1.08 Objavljen znanstveni prispevek na konferenci
1.08 Published Scientific Conference Contribution

Marko POTOKAR[*], Igor BERNIK[**]

VZPOSTAVITEV SISTEMA UPRAVLJANJA VAROVANJA INFORMACIJ ZA PROJEKT E-ARHIVIRANJA V SKLADU Z ZVDAGA IN ZVOP-1

Izvleček:

Ključni elementi pri zajemu ali hrambi gradiv v elektronski obliki so uporaba ustrezne informacijske infrastrukture, njeno strokovno upravljanje in dosledno upoštevanje uveljavljenih pravil s področja varovanja informacij (zagotavljanje zaupnosti, celovitosti in razpoložljivosti). Za zagotovitev ustrezne stopnje informacijske varnosti in tudi upravljanja z informacijsko tehnologijo se je priporočljivo nasloniti na mednarodni standard ISO/IEC 27001 (Informacijska tehnologija - Varnostne tehnike - Sistemi za upravljanje varovanja informacij - Zahteve) in ISO/IEC 27002 (Informacijska tehnologija - Varnostne tehnike - Kodeks za upravljanje varovanja informacij). Ta par standardov z ustrezno implementacijo celovito pokriva zahteve Zakona o varstvu dokumentarnega in arhivskega gradiva ter arhivih in Zakona o varstvu osebnih podatkov. Za dosego ustrezne informacijske varnosti in upravljanja informacijske tehnologije se lahko organizacija drži tudi drugih standardov ali priporočil (npr.: ITIL, COBIT), ki pokrivajo postavljene zahteve. V prispevku bo predstavljena vpeljava sistema vodenja varovanja informacij na podlagi varnostnih standardov ISO/IEC 27001 in ISO/IEC 27002, le-ta izpolnjuje enotne tehnološke zahteve iz poglavja 2.2 Informacijska infrastruktura in poglavja 3.2 Nadzor in varnost ter določila Zakona o varstvu osebnih podatkov.

Ključne besede:

varovanje informacij, SUVI, enotne tehnološke zahteve, ETZ, osebni podatki, ZVOP-1

Abstract:

Implementation of an Information Security Management System for the E-archives Project in Compliance with PDAAIA and PDPA

Key elements in gathering and keeping/storing materials in electronic form are the use of suitable information infrastructure, its professional management and consistent following of established rules from the field of information security (ensuring confidentiality, integrity and availability). To ensure an adequate degree of information security as well as information technology management, it is recommendable to apply the international standards ISO/IEC 27001 and ISO/IEC 27002. With adequate implementation, the two standards entirely cover the requirements of Protection of Documents and Archives and Archival Institutions Act (PDAAIA). In order to reach adequate information security and information technology management, an organization can also follow other standards or recommendations (for example: ITIL, COBIT) that cover the requirements set. This article deals with the introduction of information security management system based on security standards ISO/IEC 27001 and ISO/IEC 27002, which meets uniform technological requirements from chapters 2.2 Information Infrastructure and 3.2 Surveilance and Security, as well as provisions of Personal Data Protection Act.

Key words:

Information security, Information Security Management system, Uniform Technological requirements, UTZ, personal data, PDPA

[*] *Mag. Marko Potokar, predsednik sveta Inštituta za varnostno kulturo; član Inštituta za korporativne varnostne študije; član strokovnega sveta Inštituta za forenziko informacijskih tehnologij; državni nadzornik za varstvo osebnih podatkov, Informacijskih pooblaščenec Republike Slovenije, Založka 59, 1000 Ljubljana, Slovenija, kontakt: marko.potokar@ifit.si.*

[**] *Dr. Igor Bernik, predstojnik Katedre za informacijsko varnost in prodekan za izobraževalno dejavnost na Fakulteti za varnostne vede Univerze v Mariboru, Kotnikova ulica 8, 1000 Ljubljana, Slovenija, kontakt: igor.bernik@fvv.uni-mb.si.*

1 UVOD

Informacije in informacijski sistemi, ki jih podpirajo, so pomembna podpora poslovanju organizacij. Razpoložljivost, neoporečnost in zaupnost informacijskih sistemov so pomembne za vzdrževanje konkurenčnosti, finančnih tokov, donosnosti, zakonitosti in ugleda podjetja. Informacijski sistemi in informacijska tehnologija pa so neprestano tarča resnih groženj, kot so kibernetska kriminaliteta, sabotaže, odpovedi, škodljiva programska oprema in druge akcije napadalcev. Z razvojem informacijske tehnologije in njeno kompleksnostjo se pričakuje, da bodo preteče nevarnosti vedno večje.

