Prizadevanja Slovenije za obvladovanje groženj v kibernetskem prostoru

[1]Samo Maček, [2]Franci Mulec, [2]Franc Močilar
[1]Generalni sekretariat Vlade RS, Gregorčičeva ulica 20, 1000 Ljubljana
[2]Ministrstvo za zunanje zadeve, Prešernova ulica 25, 1000 Ljubljana
samo.macek@gov.si; franci.mulec@gov.si; franc.mocilar@gov.si

Izvleček

V prispevku so predstavljena prizadevanja Evropske unije in Republike Slovenije za obvladovanje izzivov na področju kibernetske varnosti. Terorizem ter organizirani in kibernetski kriminal čedalje bolj ogrožajo demokratično družbo in njene vrednote. EU je v zvezi s tem sprejela številne ukrepe. Z Evropsko agendo za varnost [3] je vzpostavila smernice za odzivanje EU na varnostne grožnje za obdobje 2015–2020. Kibernetska varnost je postala integralni del nacionalne varnosti držav in mednarodne skupnosti.

Ukrepom na ravni EU se prilagaja in jim sledi tudi Slovenija. V začetku leta 2016 je vlada sprejela strategijo kibernetske varnosti, aprila 2017 pa Uradu Vlade Republike Slovenije za varovanje tajnih podatkov razširila delovno področje in ga določila za nacionalni organ za kibernetsko varnost. S tem je bila določena podlaga za učinkovito in celovito zagotavljanje kibernetske varnosti v državi. S širšega vidika je pomembna krepitev zaupanja na državni ravni, strokovna usposobljenost zaposlenih in prenos znanja na področju kibernetske varnosti. Prav zadnje še posebej, saj se znova in znova izkazuje, da je najšibkejši člen še vedno človek. Tehnologija ne more zagotavljati varnosti, če uporabniki niso ustrezno usposobljeni, se ne zavedajo groženj ali ne upoštevajo ukrepov, s katerimi jih je mogoče obvladovati. V članku je opisano, kako se na spremenjeno strukturo groženj v kibernetskem prostoru odzivajo državni organi, ki zagotavljajo delovanje sistemov, ključnih za nemoteno izvajanje funkcij države. Dejavnosti na operativni ravni sledijo evropskim in nacionalnim usmeritvam. Predstavljeni so tudi operativni ukrepi, s katerimi obvladujemo naraščajoče grožnje in so vključeni v vladni informacijski sistem ter sisteme na področju zunanjih zadev.

Ključne besede: kibernetska varnost države, informacijski sistemi, grožnje, strategija, varnostni ukrepi.

Abstract

Efforts of the Republic of Slovenia in the management of cyberspace threats

The paper presents the current efforts of the EU and the Republic of Slovenia (RS) aimed at managing the challenges faced in the field of cyber security. Terrorism and organized cybercrime are becoming major threats to the democratic society and its values. The European Union (EU) has adopted a number of measures in this respect. The European Agenda on Security has established guidelines for the response of the EU to security threats for the period between 2015 and 2020. Cyber security has become an integral part of every country's national security as well as of the security of the international community.

Slovenia has been adapting to and following the measures undertaken at the EU level. At the beginning of 2016, the Government of the RS has adopted a strategy on cyber security and in April 2017 established a national body in charge of cyber security. From the broader perspective, it is important to boost confidence at the state level, professional competence of employees and knowledge transfer in the field of cyber security. These tasks and documents will set up the basis for the effective and comprehensive provisioning of cyber security in the country. This is particularly important since the human factor always turns out to be the weakest link. Technology cannot guarantee security if users are not properly trained, are not aware of the threats or do not apply the measures aimed at managing these threats.

We will demonstrate how government bodies respond to the modified structure of risks in cyberspace where the seamless implementation of the functions of the state is ensured through the functioning of systems that are vital for attaining this objective. Activities carried out at the operational level follow European and national policies and guidelines. In this context, we also provide examples of operational measures aimed at coping with the growing risks that are implemented in the government information system and the systems in the field of foreign affairs.

Keywords: cyber security, information systems, threats, strategy, precautions.

