procesu konfigurisanja poslovnih sistema, po zahtevima standarda ISO 27001, bitno je napraviti segmentaciju u vidu primene pravila, koja se s jedne strane odnose na bezbednost i zaštitu informacija preduzeća i zaposlenih, a sa druge strane na primenu pravila o bezbednosti i zaštiti podataka krajnjih korisnika. Za cilj u okviru prvog segmenta se nalaže sistemska konfiguracija i osposobljavanje proaktivnog pristupa za prepoznavanje potencijalnog rizika današnjeg savremenog vida poslovanja vezanog za računare. Poštujući standarde koje nalaže ISO 27001 procenat pojave pretnji se smanjuje na minimum.

Drugi segment implementacije se odnosi na bezbednost podataka krajnjih korisnika i ogleda se u tome da davalac obezbeđuje usluge krajnjim korisnicima i štiti njihove podatke i na taj način sprečava njihovu zloupotrebu. Svi nabrojani koraci preduzimaju se u cilju podizanja bezbednosti poslovnog sistema i zabrane zloupotrebe podataka korisnika naših usluga i sistema, čime se kvalitet našeg poslovanja ocenjuje kao pouzdan.

Ukoliko se ispoštuju svi preduslovi prilikom implementacije i primene standarda, i to na način da se pokrivaju informatički, administrativni i fizički sloj, standard ISO 27001 predstavlja sveobuhvatan vid zaštite. Sa strane informatičkog sloja mora se izvršiti analiza kompletne hardverske infrastrukture kompanije. Pored hardverske infrastrukture, *informatički sloj* se bavi analizom protokola, upravljanjem lozinkama, procesom šifrovanja podataka, kao i aspektom pojave rizika koji se tiču bezbednosti informacija i podataka. Ovaj korak predstavlja prvi korak u procesu implementacije.

Drugi korak u procesu implementacije se odnosi na definisanje jasnih procedura koje se odnose na generisanje informacija i manipulaciju ovim informacijama. Sve navedeno se odnosi na *administrativni sloj*.

Poslednji sloj predstavlja *fizički sloj* u kojem se reguliše fizička kontrola pristupa resursima i evidencija zaposlenih. U fizički sloj takođe spada upravljanje video-nadzorom i zaštita radnih prostorija, a naročito računskih centara i serversala.

Ako su sve prethodne stavke ispunjene i ako je implementacija uređena po ISO 27001, omogućava se podizanje bezbednosti informacije na viši nivo kroz definisanje integriteta, poverljivosti i pristupu informacijama.

Implementacija bezbednosnih protokola po standardu ISO 27001 u Narodnoj biblioteci Srbije

Prema pravilniku o bezbednosti informaciono-komunikacionih sistema Narodne biblioteke Srbije, kreirani su ciljevi koji se tiču podizanja, pre svega, opšte svesti o rizicima i opasnostima vezanim za korišćenje informacionih tehnologija, minimizaciju bezbedonosnih incidenata, kao i doprinosa razvoja odgovarajućih bezbedonosnih aplikacija. Pored navedenih ciljeva, takođe je neophodno obezbediti konzistentnost kontrole svih komponenti IKT sistema (Informaciono-komunikacione tehnologije i sistema).

Predmet zaštite obuhvata:

1. hardverske i softverske komponente informatičkih resursa,
2. podatke koji se obrađuju ili čuvaju na informatičkim resursima,
3. korisničke naloge i druge podatke o korisnicima informatičkih resursa u biblioteci (NBS).

Prema pravilniku o bezbednosti IKT sistema Narodne biblioteke Srbije, dužnosti korisnika informatičkih resursa se ogledaju u poštovanju bezbednosnih pravila, primerenog korišćenja informatičkih resursa u smislu korišćenja informatičkih resursa isključivo u poslovne svrhe. Dodatno se prema pravilniku daje saglasnost o tome da su svi podaci koji se skladište i/ili prenose i procesuiraju u okviru informatičkih resursa vlasništvo biblioteke, kao i da mogu biti predmet nadgledanja i pregledanja. Kompletnu listu dužnosti korisnika informatičkih resursa moguće je pročitati u pravilniku o bezbednosti informaciono-komunikacionih sistema Narodne biblioteke Srbije.