Za učinkovito varovanje informacijskih virov ni potrebno le razumevanje tehničnih karakteristik, operacijskih sistemov in programske opreme, temveč moramo predvsem vedeti, kaj ščitimo in katere kontrole moramo vpeljati. Glede na to, da je večina vidikov današnjega življenja odvisna od informacijske tehnologije, obstaja veliko različnih razlogov, zakaj si posamezniki in podjetja prizadevajo ohraniti varen dostop do informacij in virov organizacije. V primeru zagotavljanja varnosti je potrebno čimprejšnje varnostno ukrepanje in predhodno načrtovanje varovanja, ki dolgoročno pripomore k cenejšim in uspešnejšim rešitvam. Pri načrtovanju varnosti moramo upoštevati temeljne varnostne zahteve, ki so za vse organizacije enake. Začetne varnostne zahteve predstavljajo varnostna tveganja, kot so ogrožanje virov organizacije in njihova obstoječa ranljivost. Druge zahteve se nanašajo na upoštevanje potencialnih posledic, ki jih nevarnosti lahko povzročijo v procesih organizacije. Specifična tveganja, ki lahko ogrožajo potek procesov organizacije, lahko odpravimo šele, ko ugotovimo, kakšne nevarnosti nam pretijo. Zavest o zaščiti informacijskih virov zahteva vključevanje procesa upravljanja tveganj, načrtovanje in razvijanje politike varovanja, pravil ter postopkov obnašanja in delovanja v organizaciji. Postopek upravljanja tveganja je stalen proces ocenjevanja tveganj, poteka pa po korakih, katerih cilj je zmanjševanje tveganja na sprejemljivo stopnjo, sprejemanje dovoljenih tveganj in ohranjanja še sprejemljive stopnje tveganj. Del tega procesa predstavlja analizo tveganj, le-ta vključuje ugotavljanje dejanske vrednosti virov organizacije, opredelitev njihovih soodvisnosti, ocenjevanje groženj in prepoznavanje obstoječih varnostnih kontrol. Pri tem gre za ugotavljanje verjetnosti dogodka grožnje ter predvidevanja morebitne škode. Rezultati analize ponudijo jasne odgovore za sprejem in vpeljavo ustreznih varnostnih zaščit, ki učinkovito in ekonomsko zmanjšujejo tveganja ter zagotavljajo razpoložljivost, zaupnost in neoporečnost informacijskega sistema ter informacijske tehnologije.

Ko govorimo o varovanju informacij, se moramo zavedati, da se le-ta nanaša na zagotavljanje varnosti v izredno spreminjajočem se okolju. Ranljivosti informacijskih sistemov in informacijske tehnologije se neprestano spreminjajo in verjetnost varnostnih groženj venomer narašča. Spremembe se odražajo tudi v sami organizaciji: spremembe procesov organizacije, uvajanje novih operativnih postopkov, nakup in vpeljava nove strojne in programske opreme, njihovo posodabljanje, spremembe delovnih postopkov, fluktuacija zaposlenih in podobno. S spremembo delovnih zadolžitev se spreminjajo tudi pravice dostopanja do podatkov, informacij ali drugih informacijskih virov s strani zaposlenih. Zaradi tega je v okoljih, kjer se varnostne zahteve neprestano spreminjajo, nujna zahteva po varnostnih pregledih, sprotnem nadziranju delovanja informacijskega sistema, njegovem vrednotenju ter pridobivanju povratnih informacij o varnosti in njeni potencialni ogroženosti. Končne akcije varovanja informacijskih sistemov in informacijske tehnologije morajo biti usmerjene v zaznavanje varnostnih lukenj z vzpostavitvijo

ustreznega sistema sprotnega nadzora. Ne glede na vrsto dobrin, ki jih varujemo, velja, da bolj kot se okolje spreminja, težje je načrtovati, uvajati, nadzorovati in upravljati varnost.