1 UVOD

Evropska unija (EU) in njene države članice se spoprijemajo z velikimi izzivi na področju varnosti. Terorizem ter organizirani kriminal in kibernetska kriminaliteta čedalje bolj ogrožajo družbo v vsej Evropi. K temu prispevajo tudi kriza, spori in politična nestabilnost v neposredni soseščini. V zadnjem času se je struktura groženj zelo spremenila. Poglavitni viri groženj so hacktivizem, interesi nacionalnih držav in organizirana kriminaliteta. [2, 4]

Sistemi, ki so ključni za varnost in delovanje države, so med možnimi tarčami organiziranega kriminala ali kibernetskega terorizma. Motivacija za napade se v primerjavi z običajnim spletnim kriminalom lahko izraža tudi v želji po doseganju družbenih ali političnih sprememb.

Da prihodnost bojevanja pripada kibernetskemu prostoru, je že leta 1984 v futurističnem romanu Nevromant predvidel pisatelj William Gibson. [6] Številni napadi na kritično infrastrukturo (npr. električna omrežja), državne in politične subjekte ter druge sisteme, pomembne za delovanje družbe, dokazujejo, da se je vizija romana že uresničila, napadi v kibernetskem prostoru pa imajo lahko uničujoče posledice v realnem svetu.

Kibernetska varnost pomeni sposobnost zaščititi, varovati ali braniti kibernetski prostor pred kibernetskimi napadi. Kibernetska grožnja pomeni možnost zlonamernega poskusa poškodovanja ali prekinitve računalniškega omrežja ali sistema. [9]

EU in Slovenija sta dejavno začeli krepiti kibernetsko varnost in zaščito ključnih informacijsko-komunikacijskih sistemov z obvladovanjem groženj v kibernetskem prostoru.

2 UREJANJE KIBERNETSKE VARNOSTI NA RAVNI EU – IZBRANI MEJNIKI

Pregled dejavnosti na področju urejanja kibernetske varnosti EU smo omejili zgolj na tiste z najpomembnejšim vplivom na zdajšnja prizadevanja v Sloveniji.

Podlaga za sodelovanje med državami in zasebnimi podjetji v boju proti kaznivim dejanjem v kibernetskem prostoru je Konvencija Sveta Evrope o kibernetski kriminaliteti, podpisana novembra 2001 v Budimpešti. Slovenija jo je ratificirala leta 2004. [14]

Evropska komisija je leta 2013 objavila strategijo kibernetske varnosti EU z naslovom Odprt, varen in zavarovan kibernetski prostor ter predlog direktive o varnosti omrežij in informacij. Strategija je celostna vizija EU, kako najučinkoviteje preprečiti kibernetske motnje in napade. Direktiva je ključni del splošne strategije za zagotovitev varnega in zaupanja vrednega digitalnega okolja v EU. [2, 5]

Aprila 2015 je Evropska komisija predstavila Evropsko agendo za varnost, s katero je vzpostavila smernice za odzivanje EU na varnostne grožnje v obdobju od leta 2015 do 2020. Z njo je nadomestila predhodno strategijo notranje varnosti za obdobje od leta 2010 do 2014. Glavno odgovornost za varnost imajo še vedno države članice. Pri spopadanju s čezmejnimi grožnjami (terorizem, organizirani kriminal in kibernetska kriminaliteta) pa morajo države sodelovati tako med seboj kot z ustanovami EU. Potreben je učinkovit in usklajen odziv na ravni celotne EU. Evropska agenda za varnost je torej skupna agenda Unije in držav članic ter zagotavlja podlago za sodelovanje in skupno ukrepanje Unije. [3, 4]

Julija 2016 je Evropski parlament sprejel tako imenovano Direktivo NIS (Network and Information Security) – uredbo o varnosti omrežij in informacij, ki bo poenotila nekatere ukrepe držav članic za zaščito informacijskega oziroma kibernetskega okolja. [13]

Namen direktive je zagotoviti:

- ustrezno pripravljenost držav članic na dejanske grožnje v kibernetskem prostoru z zagotavljanjem zadostnih odzivnih zmogljivosti,
- vzpostavljanje mreže sodelovanja med članicami na operativni in strateški ravni,
- dvig kulture informacijske varnosti v različnih sektorjih, ki so ključni za družbo in gospodarstvo ter čedalje bolj odvisni od informacijskih tehnologij. [11]

Na ravni EU imajo še posebno pomembno vlogo na področju boja proti kibernetski kriminaliteti Evropol (Evropski policijski urad) center za boj proti kibernetski kriminaliteti, Urad za evropsko pravosodno sodelovanje (Eurojust) ter Agencija EU za varnost omrežij in informacij (ENISA).

Najvišji predstavniki EU in zveze NATO so 9. julija 2016 v Varšavi podpisali skupno izjavo, v kateri so poudarili pomen nadaljnje krepitve medsebojnega sodelovanja. Izpostavljene so zlasti hibridne grožnje in kibernetska varnost, poudarek pa je tudi na izgradnji obrambnih sposobnosti tako v Evropi kot s partnerskimi državami. [17]

3 UREJANJE PODROČJA KIBERNETSKE VARNOSTI V SLOVENIJI

Usmeritvam EU na področju zagotavljanja kibernetske varnosti sledi tudi Slovenija. Februarja lani je

vlada sprejela nacionalno strategijo kibernetske varnosti, ki opredeljuje grožnje kibernetskega prostora, deležnike, področja udejanjanj, cilje in ukrepe za njihovo izvedbo. Cilj strategije je vzpostavitev celovitega sistema zagotavljanja kibernetske varnosti (do leta 2020), ki bo preprečeval varnostne incidente in tudi odpravljal njihove posledice. To bo podlaga za varnejše delovanje infrastrukture, pomembne za delovanje državnih organov in gospodarstva, pa tudi za življenje vsakega posameznika. [12]

Eden izmed temeljev zagotavljanja kibernetske varnosti je kriptografska zaščita. Jeseni 2016 je vlada sprejela Strategijo kriptografske zaščite podatkov v RS. V njej so opredeljeni cilji, za dosego katerih so oblikovani okvirni načrti in ukrepi za vrednotenje kriptografskih rešitev, spodbujanje razvoja in uporabe kriptografskih rešitev, zagotavljanje kriptografskih rešitev, raziskovanje na področju kriptologije, usposabljanje uporabnikov kriptografskih rešitev in zagotavljanje kadrovskih virov.

Obvladovanje kriptografske zaščite komunikacij je pomemben del vsake samostojne države. Še posebej je pomembno, da imamo usposobljene posameznike iz gospodarstva in državne uprave ter z akademskega področja, ki sodelujejo in so sposobni pripraviti ter izdelati strokovne in sodobne kriptografske rešitve. Veseli smo, da ima tudi Slovenija razvijalce kakovostnih kriptografskih rešitev tako za nižje kot tudi za višje stopnje zaupnosti. Javna razkritja o namernih zlorabah nekaterih tujih kriptografskih rešitev z dejavnim sodelovanjem proizvajalcev zaradi nacionalnih interesov so povečala zaupanje v rešitve, razvite v državah EU, posledično pa tudi rast njihovih cen. Tako je zavzemanje države za razvoj slovenskih kriptografskih rešitev še bolj utemeljeno.

Vlada je v začetku aprila 2017 določila, da Urad Vlade Republike Slovenije za varovanje tajnih podatkov (UVTP) prevzame naloge nacionalnega organa za kibernetsko varnost oz. osrednje koordinacije nacionalnega sistema kibernetske varnosti. [18]

Vzpostavitev navedenega organa ni zgolj zahteva strategije, ampak tudi Direktive NIS, pomeni pa tudi izpolnitev zaveze, dane zvezi NATO. Ne nazadnje pa to kot eno od prednostnih nalog predvideva tudi Resolucija o strategiji nacionalne varnosti RS in je prva v nizu nujnih nalog za učinkovito in celovito ureditev področja v Sloveniji. [1]

Urad za varovanje tajnih podatkov bo na strateški ravni koordiniral zmogljivosti za zagotavljanje varnosti omrežij in informacijskih sistemov ter obvladovanja incidentov na vseh ravneh v državi, predstavljal enotno kontaktno točko v okviru mednarodnega sodelovanja, zagotavljal usklajeno delovanje in partnerstvo vseh pristojnih deležnikov v javni upravi, spodbujal in podpiral sodelovanje z znanstvenoraziskovalnimi institucijami, spodbujal sodelovanje z gospodarskimi družbami in zagotavljal povezovanje in sodelovanje z ustreznimi partnerji na mednarodni ravni.

