ZAGOTAVLJANJE INFORMACIJSKE VARNOSTI V SODOBNEM IZOBRAŽEVALNEM OKOLJU

Information security assurance in a modern education environment

Dr. Marjeta Pučko
Šolski center Kranj, EQIPerspectum
marjeta.pucko@guest.arnes.si, marjeta.pucko@gmail.com

Povzetek

V prispevku predstavljamo trende na področju informacijskih varnostnih groženj v Sloveniji in svetu. Na osnovi analize skupin ključnih tveganj definiramo smernice za informacijsko varnost v izobraževalni inštituciji. Smernice vključujejo tehnologijo, IKT opremo ter procese in organizacijske ukrepe vključno z ozaveščanjem uporabnikov. Predstavljeni so tudi aktualni pristopi k analizi podatkov v informacijskem sistemu izobraževalne inštitucije, ki pomagajo pri prepoznavanju obstoječih in potencialnih groženj na področju informacijske varnosti. Posebno pozornost namenjamo oddaljenemu dostopu do informacijskega sistema in uporabi mobilnih naprav.

Ključne besede: *informacijska varnost, varnostne grožnje, izobraževalno okolje, IKT, procesi.*

Abstract

In the article, trends of information security threats in Slovenia and globaly are presented. Basic guidelines for information security assurance in an educational institution are defined including technology, ICT equipment, processes and necessary organizational measures to make users aware of cyber security threats. In addition, up-to-date approaches to data analysis in an information system of an educational organization are presented helping to identify present and potential information security threats. Special attention is given to security issues of remote access to an information system and use of mobile devices.

Keywords: *information security, information security threats, education environment, ICT, processes.*

1 Uvod

Objave v različnih medijih nas praktično vsakodnevno seznanjajo z različnimi nevarnostmi pri uporabi svetovnega spleta in naraščanjem spletnega kriminala. Specifika informacijske varnosti interneta je v tem, da je internet kot globalno omrežje tudi globalni izvor potencialnih varnostnih groženj za kateregakoli zasebnega oziroma domačega uporabnika, podjetje ali inštitucijo. Čeprav izobraževalne inštitucije po dejavnosti ne sodijo med organizacije z najvišjimi zahtevami za nivo varnosti kot npr. finančne organizacije ali državna uprava, pa prav tako zahtevajo celoten spekter ukrepov v okviru varnostne politike, posebej v tistih izobraževalnih inštitucijah, v katerih so udeleženci izobraževalnega procesa otroci oziroma mladoletne osebe.

V prispevku predstavljamo bistvene elemente sistema varovanja informacij izobraževalne inštitucije: tehnologija, oprema, procesi, zaposleni, udeleženci izobraževanja. Za vsak element sistema je izdelana kratka analiza zahtev in podan predlog rešitev, pri čemer upoštevamo sistem varovanja kot celoto z medsebojnimi povezavami in učinki posameznih elementov po mednarodnem standardu ISO/IEC 27001:2013 (SIST ISO/IEC 27001, 2013).

