UDK 338.486.21/.22:[343.326:004.738.5
COBISS.RS-ID 6303768
DOI: 10.7251/ZRSNG1602072G

Optimizacija zaštite turističkih agencija od kompjuterskog kriminala

Security optimization of travel agencies from cyber crime

G. Grubor, N. Ristić, N. Simeunović, S. Adamović
Univerzitet Sinergija,Bijeljina, BiH

***Sažetak* - Nauka i praksa bezbednosti informacija na Internetu ušla je u svoju zreliju fazu. Dostupni su brojne metodologije za procenu rizika (preko 200), standardi zaštite, katalozi ranjivosti, pretnji i mera (kontrola) zaštite. Metodologija za procenu rizika informacija (ISO/IEC 27005:2008) usvojena je i u finansijskom sektoru u sporazumu BASEL II za procenu operativnog rizika. Iako standardizacija značajno smanjuje kompleksnost uvođenja sistema zaštite, implementacija osnovnih mera zaštite za smanjenje rizika na prihvatljiv nivo, još uvek je složena, skupa i zahteva specifična znanja i iskustva. Problem online krađe ličnih podataka i brojeva platnih kartica odnosi se upravo na turističke agencije gde klijenti masovno plaćaju račune platnim karticama. U ovom radu autori sugerišu optimalan okvir za upravljanje zaštitom informacija u Internet okruženju u turističkim agencijama, sa ciljem da se smanji kompleksnost i da se iste ohrabre da organizovano uvode sistem i praksu zaštite informacija, prema svojim potrebama i resursima.**

***Ključne reči* – pretnje, menadžment rizika, zaštita informacija, optimizacija zaštite, forenzička spremnost**

***Abstract* – Science and practice of information security on Internet come in its mature phase. Numerous risk management methodologies (over 200), security standards, lists of vulnerabilities and threats and security controls are available on Internet. Information risk methodology ISO/IEC 27005:2008 is adopted in financial sector through BASEL II agreement for assessment of operative risk. Though standardization essentially decreases establishment of security system and implementation of basic security controls for increasing risk to acceptable level, this process is still complex and costly, and requires specific knowledge and experience. Online stealing of personal data and credit cards credentials directly related to the touristic agencies, where clients pay bills by cards. In this piece of paper authors suggest an optimal information security management framework in Internet environment in travel agencies. Main goal of this work is to decrease complexity and to encourage travel agencies to implement information security system and practice through an organized method, according to their needs and resources.**

***Keywords* – threats, risk management, information security, optimal security, forensic readiness**

I. UVOD

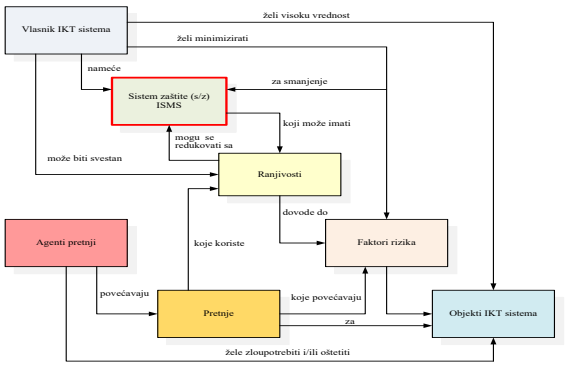
Svi standardi za upravljanje i zaštitu informacione imovine (čiste, fizičke i humane) ili informacija kao najznačajnije imovine [1], polaze od toga da se sistem zaštite i menadžment sistem bezbednosti informacija - ISMS (*Information Security Managament System*), uvode integralno na sistematičan i organizovan način uz punu podršku menadžmenta i obezbeđenje resursa uključujući kvalifikovan tim za procenu rizika i zaštitu informacija. Za projektovanje i implementaciju ISMS u turističkim agencijama (TA) na raspolaganju su široko prihvaćeni međunarodni standardi najbolje prakse za: upravljanje rizikom; mere (kontrole) za smanjenje rizika na prihvatljiv nivo; opšte prihvaćene principe zaštite; sertifikaciju i akreditaciju ISMS; metrike zaštite; integraciju digitalne forenzike u sistem zaštite itd. [2, 3, 4, 5, 6, 7, 8, 14, 15, 16, 19, 20, 21]. Kako implementacija ISMS generalno zahteva značajne resurse, u praksi se često zaštita informacija pojedostavljuje, improvizuje bez procene rizika i neadekvatno primenjuje što je možda i glavni razlog za optimizaciju, pošto se stvara iluzija o zaštiti, a istovremeno brojni gosti izlažu riziku *online* krađe brojeva platnih kartica i privatnih informacija iz lokalnih baza podataka TA.