Urad za varovanje tajnih podatkov je ključni in povezovalni element državnih zmogljivosti na področju kibernetske varnosti in je odločilnega pomena za pripravljenost, ukrepanje, koordinacijo, izmenjavo informacij, usklajevanje ter odzivanje na kibernetske grožnje oziroma incidente. Pri spremljanju stanja na področju kibernetske varnosti bo sodeloval z drugimi državnimi organi in koordiniral njihovo delo na tem področju. Organom bo predlagal ukrepe za izboljšanje kibernetske varnosti, jim svetoval, organiziral usposabljanja, odgovarjal na strokovna vprašanja ipd.

Pri tem bodo imeli posebno vlogo Slovenski center za posredovanje pri omrežnih incidentih SI-CERT na ARNES-u, Agencija za komunikacijska omrežja in storitve RS (AKOS), Institut Jožef Stefan in druge znanstvenoraziskovalne ter izobraževalne institucije ter subjekti kritične infrastrukture, ki se po potrebi vključujejo v načrtovanje in izvajanje dejavnosti kibernetske varnosti.

Urad za varovanje tajnih podatkov bo na strateški ravni izvajal in koordiniral zmogljivosti za zagotavljanje kibernetske varnosti na nižjih ravneh v državi, obenem pa bo enotna kontaktna točka pri mednarodnem sodelovanju. Sodeloval bo z ustreznimi organi EU, zveze NATO in organi drugih mednarodnih organizacij in držav ter skrbel za izvrševanje sprejetih mednarodnih obveznosti in pogodb na področju kibernetske varnosti. [18]

Kibernetski napadi so pogosto usmerjeni na sisteme kritične infrastrukture, saj imajo težave v njihovem delovanju lahko uničujoče posledice za delovanje širše družbe. Pri opredeljevanju meril za določitev kritične infrastrukture zato izhajamo iz posledic, ki bi jih imelo nedelovanje za državo, gospodarstvo in nekatere druge dejavnosti. [10] Prav zdaj se ureja tudi to področje. Ministrstvo za obrambo je pripravilo predlog Zakona o kritični infrastrukturi in ga poslalo v medresorsko obravnavo. Temeljni namen

predloga je sistemska ureditev zagotavljanja neprekinjenega delovanja in celovitosti kritične infrastrukture.

Ministrstvo za javno upravo je dne 7. septembra 2017 v javno obravnavo poslalo osnutek Zakona o informacijski varnosti, ki bo na obravnavano področje predvidoma z letom 2019 prinesel večje spremembe. Med drugim predvideva ustanovitev novega nacionalnega organa za kibernetsko varnost, ki bo te naloge prevzel od UVTP, in ureditev pristojnosti, nalog, organizacije in delovanja enotne kontaktne točke ter posameznih skupin za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij (CSIRT) na področju zagotavljanja informacijske varnosti in kibernetske obrambe. [9]

Navedene aktivnosti pomenijo začetek obvladovanja izzivov na področju kibernetske varnosti in bodo zahtevale sodelovanje gospodarstva, akademske sfere ter pristojnih organov javne uprave.

4 UKREPI VAROVANJA

Aktivnosti in usmeritve EU in posameznih držav na področju kibernetske obrambe se preko akcijskih načrtov in različnih izvedbenih aktov odražajo tudi na operativni ravni. Informacijski sistemi, ki so ključni za varnost in delovanje države, so lahko tarča organiziranega kriminala, kibernetskega terorizma ipd. Zato pri njihovem upravljanju med drugim izvajamo tudi nekatere v nadaljevanju predstavljene varnostne ukrepe, ki jim pri običajni osebni in poslovni uporabi informacijske tehnologije (pogosto) ne namenjamo posebne pozornosti. Pri njihovi implementaciji sta zelo pomembna tudi sodelovanje z upravljavci podobnih sistemov ter medsebojna izmenjava izkušenj preko primerov dobrih praks.