Pri opredeljevanju varnostnih zahtev je potrebno upoštevati tudi zakonske in pogodbene zahteve ter vse večje potrebe po standardizaciji, ki jih morajo organizacije, njihovi poslovni partnerji in izvajalci storitev upoštevati. Vse bolj stopa v veljavo standardiziranje po standardih družine ISO/IEC 27000 (predvsem ISO/IEC 27001 in ISO/IEC 27002; v nadaljevanju ISO/IEC 27001/2), sprejeli smo ga tudi v Sloveniji. Standard se je od nastanka sredi devetdesetih let do danes izpopolnil skozi izdane različice. Vse več organizacij se je začelo pri snovanju in obnovi postopkov za zagotavljanje varnosti zavedati pomena upoštevanja priporočljivih standardov.

2 SISTEM UPRAVLJANJA VAROVANJA INFORMACIJ (SUVI)

Jasno je, da je ustrezna informacijska infrastruktura postala odločilen dejavnik, ki pripomore k uspehu organizacije. Hkrati se vse bolj zavedamo pomembnosti varovanja informacij, ki mora postati del življenskega cikla v razvoju in vzdrževanju informacijskih sistemov. Varovanje informacij pojmujemo kot zaščito le-teh pred raznovrstnimi grožnjami. S tem se zagotovi neprekinjeno poslovanje, zmanjša poslovno tveganje ter doseže največji dohodek iz naložb in poslovnih možnosti. Če preletimo zahteve, ki jih določajo zakoni, predpisi in standardi, bi lahko celo rekli, da je v nekaterih okoliščinah varnost podatkov pomembnejša od podatkov samih. Pri elektronskem poslovanju lahko kot bistvene zahteve za zagotavljanje konkurenčne prednosti navedemo pravočasen in natančen dostop do podatkov, neprekinjeno razpoložljivost sistemov, varno hranjenje poslovnih in zaupnih podatkov (osebni podatki strank, podatki o transakcijah, plačilnih in kreditnih karticah ipd.), potrebo po hitrem razvoju novih sistemov in kot pomembno prodajno pot tudi ponujanje izdelkov in storitev preko interneta. Elektronsko poslovanje je omogočilo nove poslovne poti, ki se zanašajo na učinkovit program za varovanje informacij, s katerim si lahko podjetje pridobi zaupanje strank. Zakonodaja in regulativa, tako vladna kot industrijska, se še naprej razvijata in skušata zaščititi potrošnike in podjetja, ki poslujejo elektronsko. Pri nas sta poleg ostalih (Zakon o elektronskem poslovanju in elektronskem podpisu, Zakon o avtorskih in sorodnih pravicah, Kazenski zakonik, Zakon o tajnih podatkih idr.) najbolj odmevna Zakon o varstvu osebnih podatkov (v nadaljevanju ZVOP-1), ki predpisuje organizacijske, tehnične in pravne postopke ter ukrepe, s katerimi se preprečujejo neustavni, nezakoniti in neupravičeni posegi v zasebnost in dostojanstvo posameznika pri obdelavi osebnih podatkov, ter varnostni standard ISO/IEC 27001/2, ki med drugim podaja zahteve po preverjanju istovetnosti uporabnika, kontroli dostopa ter zagotavljanju razpoložljivosti in celovitosti podatkov.