Iako je praktična primena ovih standarda još uvek kompleksna i skupa, uz brojne instrukcije za primenu procesnog modela - PDCA (*Plan, Do, Chack, Act*) [1, 12] za projektovanje i implementaciju ISMS, moguće je izvršiti samoprojektovanje i implementaciju ISMS, kao prvi stepen optimizacije. Ipak implementacija ISMS u realni sistem zahteva specijalistička znanja, iskustva i veštine u procesima *menadžmenta rizika, izbora i implementacije mera zaštite.* U tom smislu, moguće je izvršiti optimizaciju određenih parametara u oba procesa, kao što su: izrada liste inventara informacione imovine (čiste informacione, fizičke i humane imovine [1]; izbor dostupne i intuitivne metodologije za procenu rizika kritičnih informcija [11, 13]; izbor broja faktora rizika za inicijalnu i regularnu procenu; prilagođavanje standardnih lista ranjivosti i pretnji kontekstu TA; izbor proceduralnih i tehničkih kontrola zaštite za smanjenje rizika na prihvatljiv nivo i određivanje prioriteta tretmana rizika [2, 4] itd.

U ovom radu autori sugerišu jedan optimalan upravljački okvir zaštite - SMF (*Security Management Framework*) za male i srednje TA, koji uključuje optimalan set standarda iz oblasti zaštite informacija, autorskih radova [12], instrukcija, dijagrama procesa i procedura za projektovanje, razvoj, implementaciju i održavanje ISMS [10, 12]. Cilj je da se smanji kompleksnost i da se manje i srednje TA ohrabre da organizovano uvode ISMS primerenu svojim potrebama i resursima.

II. FUNKCIONALNI MODEL UVOĐENJA SISTEMA ZAŠTITE INFORMACIJA

Svi aspekti zaštite informacija i ISMS u Internet okruženju mogu se sagledati iz funcionalnog modela sistema zaštite (Sl. 1).

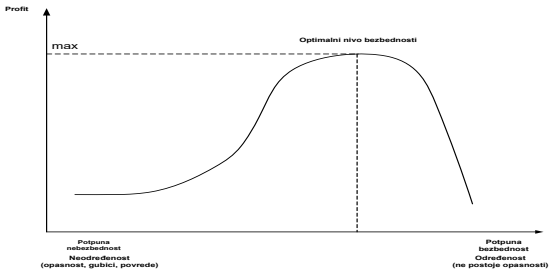


Slika 1. Funkcionalni model sistema zaštite informacija

Vlasnik sistema želi da implementira ISMS i sačuva *poverljivost, integritet i raspoloživost* (PIR) informacija od brojnih agenata pretnji (spolja i iznutra), integralnim uvođenjem ISMS i s/z za smanjenje faktora rizika na prihvatljiv nivo. Objekti zaštite su primarno informacije. Vlasnici sistema *politikom zaštite* nameću zahteve za uvođenje ISMS i s/z kroz implementaciju *proceduralnih* (upravljačkih (U), organizaciono-operativnih (O)) i *tehničkih* (T) kontrola zaštite [8, 2], sa ciljem da smanje uticaj pretnji na ranjivosti informacione imovine, odnosno, ukupan rizik imovine na prihvatljiv nivo.

III. FUNKCIONALNI MODEL OPTIMALNOG SISTEMA ZAŠTITE KRITIČNIH INFORMACIJA

U opštem slučaju pod optimalnim rešenjem ISMS podrazumeva se rentabilan i funkcionalno efektivan skup mera zaštite, koji u datim uslovima i uz najracionalniju raspodelu resursa na najbolji način zadovoljava sve zahteve zaštite [11] (Sl. 2).



Slika 2. Optimalan sistem zaštite

Dijagram na sl. 2 sugeriše da nije racionalno ulagati u skupe sisteme zaštite u toj meri da troše profit agencije, a ne doprinose povećanju nivoa bezbednosti informacija. Ovo tim pre što je realnoj praksi praktično nemoguće implementirati sistem apsolutne zaštite (iako je teoretski moguće!), pošto zahteva neograničene materijalne, finansijske i ljudske resurse koje nijedan poslovni sistem na svetu ne može obezbediti.

Optimizacija ISMS zahteva racionalizaciju brojnih parametara, kao što su procesi procene rizika, izbora, implementacije i redukcije kombinovanih m/z, troškova obuke zaposlenih itd. U procesu optimalnog, integralnog uvođenja ISMS i osnovnog s/z informacija u poslovni informacioni sitem (PIS) TA, glavni koraci su: obezbeđivanje eksplicitne podrške menadžmenta i resursa TA; organizovanje internog projektnog tima za procenu rizika kritične imovine; planiranje, implementacija, održavanje i poboljšanje ISMS i s/z. Projektni tim treba da uključuje minimalno specijalistu zaštite, administatore sistema i mreže, izvršnog menadžera, pravnika i menadžera za upravljanje ljudskim resursima. Prvi stepen optimizacije ostvaruje se integralnim procesima uspostavljanja s/z i ISMS. Naime, implementacija ISMS podrazumeva procenu faktora rizika i tretman rizika sa U, O i T merama zaštite za smanjenje rizika na prihvatljiv nivo. Kako su U,O i T kontrole zaštite suštinski deo s/z, može se smatrati da se korektnom PDCA implementacijom ISMS, implementira i s/z. Za optimalan pristup, potrebno je planirati samo ključne PDCA faze projekta implementacije ISMS: *uspostavljanje, implementacija, održavanje i poboljšanja* Ključne PDCA faze ISMS sa kratkim opisom i izlaznim rezultatima svake faze, prikazane su u Tabeli 1.