Izbor in usposobljenost kadrov

Za obvladovanje groženj v kibernetskem prostoru sta najpomembnejša strokovna usposobljenost zaposlenih in prenos znanja. Vedno znova se izkaže, da je najšibkejši člen človek. Tehnologija ne more zagotavljati varnosti, če uporabniki niso ustrezno usposobljeni, se ne zavedajo tveganj ali ne upoštevajo ukrepov, s katerimi jih je mogoče obvladovati. Na Ministrstvu za zunanje zadeve izobražujemo vse zaposlene o grožnjah in ravnanjih v kibernetskem prostoru, tako diplomate, informatike, druge zaposlene kot študente na praksi. Pri tem uporabljamo tudi e-učilnico Ministrstva za obrambo. Seveda se zavedamo, da je nekajurno izobraževanje premalo (v naši nekdanji skupni državi so podobna izobraževanja potekala tudi po več tednov).

Za dejanji, ki so v nasprotju z interesi države ali delodajalca, pogosto stojijo nezadovoljni posamezniki, zamere iz preteklosti ali nasprotni politični interesi. S tajnimi vsebinami zato lahko delajo samo preverjene osebe, za katere lahko zagotovimo, da so vredne zaupanja. Zato pred izdajo dovoljenja za dostop izvedemo postopek varnostnega preverjanja – opravi ga pristojni državni organ (MNZ, MORS ali SOVA). V postopku zberejo podatke o morebitnih varnostnih zadržkih. Nekatera možna tveganja, ki jih preverjajo, so:

- zasvojenost z alkoholom, drogami ali druge oblike zasvojenosti,
- bolezen ali duševne motnje,
- stiki s tujimi varnostnimi in obveščevalnimi službami,
- članstvo ali sodelovanje v organizacijah ali skupinah, ki ogrožajo vitalne interese države ali političnih, obrambnih in varnostnih zvez, katerih del je Slovenija,
- neizbrisani disciplinski ukrepi,
- tekoči kazenski postopki,
- sodelovanje v tujih oboroženih silah ali drugih oboroženih formacijah,
- finančne obveznosti in prevzeta jamstva ter lastništvo nepremičnin,
- lastnosti in druge okoliščine, zaradi katerih bi bili lahko izpostavljeni izsiljevanju ali drugim oblikam pritiska (povzeto po Zakonu o tajnih podatkih).

Izolacija sistemov

Podatki, ki so zelo pomembni za varnost oziroma interese države, se obravnavajo samo v posebnih sistemih, ki so fizično popolnoma ločeni od druge informacijsko-komunikacijske infrastrukture in niso povezani z internetom.

Namenske šifrirne rešitve

Zaščita prenosa podatkov je med ključnimi vidiki kibernetske varnosti. To se je dodatno potrdilo z razkritjem zlorab nekaterih splošno uveljavljenih (priznanih) produktov. Uporabljajo se lahko samo rešitve, ki so ustrezno preverjene in imajo izdano potrdilo o varnostni ustreznosti.

Zaščita pred neželenimi elektromagnetnimi emisijami – TEMPEST

Gre za posebno namensko opremo, ki je zaščitena pred odtekanjem podatkov prek elektromagnetnega sevanja in prevodne (podatkovne, napajalne) infrastrukture. Obravnavane vsebine namreč tako lahko nenadzorovano odtekajo iz sistemov. Zahteve določa Natov standard SDIP-27, ki ima določeno stopnjo tajnosti in ni javno objavljen.