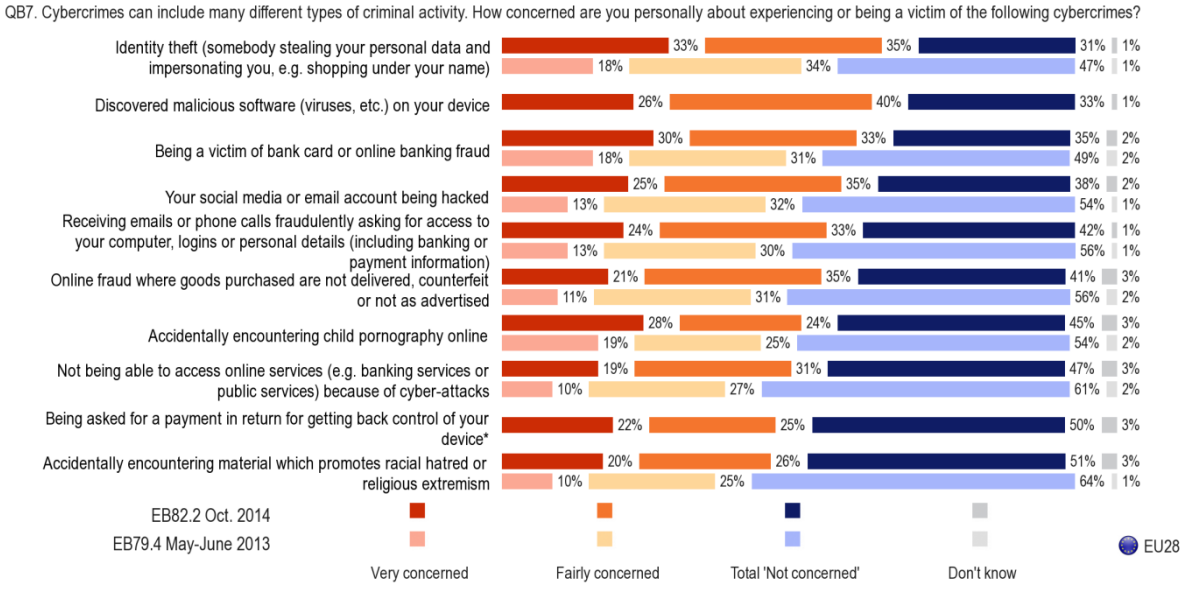
Osnovne zahteve za varnost informacij po omenjenem standardu, hkrati pa tudi varnostna tveganja, grožnje in z njimi povezani varnostni incidenti, se nanašajo na tri osnovne vidike varovanja informacij, ki vplivajo na celotni sistem varovanja informacij v organizaciji vključno s tehnologijo, procesi in uporabniki:

- **zaupnost:** da informacije niso dostopne nepooblaščenim osebam,
- **integriteto ali celovitost/neokrnjenost:** da pooblaščene osebe, ki imajo dostop do informacij, te informacije prejmejo nepoškodovane in nespremenjene,
- **razpoložljivost:** da so informacije oziroma informacijski sistemi dostopni ter razpoložljivi, kadar pooblaščene osebe želijo do njih dostopati.

2 Trendi na področju varnostnih groženj

2.1 Naraščanje spletnega kriminala

Širše v globalnem in evropskem merilu je opazen izrazit trend naraščanja spletnega kriminala. K navedenemu največ prispevajo hitro naraščanje števila uporabnikov spleta in spletnih storitev, predvsem na bolj ogroženih mobilnih napravah, prenizka osveščenost uporabnikov ter povezovanje t.i. kibernetskega kriminala z ostalimi vrstami kriminala. Kot prikazano na sliki 1, se je po prepričanju in izkušnjah državljanov držav EU v letu 2014 v primerjavi z letom prej opazno povečala ogroženost na področju informacijske varnosti (European Commision, 2015, str. 54). Med prevladujočimi grožnjami so kraja identitete, okužbe z zlonamerno programsko opremo in bančne goljufije.



Slika 1: Prisotnost groženj informacijske varnosti – povprečje EU

V prvi polovici leta 2015 se je v Sloveniji, kot navaja polletno poročilo nacionalnega odzivnega centra za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij SI-CERT, močno povečalo število incidentov na področju informacijske varnosti, predvsem na področju zlonamerne programske opreme, socialnega inženiringa ter spletnih goljufij in prevar (SI-CERT, 2015). Že v začetku leta se je izrazito povečalo število t.i. phishing napadov v e-bančništvu, kjer gre za krajo identifikacijskih podatkov komitentov, in razširjenost izsiljevalskih virusov, ki uporabnikom zašifrirajo datoteke, da ne morejo dostopati do njihove vsebine, dokler izsiljevalcem ne plačajo odkupnine. Karakteristike varnostnih groženj predstavljamo v tabeli 1. Iz njih je razvidno, da je glede na najpogostejše vrste napadov tarča lahko katerikoli uporabnik spleta na katerikoli napravi, ki jo uporablja.