TABELA 1. KLJUČNE FAZE PROJEKATA PLANIRANJA, IMPLEMENTACIJE, ODRŽAVANJA I POBOLJŠANJA ISMS

R.b.	Faza projekta	Kratak opis	Izlaz
1.	Izrada i usvajanje *politike zaštite informacija*	Napisane i usvojene modularne politike: *ISMS, Upravljanje lozinkom*, *Udaljeni pristup i mobilni rad*, *Upravljanje rizikom* itd., zavisno od tipa i potreba TA. Usvojen PDCA procesni model i plan uspostavljanja ISMS-a [1]	*Politika zaštite informacija*
2.	Organizacija projektnog tima za ISMS	U tim uključiti: specijaliste zaštite i procene rizika (zaposleni ili iznajmljeni), projektanta IS, administratore sistema i mreže, pravnika, izvršnog menadžera i menadžera za ljudske resurse. Timove organizovati po potrebi.	Tim za zaštitu
3.	Inventar imovine	Iventarisati *čistu, fizičku i humanu* imovine i izraditi liste sa prioritetima vrednosti za poslovanje, u odnosu na PIR, rangiranim sa: *nizak* (N), *srednji* (S) i *visok* (V) ili 1, 2, 3.	Lista imovine
4.	Procena rizika (R)	*Standardne* liste ranjivosti i pretnji [1] ažurirati u odnosu na kontekst TA. Izabrati metodologiju za procenu rizika [5, 13]. Organizovati privremeni tim za analizu i procenu rizika. Proceniti kritične faktore rizika sa listom prioriteta, grupisanih u: N,S,V kategorije.	Lista N,S,V faktora rizika
5.	Izbor i implementacija mera zaštite (m/z)	Iz kataloga m/z [2, 4] tim bira optimalno kombinovane U, O i T m/z sa obrazloženjem izostavljenih i novo uvedenih m/z i predlogom akcionih planova prioriteta za implementaciju, kroz 4-fazno ublažavanje V, S, N faktora rizika [13], a prema potrebama i resursima TA.	Anex A ISO/IEC 27001:2013
6	Usvajanje plana tretmana R	Usvajanje dokumenata *Plan tretmana rizika* ili *Izjava o primenljivosti* – SoA (*Statement of Aplicability*) predložen od strane tima za ISMS [2, 4]	Odobren SoA dokument
7.	Rad i održavanje ISMS	U operativnom radu neprekidno monitorisati ISMS u domenu odgovornosti zaposlenih u TA. Administratori zaštite operativno održavaju ISMS. Menadžment vrši menadžersku	Izveštaji menadžerske i

R.b.	Faza projekta	Kratak opis	Izlaz
		reviziju barem jedanput godišnje sa težištem na kontroli dokumentacije zaštite i usaglašenosti sa praksom, standardima i politikom zaštite. Menadžer ISMS organizuje, tim za internu reviziju i po potrebi/zahtevu priprema ISMS za nezavisnu sertifikaciju [11].	interne i nezavisne revizije ISMS
8.	Poboljšanje ISMS	Rezultati revizija ISMS koji ukazuju na propuste i neusaglašenosti zahtevaju korektivne akcije u realnom vremenu.	Procedure za korektivne akcije
9.	Reinženjering ISMS	U skladu sa organizacionim promenama u TA, promenama u IKT i tehnologijama zaštite, kao i promenama u naprednim tehnikama malicioznih napada iznutra ili spolja, preduzimati reinženjering ISMS u novom cikličnom PDCA procesu.	Plan reinženjeringa ISMS