2.1 Procesni pristop SUVI

Pri uveljavljanju varnostnih zahtev oziroma vpeljavi sistema upravljanja varovanja informacij (SUVI) mora organizacija prepoznati svoje varnostne potrebe. Kodeks dobre prakse ISO/IEC 27002 navaja tri glavne vire varnostnih zahtev:

- ocena tveganja, s katero prepoznamo grožnje, ki ogrožajo sredstva organizacije, ovrednotimo ranljivost in verjetnost pojava ter predvidimo možne posledice,

- niz načel, ciljev in poslovnih zahtev za obdelavo informacij, ki jih razvije organizacija v podporo svojim poslovnim procesom,
- zahteve, ki jih določajo zakoni, statuti, predpisi in pogodbe ter jih morajo izpolnjevati organizacija, njeni poslovni partnerji in okolje, v katerega je umeščeno poslovanje organizacije.

Pri upravljanju varovanja informacij se srečamo s procesnim pristopom. Upravljanje je proces, ki ima vhode in ima 'procesni del', ki le-te pretvarja v izhode. Proces varovanja informacij popišemo z znanim krogom PDCA (*P*lan, *D*o, *C*heck, *A*ct), ki zagotavlja nenehno nadzorovanje in izboljševanje procesa varovanja informacij. S procesnim pristopom se srečamo že pri vzpostavitvi sistema upravljanja varovanja informacij in analizi tveganj. Začnemo s popisom informacijskih virov, ki jih nato umeščamo znotraj procesov. Pri tem moramo popisati in določiti ustrezne procese, v katerih sodelujejo opredeljeni informacijski viri. Pri tem ni vedno najboljši način, da izhajamo iz organizacijske sheme organizacije, saj je v določenih primerih bolj smotrno oblikovati procese glede na vsebino in glede na izvajanje posameznih funkcij znotraj organizacije. Pri tem ne smemo pozabiti na določitev lastnikov posameznih procesov. Šele ko opredelimo procese, sledi popis informacijskih virov, njihovo razvrščanje in umeščanje v procese. Nadaljujemo z ocenjevanjem tveganj: vrednotenje virov, določitev ranljivosti in groženj ter opredelitev velikosti posameznih tveganj. Sledi obravnava tveganj. Cilj je zmanjšanje nesprejemljivih tveganj na raven, določeno s kriterijem sprejemljivosti. Zmanjševanje dosežemo z izbiro ustreznih nadzorstev, lahko pa tudi z zavarovanjem tveganj pri zavarovalnici ali s prenosom tveganj na drugo osebo. Sledi izjava o primernosti, v kateri navedemo, katera nadzorstva (kontrole) varnostnega standarda ISO/IEC 27001 smo pokrili in katere ne ter zakaj. Sledi izdelava načrta obravnave tveganj, ta predstavlja formalni načrt za uvajanje ukrepov za zmanjševanje tveganj. V njem med drugim opredelimo odgovornosti za obravnavo tveganj, prioritete, cene ukrepov, potrebne (tudi nove) tehnologije, potrebno delo za vpeljavo in izobraževanje ter terminski rok izvedbe. Rezultati obravnave tveganj zgolj opredeljujejo, katera nadzorstva potrebujemo, v načrtu obravnave pa podrobneje opredelimo in ovrednotimo izbrano možnost obravnave tveganja. Natančno ugotavljamo, kako bomo zmanjšali tveganje in koliko nas bo to stalo. Eventuelna (pre)visoka cena zahteva ponovno potrjevanje upravljanja. Obravnava tveganj, ki je bila na prvi pogled najprimernejša, tako ni najustreznejša, moramo jo izboljšati ali spremeniti, zato se vrnemo na točko tovrstne obravnave. V tem primeru uporabimo krog izboljševanja (PDCA) za doseganje pričakovanih ciljev upravljanja. In vse skupaj se zavrti v nov krog.

2.2 Vloge in razmerja v procesu SUVI

Na upravljanje varovanja informacij torej gledamo kot na vzpostavitev in vzdrževanje sistema za zagotavljanje usklajenosti strategije varovanja informacij s poslovnimi cilji organizacije in skladnosti z veljavnimi zakoni ter predpisi. Tako je pri vzpostavitvi SUVI potrebno identificirati obstoječe in možne pravne ter druge regulatorne zadeve, ki vplivajo na varovanje informacij, s tem pa ocenimo njihov vpliv na poslovanje organizacije. Varnost oziroma zaščito informacij pred raznimi grožnjami dosežemo z vpeljavo ustreznih kontrol oziroma nadzorstev, ki obstoječa tveganja zmanjšajo na sprejemljivo raven. Seveda morajo biti izbrana taka nadzorstva, ki so v skladu z državnimi in mednarodnimi zakoni ter predpisi. ISO/IEC 27002 kot ključna nadzorstva (z zakonskega vidika), pomembna za organizacijo,

navaja zaščito podatkov in varstvo osebnih podatkov, zaščito organizacijskih zapisov in pravico do zaščite intelektualne lastnine.