Tabela 1: Karakteristike varnostnih groženj v Sloveniji v prvi polovici leta 2015 po podatkih SI-CERT

Karakteristika	Numerično
Povečanje števila obravnavanih varnostnih incidentov	6 kratno v primerjavi z 2014
Povečanje števila prijavljenih varnostnih incidentov	več kot 2000 incidentov
Množični phishing napadi na e-bančništvo	na 6 slovenskih bank
Porast širjenja izsiljevalskih virusov	do 600 EUR škode na uporabnika
Porast socialnega inženiringa na družabnih omrežjih	do 5.000 ali več EUR na uporabnika
Porast spletnih goljufij in prevar (spletna trgovina)	do 24.000 EUR na uporabnika

2.2 Ključna varnostna tveganja v izobraževalnih inštitucijah

Izobraževalne inštitucije se širše gledano soočajo z nekaj ključnimi varnostnimi tveganji:

- z nizkimi proračuni za informatiko,
- z vse večjim poudarkom na uporabi lastnih mobilnih naprav zaposlenih in udeležencev izobraževanja,
- z njihovo dokaj nizko osveščenostjo v zvezi s potencialnimi varnostnimi grožnjami, in
- s pomanjkanjem strokovnjakov za informacijsko varnost.

Kot na podlagi analize še ugotavljajo v podjetju Dell (Dell Secure Works, 2015, str. 2), izobraževalnim organizacijam pogosto primanjkuje pregleda nad varnostnimi grožnjami na celotni infrastrukturi. Osredotočajo se predvsem na zagotavljanje osnovne varnosti v internem omrežju in manj na potencialne grožnje od zunaj iz spleta.

Učinkovitega zagotavljanja informacijske varnosti v katerikoli inštituciji ni mogoče zagotavljati brez predhodne analize informacijskih varnostnih tveganj, ki vključuje analizo informacijskih virov ter z njimi povezanih varnostnih ranljivosti in groženj, postavitve sistema varovanja informacij ter učinkovitega izvajanja ukrepov in nadzorstev za obvladovanje prepoznanih informacijskih varnostnih tveganj. Kljub dejstvu, da stoodstotne informacijske varnosti ni mogoče zagotoviti, s tovrstnim pristopom, ki ima podlago v mednarodnem standardu ISO/IEC 27001:2013, postanejo varnostna tveganja bistveno bolj obvladljiva.

3 Sistem varovanja informacij v izobraževalni inštituciji

3.1 Pristopi izobraževalnih inštitucij k varovanju informacij

Na področju informacijske varnosti so pristopi izobraževalnih inštitucij v Sloveniji dokaj različni:

- Sledijo le zahtevam zakonodaje, predvsem Zakona o varstvu osebnih podatkov.
- Bolj ozaveščena vodstva šol zagotovijo celovito politiko varovanja informacij za zaposlene in udeležence izobraževanja.

Na področju tehnologije in varovanja informacijskih sistemov imajo organizacije, katerih osnovna dejavnost je izobraževanje na različnih nivojih in sektorjih (od vrtca, osnovnih šol, srednjega šolstva, višjega in visokega šolstva, izobraževanja odraslih), različne pristope (Pučko, 2014, str. 204), kot npr.:

- Sledijo praksam drugih šol, uporabljajo javno dostopno programsko opremo, aplikacije in e-gradiva.
- Z lastnimi kadri in znanjem razvijajo svojim zahtevam in procesom prilagojene rešitve.
- Izobraževalni proces podprejo z digitalno tehnologijo in sistemi za e-učenje do te mere, da je mogoče izvajati izobraževanje/študij na daljavo, pri čemer je poskrbljeno tudi za varovanje informacij.

Različni pristopi so predvsem posledica dejstva, da v izobraževalnih organizacijah informatika in celovito varovanje informacij nista povsod prepoznana kot strateško pomembna, hkrati pa v okviru zakonodaje, z izjemo varstva osebnih podatkov, regulative in nacionalnih politik to področje ostaja dokaj odprto.