Faze proces uspostavljanja, implementacije, održavanja i poboljšanja ISMS, sugerisane u Tabeli 1 zasnivaju se na standardima najbolje prakse zaštite i praktičnim iskustvima autora. Za uspostavljanje ISMS najznačajnije je obezbediti eksplicitnu podršku menadžmenta TA, kroz odobrenu i objavljenu *ISMS politiku zaštite,* koja odražava nameru TA da uvede ISMS. Ako u TA nema zaposlenih specijalista zaštite ili informatičara koji su polagali predmete o zaštiti informacija, treba ih uključiti kao spoljne konsultante za sve faze PDCA procesa. U fazi održavanja implementiranog ISMS i slučajevima kompjuterskog incidenta, u tim za zaštitu treba, po mogućnosti, uključiti i digitalnog forenzičara (zaposliti ili angažovati kao konsultanta) za oporavak sistema i istragu napada. Inventar imovine TA treba da uključi sve resurse, rangirane prema značaju za poslovanje i misiju TA. Standardi [5, 13] sugerišu kvalitativnu metodu procene rizika i rangiranje svih parametara analize rizika sa N,S,V. Praksa je pokazala da male i srednje TA retko primenjuju metodološku procenu rizika informacija [5, 13, 15]. U pokušaju optimizacije svih aspekata upravljanja rizikom i ISMS na raspolaganju je nekoliko modela i standarda zaštite. Autori sugerišu intuitivne i besplatne BAR (*Brzu analiza rizika*) ili OCTAVE (*Organizational Critical Trate, Asset and Vulnarability Evaluation*) analize rizika [12] za inicijalnu procenu kritičnih faktora rizika, koje izvršni menadžeri i zaposleni u TA najbolje poznaju. Inicijalna procena rizika kritične imovine može se izvršiti i primenom BAR analize rizika [10] posebno za TA koje nemaju iskustva u proceni rizika. Brza analiza rizika uključuje informatičara koji poznaje osnovnu metodologiju procene rizika i zaposlene u procesima TA koji najbolje poznaju ranjivosti, pretnje i potencijalne rizike. Proces BAR analize rizika podrazumeva bezbednosnu kategorizaciju imovine u grupe sa zajedničkim bezbednosnim ciljevima, čime se dodatno smanjuje kompleksnost sistema zaštite. Bezbednosna kategorizacija se vrši u odnosu na PIR parametre informacione imovine po principu najvećeg rizika. Na primer, ako se rizik servera za P procenjuje sa nizak - N (P), za I srednji - S(I), a za R visok - V(R), onda se server svrstava u grupu sa najvećim rizikom (V). Takođe, proces BAR analize zahteva i poznavanje tokova informacija i međuzavisnosti između bezbednosnih zona kategorija informacione imovine, što najbolje poznaju zaposleni u procesima TA. Tako modeli OCTAVE nude samoevaluacione procese za male i velike agencije sa četverofaznom prioritetnom implementacijom m/z za smanjenje visokih faktora rizika kritične imovine za poslovanje i misiju TA. Kroz ovu procenu rizika TA stiče neophodna iskustva za detaljnu i regularnu procenu rizika koja se zahteva standardima [22], posebno za e-poslovanje. Za analizu i procenu velikog broja faktora rizika kod većih TA, može se koristiti interaktivna softverska aplikacija *Hestia* [22]. U izboru i predlogu m/z za smanjenje rizika do prihvatljivog nivoa, tim treba da sugeriše više jeftinijih proceduralnih, a manje skupljih tehničkih m/z u skladu sa kapacitetima i resursima TA. Plan implementacije m/z realizuje se na osnovu odobrenog SoA dokumenta, optimalno sa projektima u četiri faze [12]. U prvoj fazi treba implementirati m/z za smanjenje najvećeg broja (ili svih) **V** faktora rizika, ostatak **V** faktora i veći broj **S** faktora rizika u drugoj fazi, najveći broj **S** fakora rizika u trećoj fazi, a ostatka **S** faktora rizika u četvrtoj fazi. Sve N faktore rizika treba neprekidno monitorisati, jer vremenom mogu preći prag prihvatljivosti. Sve projekte zaštite dobro je planirati u jednoj fiskalnoj godini, da bi se osigurala dostupnost obezbeđenih resursa. Ovakav pristup rasterećuje godišnji budžet za zaštitu, a ne ugrožava bezbednost informacija. Nezavisna sertifikacija ISMS TA prema standardu [2] je dobra praksa, jer obezbeđuje konkurentsku prednost na e-tržištu. Procesi zaštite se po svojoj prirodi ciklično neprekidno obnavljaju i zahtevaju poboljšanja, zavisno od promena u organizacionoj strukturi TA, IKT i tehnologijama zaštite, kao i od sve veće sofistikacije napada koji zahtevaju uvođenje proaktivnih i prediktivnih (inteligentnih) m/z. U uslovima rapidnog porasta kibernetičkog (eng. *cyber*) kriminala (iznosi 59% od ukupnog kriminala, prema *Gartner Groop*, 2012) i sofisticiranih ciljnih napada nultog dana (istog dana je otkrivena i iskorišćena ranjivost za napad), realno treba očekivati proboj s/z. Oporavak PIS i trajno otklanjanje uzroka napada, pored otklanjanja posledica, može obezbediti samo kompetentan digitalni forenzičar [8]. U nastojanju dalje optimizacije resursa i smanjenja kompleksnosti implementacije održivog ISMS u PIS malih i srednjih TA, zahteva se integrisanje *digitalnog forenzičara* sa potrebnim znanjima, tehnikama i alatima u tim za upravljanje kompjuterskim incidentom.