Fizični ukrepi varovanja

Ključne sestavine sistema se namestijo v varnostnih območjih. Gre za poseben stalno varovan prostor iz betona in jekla s protivlomno zaščito in tehničnimi ukrepi varovanja, v katerem je samo nujno pohištvo ter čim manj opreme in napeljav. Osnovni pogoji, ki jim mora ustrezati varnostnotehnična oprema, so določeni s sklepom vlade. [16]

Preprečevanje optičnih napadov

Oprema je postavljena tako, da je preprečeno prestrezanje zaslonske slike, neposredno ali prek odboja.

Preprečevanje akustičnih napadov

Redno izvajanje protiprisluškovalnih pregledov in preprečevanje napadov prek vibracij okenskih stekel (z laserskim mikrofonom) in predmetov v prostoru. Med te ukrepe je mogoče uvrstiti tudi prepoved vnosa naprav, ki omogočajo snemanje zvoka ali slike.

Uporaba neinformacijske opreme

V nekaterih posebnih primerih je tveganje uporabe informacijske tehnologije ne glede na posebne varnostne ukrepe še vedno lahko previsoko. Vsebine se obravnavajo v tako imenovanih gluhih sobah brez elektronske opreme. Morebitni dokumenti se izdelajo na papirju, med lokacijami pa jih prenašajo le pooblaščeni in posebej usposobljeni kurirji.

5 SKLEP

Kibernetska varnost je postala integralni del varnosti držav in mednarodne skupnosti. Grožnje presegajo meje virtualne sfere in lahko povzročijo uničujoče posledice v resničnem svetu. Obravnavati jih moramo na različnih ravneh, od kritične infrastrukture držav, sistemov, ki so pomembni za delovanje družbe, do posameznikov. Slovenija je dejavno pristopila k obvladovanju izzivov na tem področju. Z ustanovitvijo nacionalnega organa za kibernetsko varnost se postavljajo temelji za celovito obravnavo problematike in usklajevanje dejavnosti na strateški ravni. Motivi kibernetske kriminalitete se izražajo predvsem v želji po vplivu na družbene in politične spremembe. Tarča takih napadov so zato sistemi kritične infrastrukture oziroma informacijsko-komunikacijski sistemi, ki so ključni za delovanje države. Ker so teroristične in kriminalne združbe pri napadih tehnično usposobljene in inovativne, je treba temu prilagoditi tudi varovanje, ki se mora izvajati na različnih ravneh. Sem spadajo ukrepi, na katere pri običajni poslovni ali osebni uporabi računalniške opreme niti ne pomislimo. Predvsem pa so pomembni krepitev zaupanja na državni ravni, strokovna usposobljenost kadra in prenos znanja na področju kibernetske varnosti. Kljub tehniki se namreč pogosto izkaže, da je najšibkejši člen še vedno človek.

6 LITERATURA IN VIRI

[1] Državni zbor RS, Resolucija o strategiji nacionalne varnosti RS. (2010). Uradni list RS, št. 27/2010.

[2] Evropska komisija, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. (2013). http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf (obiskano 10. 9. 2017).

[3] Evropska komisija, Evropska agenda za varnost. (2015). europa.eu/rapid/press-release_IP-16-1445_sl.pdf (obiskano 16. 9. 2017).

[4] Evropska komisija, Evropska agenda za varnost: Vprašanja in odgovori. (2015). europa.eu/rapid/press-release_MEMO-15-4867_sl.pdf (obiskano 16. 9. 2017).

[5] Evropska komisija, Načrt kibernetske varnosti EU za zaščito odprtega interneta ter svobode in priložnosti na spletu – sporočilo za medije. (2013). http://europa.eu/rapid/press-release_IP-13-94_sl.htm (obiskano 16. 9. 2017).

[6] Gibson, W. (1984). *Neuromancer*. New York: Ace Science Fiction Books.

[7] Government Business Council, Achieving Holistic Cybersecurity: 2016 Progress Report. (2016). http://www.govexec.com/insights/reports/achieving-holistic-cybersecurity-2016-progress-report/127435/ (obiskano 16. 9. 2017).

[8] Maček, S., Močilar, F., Mulec, F. (2016). Osnovni koncepti zagotavljanja kibernetske varnosti. *Sodobne tehnologije in storitve OTS 2016: zbornik enaindvajsete konference, Maribor, 14. in 15. junij 2016*.