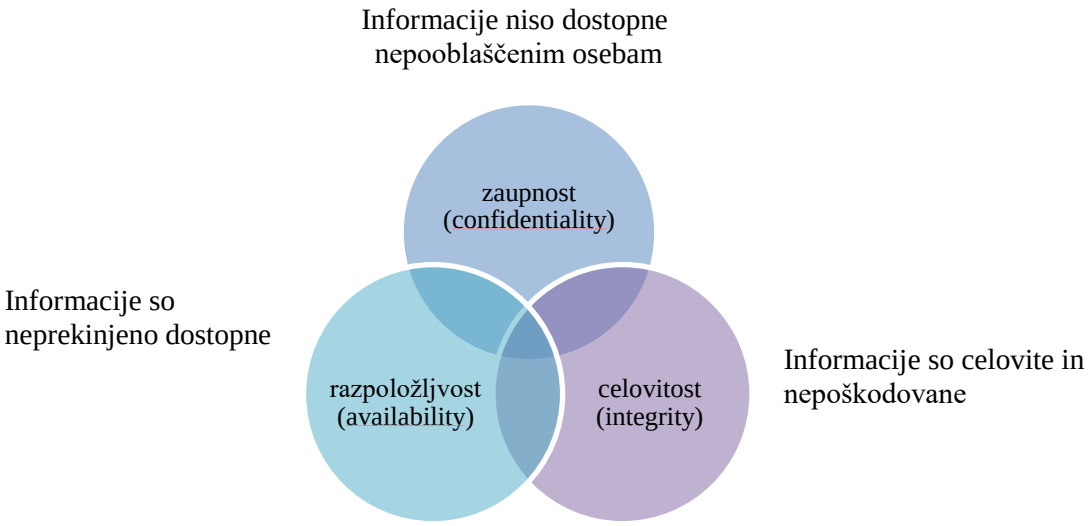
3.2 Zahteve za sistem varovanja informacij za izobraževalno inštitucijo in uporabljena metodologija

Kot je bilo že uvodoma predstavljeno, izhodišče za sistem varovanja informacij predstavlja t.i. trojček CIA (angleško »C - confidentiality, I – integrity, A – availability«), prikazan na sliki 2, ki vključuje tri glavne vidike informacijske varnosti. Navedeni vidiki so vpeti v vse elemente standarda ISO/IEC 27001:2013. Le-ta je v osnovi upravljavski standard. Vodstvo organizacije, v primeru tega prispevka vodstvo izobraževalne inštitucije, opredeli krovno politiko informacijske varnosti po področjih delovanja s poudarkom na tistih vidikih informacijske varnosti in tipih podatkov, ki so za neprekinjeno delovanje inštitucije, izpolnjevanje zahtev zakonodaje in pogodb z drugimi organizacijami bistvenega pomena.

Po smernicah krovne politike organizacija izdela podrobnejše varnostne politike za posamezna področja, ki že vključujejo tehnologijo, procese in uporabnike, opredeli odgovornosti ter vzpostavi sistem varovanja informacij po načelu kroga PDCA (angleško »P - Plan, D - Do, C - Check, A - Act«, oziroma v slovenskem prevodu »načrtuj, naredi, preveri, ukrepaj«).

V nadaljevanju vzpostavljanja sistema uporabimo dobre prakse, kako zagotavljati informacijsko varnost v okviru podrobnejše varnostne politike po posameznih področjih npr. pri uporabi elektronske pošte, nadzoru fizičnega dostopa do IKT infrastrukture, nadzoru

dostopa do informacijskih sistemov itd. Pri tem nam je v pomoč standard ISO/IEC 27002:2013 (SIST, ISO/IEC 27002, 2013). Izbira konkretnih dobrih praks in podpornih tehnoloških rešitev je seveda prepuščena posamezni organizaciji oziroma njenemu vodstvu po predhodni analizi informacijskih varnostnih tveganj. Vodilo pri odločanju je ponavadi razmerje med stopnjo tveganja in zahtevano investicijo.