Kritične mere zaštite (k/m/z) se definišu kao set najefektivnijih, specifičnih proceduralnih i tehničkih m/z za detekciju, sprečavanje, odgovor ili ublažavanje štete od najčešćih, sofisticiranih kibernetičkih napada, uključujući i detekciju kompromitovanih mašina u mreži i sprečavanje daljih akcija napadača [17]. Ove k/m/z su rezultat iskustava i znanja globalne interesne zajednice za zaštitu informacione imovine [1, 2, 3, 4, 17], iako nisu potpuna zamena za formalnu, sveobuhvatnu procenu i tretman rizika informacione imovine [5]. U dostupnim katalozima m/z broj ovih kontrola za formalnu zaštitu iznosi od 114 [5] do 198 [13], a za implementaciju zahtevaju značajne resurse, dosta rada, znanja i iskustava. S druge strane, k/m/z su fokusirane na manji set prioritetnih kontrola za ublažavanje rizika kritične informacione imovine za poslovanje i misiju TA, po principu „*što se mora uraditi*“. Zato se set k/m/z mora smatrati inicijalnim sistemom osnovne zaštite (SOZ). Pri tome se za SOZ zahteva procena rizika kritične imovine, izbor i implementacija k/m/z koju individualne agencije mogu proaktivno izvršiti, pre standardne, detaljne procene i tretmana rizika [5].

Kritične mere zaštite treba da obezbede da se:

- iskustva iz napada primenjuju za odbranu od napada;
- prioritetno ublažavaju posledice uticaja najvećih (**V**) faktora rizika;
- ugrađuju i prate metrike za merenje efektivnosti implementiranih k/m/z;

- vrši neprekidna dijagnostika efektivnosti k/m/z i ublažavanja rizika;
- uvodi neki stepen automatizacije procesa ublažavanja rizika.

Implementirane k/m/z treba da obezbede:

- *Brze efekte* proceduralnih i tehničkih m/z koje ostvaruju značajno ublažavanje rizika bez glavnog finansijskog ulaganja, kao što su: praćenje aplikacija sa bele liste (ne samo crne liste), primena standarda i bezbedne hardversko-softverske konfiguracije, primena bezbednosnih popravki (*peches*) u toku 24h, ograničavanje privilegovanih naloga, primena sistemskih mera zaštite [10] itd.

- *Vidljivost i merenje doprinosa* kontrola za poboljšanje procesa, arhitekture i tehničkih m/z kroz monitoring mreže, detekciju upada, identifikaciju kompromitovanih mašina itd.

- *Poboljšanje konfiguracije PIS i s/z informacija* za smanjenje mrežne ranjivosti.

- *Napredne (prediktivne, inteligentne) mere zaštite* koje primenjuju nove T m/z za maksimalnu zaštitu, automatizaciju metrika, merenje efektivnosti kontrola i lakšu praktičnu implementaciju.

Predloženi detaljni model k/m/z [17] suštinski integriše proaktivnu mrežnu forenziku. Glavni zahtev za proaktivnu mrežnu forenziku je jak monitoring sistem računarske mreže PIS-a, centralno logovanje u zaštićenom log serveru log datoteka svih aktivnih mrežnih uređaja za registrovanje bezbednosno i forenzički relevantnih podataka, što predstavlja značajan doprinos optimizaciji ISMS. U Prilogu 1 dat je optimalan set k/m/z sa uključenim merama proaktivne mrežne forenzike.

Optimizacija ISMS i s/z primenom seta k/m/z [17] podrazumeva da TA iz preporučenog seta bira proceduralne i T m/z u skladu sa realnim stanjem bezbednosti informacione imovine u kontekstu TA i raspoloživim resursima – skupe T ili jeftinije proceduralne m/z. Implementacija optimalnog sistema zaštite zahteva sveobuhvatan, procesni i sistem inženjerski pristup sa aktivnim učešćem i radom svih informatičara (programera, projektanata i analitičara) pored specijalista zaštite i digitalne forenzike. Određen stepen optimizacije ISMS i s/z nudi i ISMS standard [2] kroz usvajanje SoA dokumenta kada menadžment agencije (ne)prihvati predloženi set m/z za smanjivanje procenjenog rizika na prihvatljiv nivo. Dokument SoA je u stvari lista kontrola zaštite iz Aneksa A standarda [2] sa obrazloženjem isključenih kontrola zaštite. Predloženi sistem k/m/z optimalne zaštite nudi veću slobodu izbora i kombinovanja k/m/z u skladu sa resursima TA.

IV. Zaključak

Kompleksnost i troškovi implementacije kontrola (mera) zaštite u ionako kompleksne PIS postaje prepreka za aktivno upravljanje (otkrivanje, praćenje, sprečavanje, ublažavanje) brojnim faktorima rizika za informacionu imovinu. Posledice su improvizacija implementacije k/m/z, bez procene rizika i sa ugradnjom samo univerzalnih, proceduralnih (sistemskih mera razdvajanja dužnosti, ograničenja privilegija, dužne pažnje itd.) i tehničkih k/m/z (*firewalls* i antivirusne zaštite). Ovakvim pristupom se neoptimalno troše svi resursi agencije, ne obezbeđuje se sveobuhvatna zaštita i, što je najgore, stvara se iluzija o dobroj zaštiti informacione imovine. U slučaju glavnog incidenta i nanete materijalne i nematerijalne štete PIS-u, menadžment često pristupa kupovini najskuplje tehnologije za prekomernu i redundantnu zaštitu, što je još dalje od optimalne zaštite. Predloženi model k/m/z obezbeđuje zaštitu kritične informacione imovine agencije od *visokih* faktora rizika, a time u velikoj meri i od *srednjih* i *niskih* faktora rizika, pošto uključuju neprekidan nadzor i praćenje eskalacije svih faktora inicijalne procene rizika. Autori ovog rada za sistem osnovne zaštite predlažu kombinovanje inicijalne BAR analize rizika i ublažavanje sa setom kritičnih proceduralnih i tehničkih kontrola zaštite, kao optimalni inicijalni sistem osnovne zaštite informacione imovine koji najveći broj malih i srednjih TA može obezbediti kombinujući raspoložive resurse i predložene k/m/z. Uspostavljanje, implementacija, održavanje i poboljšanje optimalnog ISMS u malim i srednjim TA, podrazumeva aktivni rad informatičara, administratora sistema i mreža, programera, projektanata i analitičara u informatičkim odeljenjima TA u timovima za zaštitu, procenu rizika i upravljanje kompjuterskim incidentom.