[9] Ministrstvo za javno upravo, Javna obravnava osnutka predloga Zakona o informacijski varnosti – redni postopek, številka: 007-644/2017-1. (2017).

[10] Ministrstvo za obrambo, Veljavni kriteriji kritičnosti za določanje kritične infrastrukture državnega pomena v RS. (2014). http://www.mo.gov.si/si/delovna_podrocja/zascita_kriticne_infrastrukture (obiskano 16. 9. 2017).

[11] SI-CERT, EU enotno k zaščiti interneta, https://www.cert.si/eu-enotno-k-zasciti-interneta/ (obiskano 16. 9. 2017).

[12] Strategija kibernetske varnosti. (2016). http://www.uvtp.gov.si/fileadmin/uvtp.gov.si/pageuploads/Startegija_KV.pdf (obiskano 16. 9. 2017).

[13] Svet EU, Direktiva 2016/1148/ES Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji – Direktiva NIS. (2016). *Uradni list EU, 194*, 1–30.
[14] Svet Evrope, Konvencija Sveta Evrope o kibernetski kriminaliteti. (2001). http://www.svetevrope.si/sl/dokumenti_in_publikacije/konvencije/185/ (obiskano 16. 9. 2017).
[15] Urad za varovanje tajnih podatkov, Nacionalni organ za kibernetsko varnost. (2017). http://www.uvtp.gov.si/si/medijsko_sredisce/novica/article/335/1360 (obiskano 16. 9. 2017).
[16] Vlada RS, Sklep o določitvi pogojev za varnostnotehnično opremo, ki se sme vgrajevati v varnostna območja. (1994). *Uradni list RS,* št. *94/06.*
[17] Vlada RS, Sporočila za javnost. (2016). http://www.vlada.si/predsednik_vlade/ sporocila_za_javnost/a/premier_dr_cerar_varsavski_vrh_prelomen_za_ustreznejse_odzive_zaveznistva_na_sodobno_varnostno_okolje_63 (obiskano 16. 9. 2017).
[18] Vlada RS, Vladno gradivo, številka 007-8/2017/11. (2017). http://vrs-3.vlada.si/MANDAT14/VLADNAGRADIVA.NSF/ 18a6b9887c33a0bdc12570e50034eb54%2F3c2877f0c0cfeb87c12580f3002993fa%2F%24FILE%2FVG_sklep.doc (obiskano 16. 9. 2017).

▪

Samo Maček je po izobrazbi magister znanosti s področja računalništva in informatike. Zaposlen je kot vodja Sektorja za informatiko v Generalnem sekretariatu Vlade RS, kjer med drugim opravlja naloge na področju informacijske varnosti, informacijskih sistemov za obravnavanje tajnih podatkov, razvoja spletnih aplikativnih rešitev ter upravljanja dokumentnih in relacijskih baz podatkov. Pred tem je vodil Oddelek za organizacijo in kadrovsko informatiko na Ministrstvu za notranje zadeve. Razvil je številne informacijske rešitve, ki so v uporabi v vladnem informacijskem sistemu, organih državne uprave in gospodarskih družbah.

▪

Franci Mulec je magistriral na Fakulteti za organizacijske vede Univerze v Mariboru. Zadnjih 15 let se ukvarja z razvojem in zagotavljanjem informacijske varnosti visoko varnih sistemov. Je arhitekt več sistemov Republike Slovenije, član ISACA (Information Systems Audit and Control Association) in nosilec CISA (Certified Information Systems Auditor).

▪

Franc Močilar je diplomiral in magistriral na Fakulteti za računalništvo in informatiko Univerze v Ljubljani. Zadnjih 15 let se ukvarja z zagotavljanjem informacijske varnosti. Leta 2005 je opravil izpit in pridobil potrdilo CISSP (Certified Information Systems Security Professional) mednarodne neprofitne organizacije ISC2 (http://www.isc2.org) za preverjanje znanj in podeljevanje ter vzdrževanje potrdil s področja varovanja informacij. Zaposlen je na Ministrstvu za zunanje zadeve RS.