Slika 2: Trojček CIA

Za obvladovanje varnostnih tveganj srednje ali velike izobraževalne inštitucije v nadaljevanju predstavljamo osnovni nabor varnostnih nadzorstev, za katera na osnovi uveljavljenih dobrih praks v svetu in poznavanja sistemov varovanja informacij ocenjujemo, da zagotavljajo priporočljiv nivo varovanja:

- Močan požarni zid in namestniški strežnik (imenovan tudi proxy strežnik) za nadzor dostopa od zunaj in od znotraj.
- Uporaba gesel za dostop do informacijskih sistemov z zamenjavo na vsaj tri mesece.
- Močan protivirusni programski paket in oprema za odkrivanje in odstranjevanje druge zlonamerne programske opreme ter odkrivanje in preprečevanje vdorov.
- Uporaba brezžičnega omrežja z geslom, brezžične povezave naj vodijo do požarnega zidu.
- Uporaba priporočil za zaščito (predvsem mladoletnih) udeležencev izobraževanja v zvezi z spletnimi vsebinami in potencialnimi poskusi socialnega inženiringa.
- Nadzor lokalnega omrežja s strani omrežnih administratorjev.
- Stalen nadzor s strani predavateljev, knjižničarjev in sistemskih administratorjev.
- Fizično varovanje prostorov in protipožarna zaščita.
- Ukrepi za zagotavljanje ustrezne stopnje razpoložljivosti informacijskih sistemov, vezani na razpoložljivost strojne opreme, varnostno kopiranje in licenciranje programske opreme.
- Osveščanje in usposabljanje zaposlenih in udeležencev izobraževalnega procesa v zvezi z varnostnimi grožnjami in njihovo vlogo pri zagotavljanju informacijske

varnosti. Priporočila za uporabo njihovih lastnih naprav v omrežju izobraževalne inštitucije.

3.3 Tehnologija in oprema

Pri tehnologiji sta pomembna predvsem dva nivoja, ki morata biti pri načrtovanju varnosti enakovredno obravnavana. Prvi nivo predstavlja varnost osnovne IKT infrastrukture vključno z njeno razpoložljivostjo kot celoto, drugi nivo pa varnost posameznih informacijskih sistemov in aplikacij.

Ponudba na tržišču varnostne opreme za preprečevanje škodljive programske opreme, vdorov in odtekanja podatkov je v zadnjih letih postala izredno široka. Na voljo je skoraj nepregledno mnogo različnih produktov strojne ali programske opreme, ki v različnih kombinacijah opreme enega ali več proizvajalcev omogočajo vzpostavitev celovite varnostne arhitekture za zaščito celotne organizacije. Za razliko v primerjavi s stanjem izpred petih let je postala tovrstna oprema tudi cenovno dostopnejša predvsem zaradi večje konkurence med proizvajalci ter novih inovativnih produktov, namenjenih malim in srednjim podjetjem, prav tako uporabnih tudi za izobraževalne inštitucije. Tovrstni produkti za enotno obvladovanje varnostnih groženj oz. obvladovanje na enem mestu (poimenovani angleško s kratico UTM - unified threat management) v eni napravi združujejo omrežne in varnostne funkcije, pokrivajo vseh sedem plasti omrežnega modela OSI in so sposobni prepoznati uporabnika z enotno identifikacijo ne glede na to, iz katere naprave dostopa v interno omrežje inštitucije.

Izobraževalne inštitucije si za razpoložljivost IKT infrastrukture in informacijskih sistemov večinoma ne postavljajo tako visokih zahtev kot npr. finančne organizacije ali vladne inštitucije. Razloga sta dva:

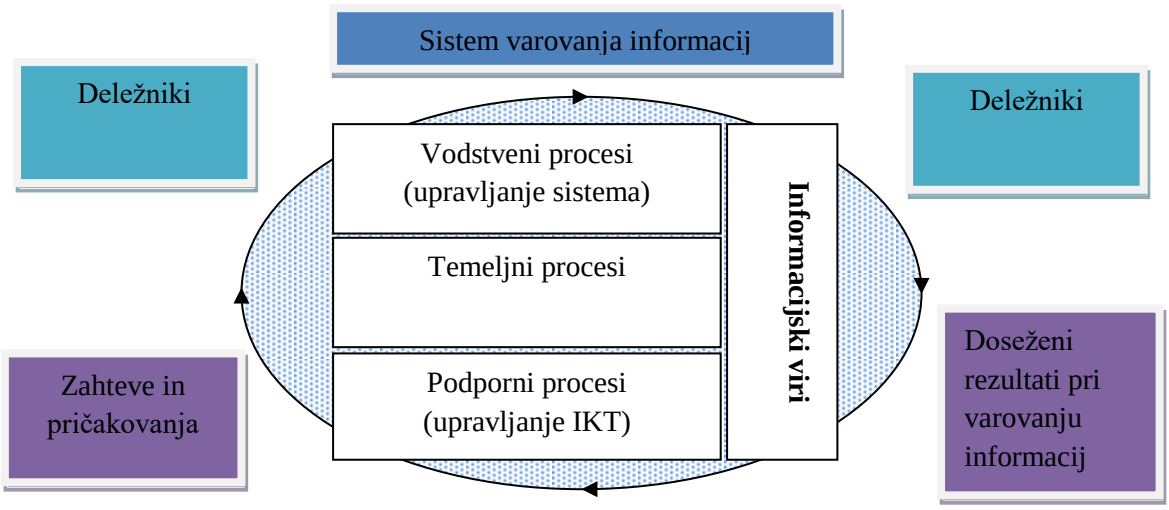
1. Izobraževalni proces se, vsaj v klasični obliki, ne izvaja 24 ur dnevno in 7 dni tedensko.
2. Izobraževalne inštitucije glede na razpoložljiva finančna sredstva tipično ne morejo investirati v IKT arhitekture z visoko stopnjo razpoložljivosti, v rezervne lokacije ipd.

Pri tekočem spremljanju stanja informacijske varnosti v organizaciji je potrebno vzpostaviti pregled nad varnostnimi dogodki in incidenti na osnovi podatkov o poskusih nepooblaščenega dostopa iz zunanjega in internega omrežja, okužbah z zlonamerno programsko opremo, izpadih delovanja ali nenačrtovani nedostopnosti posameznih informacijskih sistemov. Podatke pridobimo z rednim ali vsaj občasnim pregledovanjem dnevniških zapisov, analizo omrežnega prometa, poročili iz različnih informacijskih sistemov ipd. Analiza podatkov nam zagotovi pregled nad dejanskim stanjem informacijske varnosti in pomaga načrtovati potencialne ukrepe.

3.4 Procesi

Varovanje informacij zajema vse procese organizacije, ki za svoje izvajanje uporabljajo informacijske vire. Informacijski viri so vsi elektronski viri, klasični oz. papirni viri ter oprema, katero v organizaciji uporabljamo za procesiranje, hrambo in varovanje informacij. V vodstvene procese naj bo vsebinsko vključen tudi podproces upravljanja sistema varovanja informacij, v podporne procese pa proces ali podproces upravljanja IKT. Prvi obsega

postopke in aktivnosti v zvezi z definiranjem, izvajanjem, spremljanjem in izboljševanjem celotnega sistema varovanja informacij od krovnih varnostnih politik navzdol. Drugi vsebuje množico postopkov in aktivnosti za vzpostavljanje in vzdrževanje IKT do operativnega tehničnega nivoja. Vpetost procesov v sistem varovanja informacij prikazuje slika 3.



Slika 3: Vpetost procesov in informacijskih virov v sistem varovanja informacij

Kot za vse ostale postopke in aktivnosti, morajo imeti procesi opredeljene vhode in izhode, vire, odgovornosti, povezave z drugimi procesi im meritve, s katerimi spremljamo njihovo uspešnost in učinkovitost. Za podporo postopkom vodenja informacijskih virov in obvladovanja z njimi povezanih informacijskih varnostnih tveganj je na voljo tudi različna komercialna programska oprema ali njene prosto dostopne različice.