Literatura

[1] ISO/IEC 27001:2005, *Informacione tehnologije –Tehnike zaštite – Menadžment sistem zaštite informacija – Zahtevi,* www.iso27001standard.com.

[2] ISO/IEC 27001:2013, *Informacione tehnologije – Tehnike zaštite – Menadžment sistem zaštite informacija – Zahtevima* www.iso27001standard.com.

[3] ISO/IEC 17799:2005, *Information technology – Security techniques – Code of practice for information - security management,* www.iso17799standard.com.

[4] ISO/IEC 27002:2013, *Information technology – Security techniques – Code of practice for information security managament,* www.iso27002standard.com.

[5] ISO/IEC 27005:2008, *Information technology – Security Techniques – Information security risk Management,* www.iso27005standard.com.

[6] ISO/IEC 27006, *Information technology — Security techniques— Requirements for bodies providing audit and certification of information security management systems,* 2007.

[7] *Generaly Accepted Information Security Principless* (*GAISP*) *V.3.0,* http://www.gaisp.org, 2007.

[8] Karen K., at all., *Guide to Integrating Forensic Techniques Incident Response,* NIST SP 800-86, 2006.

[9] S.T.Arnson, K.D.Willet, *2001 Certification – An Example of Complied Management*, Taylor&Francis Group, 2008.

[10] G.Grubor, M.Milosavljević, *Osnovi zaštite informacija*, Singidunum, 2011.

[11] G.Grubor, *Projektovanje menadžment sistem bezbednosti informacija*, Singidunum, 2011.

[12] *Introduction to the OCTAVE Approach*, http://www.cert.org/octave, 2005.

[13] G. Stoneburner, A. Goguen, and A. Feringa, NIST SP 800-30, *Risk Management Guide for Information Technology Systems,* 2008.

[14] R. Ross, A. Johnson, S. Katzke, P. Toth, G. Stoneburner, G. Rogers,, NIST SP 800-30, *Guide for Assessing the Security Controls in Federal Information System,* 2008.

[15] J.Hansen, L. Nilsson, *Risk Management: A New Approach To Improving Safety*, Sweden National Report, Strategic Direction Session ST 3, 2007.

[16] L. Hayden, *IT Security Metrics: A Practical Framework for Measuring Security& Protecting Data*, 2010.

[17] Council on Cyber Security, *The Critical Security Controls for Effective Cyber Defense, V.5.0,* 2015.

[18] Information Security & Business Continuity Academy, *ISO 27001 implementation checklist,* 2013

[19] NIST SP 800-14, *Generally Accepted Principles and Practices for Security*, http://csrc.nist.gov/publications/nistpubs/800-14/sp800-14.pdf, 2002.

[20] NIST SP 800-53, *Recommended Security Controls For Federal IS*, http://csrc.nist.gov/publications/nistpubs/800-53/sp800-53.pdf, 2004.

[21] Swanson M., & all, *Security Metrics Guide for Information Technology Systems*, NIST SP 800-55, http://csrc.nist.gov/publications/nistpubs/800-55/sp800-55.pdf, 2003.

[22] D. Adelsberger, *Upravljanje rizicima za ISO 27001 pomoću programa HESTIA ISMS*, Festival kvaliteta 2008, Kragujevac, 25-28 maj 2008, http://www.cqm.rs/2008/pdf/35/11.pdf