Što se tiče bezbednosti profila korisnika informatičkih resursa, korisnik je u obavezi da ima lozinku koja je jakog karaktera (minimum sedam karaktera kombinovanih od malih i velikih slova, cifara i specijalnih znakova). Korisnik se vezuje za korisnički nalog kojim može upravljati samo korisnik kome je dodeljen. U slučaju uočavanja ili sumnje o nastupanju incidenta kojim se ugrožava sigurnost IKT sistema, korisnik je dužan da obavesti neposrednog rukovodioca i Odeljenje za održavanje i razvoj računarsko-informatičkog sistema.

Zaštita od zlonamernih softvera (virusa, malvera...) je definisana članom ovog pravilnika kojim se obezbeđuje bezbednost korisnika i to u cilju zaštite od virusa i druge vrste zlonamernog koda koji u računarsku mrežu mogu dospeti internetskom konekcijom, zaraženim prenosivim medijima, instalacijom nelicenciranog softvera i sl.

U cilju sigurnosti korišćenja servisa elektronske pošte moraju se poštovati pravila koja se odnose na priloge koji stižu sa sumnjivih ili nepouzdanih adresa. Takođe, zabranjeno je koristiti elektronsku poštu u privatne svrhe, kao i korišćenje privatnih naloga u poslovne svrhe.

Kada je u pitanju procedura postupka sa prenosivim medijima, neophodno je ispoštovati sledeće korake. Prenosivi mediji koji sadrže podatke moraju biti propisno obeleženi i popisani, da se čuvaju u zaštićenoj biblioteci magnetnih ili elektronskih medija. Sledeći parametar koji se razmatra je fizička sigurnost informatičkih resursa te se u cilju fizičke sigurnosti informatičkih resursa moraju obezbediti server sala, serveri, storidži (storage) i komunikaciona čvorišta. Kako bi ispunili zahteve koji se standardom nalažu, potrebno je da budu smešteni u posebnoj prostoriji koja ispunjava standarde protivpožarne zaštite, poseduje redudantno napajanje električnom energijom, kao i adekvatnu regulaciju temperature server-sale. Pored navedenih uslova, zabranjuje se pristup nezaposlenim licima, a osobama koje su zadužene za održavanje IKT sistema moguć je pristup serversali samo uz prethodno odobrenje rukovodioca Odeljenja za održavanje i razvoj računarsko-informatičkog sistema. Radne stanice moraju biti primereno fizički obezbeđene sa ciljem detekcije i mogućnošću fizičkog pristupa. Svaki pristup komponentama IKT sistema mora biti autentifikovan putem šifara i elektronskim karticama. Za pravilno instaliranje i pravilno konfigurisanje celokupnog softvera zaduženi su isključivo administratori Odeljenja za održavanje i razvoj računarsko-informatičkog sistema. Administratori su dužni da postupaju u skladu sa propisanim procedurama i uputstvima o zaštiti i bezbednosti IKT-a Narodne biblioteke Srbije.

U cilju praćenja i analize bezbednosti IKT, kao i evidentiranja incidentnih situacija, u NBS je formiran tim za praćenje bezbednosti. Zadatak tima je da svakog meseca kreira izveštaj na osnovu dešavanja iz tog meseca i da podnese godišnji izveštaj o bezbednosti. Na osnovu ovog izveštaja se prave planovi o poboljšanju bezbednosti i inoviranju propisanih procedura.

Literatura

Grubor, G. 2012. *Projektovanje menadžment sistema bezbednosti informacija: udžbenik*. Beograd: Univerzitet Singidunum, Beograd.

ISO / IEC 2700. http://iso.org.rs/iso-27001/. Datum pristupa: 1. 12. 2018.

Zakon o informacionoj bezbednosti. "Sl. glasnik RS", br. 6/2016.

Zakon o informacionoj bezbednosti. "Sl. glasnik RS", br. 94/2017.