3.5 Vloga zaposlenih in udeležencev izobraževanja

Kot lahko zaključimo iz zahtev za sistem varovanja informacij, tehnologija in procesi sami po sebi ne morejo zagotoviti informacijske varnosti. Izjemno pomembna je ustrezna osveščenost in usposobljenost uporabnikov, v primeru izobraževalne inštitucije zaposlenih oziroma sodelavcev ter udeležencev izobraževalnega procesa. Za doseganje tega cilja so smiselne naslednje aktivnosti:

- Redno in sistematično seznanjanje uporabnikov s potencialnimi varnostnimi grožnjami in postopki varovanja informacij v izobraževalni organizaciji. Smiselno je, da izobraževalna inštitucija izvede izobraževanje o informacijski varnosti za vse zaposlene, ter za vsako generacijo udeležencev izobraževanja.
- Poleg zagotavljanja osnovne varnosti na uporabniških napravah za službeno opremo (delovne postaje, prenosniki, telefoni, tablice) s strani sistemskih administratorjev, je potrebno tudi seznanjanje uporabnikov s priporočili in varnostnimi nastavitvami za opremo v lasti uporabnikov, če z njo dostopajo v interno omrežje inštitucije.
- Posebna pozornost informacijski varnosti naj bo namenjena osveščanju mladoletnih oseb, s poudarkom na spletni varnosti in pazljivi uporabi družbenih omrežij.

- Vključevanje učiteljev in ostalih zaposlenih ter udeležencev izobraževanja v postopke preverjanja delovanja sistema varovanja informacij.
- Posredovanje povezav uporabnikom do koristnih napotkov na spletu in spletnih tečajev v zvezi z informacijsko varnostjo (primer spletnega tečaja ARNES »Varni na internetu«, dostopen na http://www.arnes.si/storitve/varnost/mooc-v.html).

4 Zaključek

Glede na povečevanje informacijskih varnostnih groženj v globalnem in slovenskem merilu je zagotavljanje informacijske varnosti področje, katerega tudi izobraževalne inštitucije ne smejo prepustiti naključju. V prispevku smo analizirali ključne zahteve in predlagali smernice za sistem varovanja informacij v izobraževalni inštituciji. Na področju tehnologije je potrebno zagotavljati vsaj osnovno zaščito s požarnim zidom, ustrezno politiko gesel, zaščito pred škodljivo programsko opremo in varnost v brezžičnem omrežju. Povečuje se cenovna dostopnost UTM opreme, ki združuje omrežne in varnostne funkcije in je primerna tudi za izobraževalne inštitucije. Varovanje informacij vključuje vse procese, ki uporabljajo informacijske vire, pri tem je priporočljiva standardizirana osnova kot je ISO/IEC 27001:2013. Prav tako je bistveno usposabljanje zaposlenih in udeležencev izobraževanja v smislu poznavanja, zavedanja in preprečevanja varnostnih ranljivosti in groženj.

Pri izjemno hitrem naraščanju uporabe lastnih mobilnih naprav uporabnikov se težišče pri varovanju informacij seli k usposabljanju in osveščanju uporabnikov ter vzdrževanju osnovne zaščite njihovih naprav. To je tudi eno od področij, ki predstavlja največji izziv inštitucijam, proizvajalcem opreme in uporabnikom v prihodnjih letih.

Viri

Dell Secure Works, *Top 2 Information Security Challenges for Higher Education,* 2015. (Citirano 16.11.2015) Dostopno na internetu na naslovu: http://www.secureworks.com/assets/pdf-store/white-papers/wp-top-2-info-security-challenges-for-higher-edu.pdf

European Commision, DGHA, Special Eurobarometer 423, *Cyber Security Report,* February 2015.

Pučko, M. (2014), Informacijski sistemi in informacijska varnost za podporo izobraževalnemu procesu, *Zbornik konference VIVID 2014*, Institut Jožef Stefan, Ljubljana, 2014, str. 202 - 208.

SI-CERT (2015), *Kako (ne)varen je bil splet v prvi polovici leta 2015?,* julij 2015. (Citirano 16.11.2015) Dostopno na internetu na naslovu: https://www.cert.si/kako-nevaren-je-bil-splet-v-prvi-polovici-leta-2015/

SIST ISO/IEC 27001:2013 (2013). *Informacijska tehnologija - Varnostne tehnike - Sistemi upravljanja informacijske varnosti – Zahteve.* Slovenski inštitut za standardizacijo, 2013.

SIST ISO/IEC 27002:2013 (2013). *Informacijska tehnologija - Varnostne tehnike - Pravila obnašanja pri upravljanju informacijske varnosti.* Slovenski inštitut za standardizacijo, 2013.