PRILOG 1: TABELA 2. PREGLED OPTIMALNOG SETA KRITIČNIH MERA ZAŠTITE

Rb.	Grupa k/m/z	Funkcionalni opis	Alati za implementaciju
1.	Inventar (ne)licenciranog mrežnog hardvera (hw) PIS-a (**7 k/m/z**)	Aktivno inventarisanje, praćenje i korigovanje svih hw mrežnih uređaja i davanje prava pristupa samo licenciranim uređajima. Za implementciju koristiti T i proceduralne m/z	Tehnički i proceduralni. Na primer aktivni i pasivni skeneri RM.
2.	Inventar (ne)licenciranog softvera u RM PIS-a (**9 k/m/z**)	Aktivno inventarisanje, praćenje i korigovanje svih sw sistema u mreži i instaliranje samo licenciranih sw. Za implementaciju se zahteva primena *bele i crne liste* sw-a i vendora antivirusnih sw.	Bele liste sw. Komercijalni alati za inventar licenciranosti sw na bazi izvršne putanje, heša, sertifikata itd.
3.	Uspostavljanje bezbedne konfoguracije hw i sw PIS (**10 k/m/z**)	Uspostavljanje, implementacija i aktivno upravljanje bezbedne konfiguracije servera, radnih stanica, laptopova i mobilnih uređaja radi sprečavanje napada. Koristiti javno dostupne kontrolne (ček) liste, umesto osnovnog s/z za svaki sw.	Prilagoditi dostupna *banchmark* uputstva (www.cisecurity.org), ček liste (www.checklists.nist.gov) i alate *ISMS politici zaštite*.
4.	Monitoring i stalna procena ranjivosti PIS-a i remedijacija (**10 k/m/z**)	Neprekidno otkriva, procenjuje i preduzima korektivne akcije za smnjenje ranjivosti i prilika za napade. Zahteva alate (skenere) za otkrivanje ranjivosti sistema i mreža i testiranje na proboj.	Skeneri ranjivosti računarskih sistema i mreža i nebezbedne konfiiguracije. Alati za automatsko ažuriranje pečeva.
5.	Antivirusna zaštita (avz) (**11 k/m/z**)	Kontrola instalacije, širenja i izvršavanja melvera na više tačaka u RM TA i optimizacija automatskog ažuriranja avz, skupljanje i uklanjanje malvera. Zahteva se centralizovano upravljanje avz i HIDPS/NIDPS sistemima, uključujući i *honeypots*.	Automatizovani alati za centralno upravljanje avz, NIDPS sistemi i *honeypots* i centralizovano logovanje bezbednosnih događaja.
6.	Zaštita aplikativnog sw (**11 k/m/z**)	Upravljanje životnom ciklusom razvijenih i kupljenih aplikacija i sprečavanje, detekcija i korekcija bezbednosnih ranjivosti. Zahteva se proizvodnja bezbednog sw.	Kompleksni U,O,T alati (*firewalls, skeneri ranjivosti*) za zaštitu internih i web aplikacija. (*www.owasp.org)*
7.	Monitoring i kontrola bežičnog pristupa PIS-u (**10 k/m/z**)	Procesi i alati za aktivno upravljanje bežičnom lokalnom mrežom (WLAN), pristupnom tačkom i sistemima klijenata. Zahtevaju se komercijalni/otvoreni alati za skeniranje, detekciju i otkrivanje upada u WLAN mreže.	Skeneri ranjivosti WLAN i bežični IDS monitoring sistemi. Skeneri (npr. *Kali*) bežičnog saobraćaja. Bezbedna konfiguracija sistema i mreže.
8.	Forenzički kapaciteti za oporavak podataka kompromitovanog sistema (**4 k/m/z**)	Procesi i alati za bekapovanje sistemskih i aplikativnih sw, informacija i podataka. Upotreba tehnika i alata proaktivne mrežne forenzike - sistem jakog monitoringa RM, centralnog logovanja bezbednosno/forenzički relevantnih događaja i forenzičkih alata za oporavak podataka i sistema.	Sistemi za bekapovanje sistemskog i aplikativnog softvera. Forenzički alati za oporavak podataka i otkrivanje uzroka napada.
9.	Procena bezbednosnih znanja i veština i adekvatna obuka (**5 k/m/z**)	Obezbediti za svaku ulogu, a prioritetno kritične za obavljanje misije TA, identifikaciju specifičnih znanja i veština potrebnih za zaštitu i preduzimati korektivne akcije kroz planove, politiku zaštite, specijalizovanu obuku i razvoj *svesti o potrebi zaštite*.	*Politikom zaštite* definisati ciljnu obuku zapolsenih za svaku promenu i usaglasiti sa k/m/z i preporukama (*EU Council on Cyber Security, NIST).*
10	Bezbedna konfiguracija aktivnih mrežnih uređaja -*firewalls*, rutera i svičera (**6 k/m/z**)	Uspostavljanje, implementacija i aktivno upravljanje bezbednom konfiguracijom aktivnih mrežnih uređaja, primenom alata za rigorozno upravljanje konfiguracijom i promenama, alata za filtriranje saobraćaja u mreži i lista za kontrolu pristupa (ACL).	Komercijalni alati za evaluaciju skupa pravila za filtriranje ili ACL mrežnih uređaja posle svake značajnije organizacione ili tehnološke promene.
11	Ograničavanje portova/ protokola/servisa RM (**7 k/m/z**)	Aktivno upravljanje tekuće operativne upotrebe portova, protokola i servisa mrežnih uređaja radi smanjenja ranjivosti i prilika za napad. Za implementaciju zahteva skenere portova.	Aktivni skeneri portova, mrežnog saobraćaja i web sajtova.
12	Kontrolisana upotreba privilegovanih naloga (**14 k/m/z**)	Procesi i alati za aktivno upravljanje upotrebom, zadacima i konfiguracijom adminstrativnih privilegija na računarima, RM i aplikacijama. Za implementaciju zahteva redovnu kontrolu i ažuriranje liste naloga sa superkorisničkim privilegijama	*Politikom zaštite* zahtevati upotrebu jakih korisnički izabranih pasvorda, kontrolu i smanjenje privilegovanih naloga i 2-slojnu autentifikacija za administratorske naloge.
13	Zaštita perimetra (DMZ) mreže (**14 k/m/z**)	Aktivno upravljane toka informacija iz RM sa fokusom na bezbednosno kritične podatke. Implementacija zahteva bezbednu konfiguraciju uređaja RM i uspostavljanje DMZ domena zaštićenog sa dva *firewalls* - do Interneta i do intraneta.	Bezbednosna segmentacija mreže uspostavljanjem DMZ, NIDPS*, sniferskih alata mrežnih paketa i forenzičkih alata za praćenje napada.
14	Monitoring, održavanje. analiza i centralno upravljanje *log* fajlova (**10 k/m/z**)	Skupljanje, upravljanje i analiza *log* fajlova za reviziju događaja za otkrivanje, razumevanje i oporavak sistema od napada. Implementacija zahteva konfigurisanje logova aktivnih mrežnih uređaja za centralno logovanje bezbednosno i forenzički relevantnih događaja u zaštićen log server.	Bezbednosno konfigurisanje svih aktivnih mrežnih uređaja i centralno logovanje podataka. Skeneri log datoteka za analizu napada. Specijalisti zaštite i digitalne forenzike.
15	Kontrolisani pristup PIS-u na bazi „*znati samo što treba*“ (**5 k/m/z**)	Procesi i alati za aktivno upravljanje pristupom kritičnoj imovini, zasnovanim na klasifikaciji uloga u agenciji i potreba za obavljanje poslova. Zahteva se bezbednosna kategorizacija.	*Politikom zaštite* zahtevati bezbednosnu ktegorizaciju osetljivih informacij, DMZ i RBAC** kontrolu.
16	Monitoring i kontrola korisničkih naloga (**17 k/m/z**)	Aktivno upravljanje životnim ciklusom sistemskih i aplikativnih naloga. Za implementaciju zahteva se omogućavanje logovanja upotrebe naloga i centralno upravljanje nalozima.	Kontrola i praćenje upotrebe naloga ACL/ACM***. Analizatori logova AC.
17	Zaštita osetljivih podataka (**15 k/m/z**)	Procesi i alati za sprečavanje i ublažavanje oticanja podataka, zaštite privatnosti i integriteta osetljivih informacija. Zahteva se kombinovana primena alata za šifrovanje i sprečavanje gubittka podataka u prenosu, mobilnom radu i *cloud*-u.	Alati za kriptozaštitu, upravljanje ključem i sprečavanje oticanja podataka primenom DLP (*Data Likage Protection*) alata.

Rb.	Grupa k/m/z	Funkcionalni opis	Alati za implementaciju
18	Prvi odgovor i upravljanje kompjuterskim incidentom (**7 k/m/z**)	Razvoj i implementacija infrastrukture *proaktivne mrežne forenzike* za odgovor na incident, brzo otkrivanje napada, blokiranje pristupa napadača, efektivno saniranje štete i restauraciju integriteta mreže i sistema. Zahteva vanrednog događaja kroz obuku i simulacije napada i uključivanje digitalnog forenzičara u tim upravljanje incidentom.	Periodična obuka scenarija napada (incidenta), prvog odgovora na incident i oporavka sistema. Procedura za upravljanje incidentom i BCM****. Infrastruktura *korporacijske digitalne forenzičke istrage*.
19	Sistem inženjerski i PDCA procesni pristup bezbednosti PIS (**4 k/m/z**)	Osigurati bezbednost PIS TA kroz specifikaciju, projektovanje i implementaciju optimalnih k/m/z koje omogućavaju siguran rad, smanjujući prilike za napade. Zahteva održavanje ažurnog mrežnog dijagrama aktivnih uređaja, arhitekture i servisa na najvišem nivou bezbednosti.	Bezbedna arhitektura RM (DMZ, segmentacija, 3-slojna arhitektura DNS) zahtevana *politikom zaštite* i podržana dijagramima topologije RM i mrežnih servisa.
20	Testiranje na proboj i jačanje bezbednosne i forenzičke spremnosti (**8 k/m/z**)	Testiranje ukupne bezbednosne i forenzičke spremnosti i kapaciteta TA kroz simulaciju ciljeva i akcija napadača. Zahteva se uključivanje digitalnog forenzičara u tim za zaštitu informacija.	Procedura preventivnog testiranja sistema na proboj (alati tipa *Metasploit*) i trajno otklanjanje uzroka napada forenzičkim alatima.
Legenda:		**NIDPS***- Mrežni detektor upada u sistem; **HIDPS**- Detektor upada u računarski sistem **RBAC****- Kontrola pristupa na bazi uloga; **ACL/ACM*****-lsta kontrola pristupa/Matrica kontrola pristupa BCM****-Menadžment kontinuiteta poslovanja	