Kot glavni in odgovorni za uspešno in učinkovito upravljanje SUVI mora imeti upravljavec varovanja informacij (angl.: Chief Security Officer; CSO) poleg specifičnih znanj (kot so znanja s področja standardov za upravljanje varovanja informacij, poznavanje metodologije oblikovanja in izvajanja standardov, poznavanje metodologije izvajanja varovanja in nadzorov, poznavanje strategije poslovanja in poslovne politike podjetja, poznavanje IT-področja ipd.) tudi znanja s pravnega področja. Ker upravlja tudi z zagotavljanjem skladnosti z zakonodajo in ostalimi pravnimi zahtevami v zvezi z varovanjem informacij, mora poznati pravne in regulatorne zadeve, povezane s prenosom podatkov, šifriranjem, varovanjem osebnih podatkov, upoštevanjem avtorskih pravic, varovanjem poslovnih skrivnosti itd.

Seveda upravljavec informacijske varnosti praviloma nima formalne izobrazbe pravne smeri, ampak je veliko pogosteje izobražen s področja t. i. tehničnih ved (računalništvo, informatika ipd.). Tudi njegova predhodna profesionalna kariera je pogosto vijugala po virtualnih poteh računalniških in informacijskih svetov, ne pa v gozdovih zakonov in pravil ter njihovih interpretacij. Ker je iluzorno pričakovati, da bo upravljavec varovanja informacij popoln strokovnjak na vseh področjih (in s tem tudi na pravnem), si lahko zamislimo, da si pri svojem delu, ki zadeva pravno področje, pomaga z nasveti in komentarji, pridobljenimi s strani ustreznih strokovnih oseb oziroma služb. Tako se v trikotniku CEO/CIO/CSO pojavi še ogljišče LO (angl.: Law-Office; slov.: pravniška pisarna), slednja v obstoječe odnose (ki so po definiciji konfliktni) pristavi še del svojih interesov. Tako vloga upravljavca varovanja informacij postane še težja, saj je ponavadi on tisti, ki pred vodstvom (CEO, CIO) zastopa tudi interese pravne službe. Tako postane upravljavec informacijske varnosti v očeh CEO in CIO še bolj moteč element v procesu doseganja ciljev organizacije: v informacijski sistem organizacije je ponavadi potrebno vgraditi še kakšno 'nepotrebno' varnostno funkcionalnost, kar seveda za seboj potegne dodatne stroške; hkrati je potrebno sprejeti še kakšno popravljeno varnostno politiko (če že ne napisati nove), s tem pa ponavadi posežemo v obstoječe organizacijske odnose in pravila ter tako povzročimo še nezadovoljstvo zaposlenih.

V takem okolju je pomembno zavedanje, da je za organiziranost, nadzor delovanja, zagotavljanja virov in razvoj celovitega upravljanja z informacijskimi tveganji odgovorno najvišje vodstvo organizacije, saj določa politiko ter cilje in je odgovorno za nadzor nad delovanjem sistema in koordinacijo vseh področij. Vodstvo organizacije tudi načrtuje in zagotavlja vse potrebne vire (človeške, finančne, materialne, informacijske) za učinkovito delovanje sistema, vključno s primerno infrastrukturo in delovnim okoljem. Za samo izvedbo politike in načrtov je operativno odgovoren upravljavec varovanja informacij, ki svoje delo opravlja v okviru danih možnosti in virov. Tako je še toliko bolj pomembno, da se s strani vodstva izražena zavezanost in podpora varovanju informacij, kot pomembni poslovni aktivnosti organizacije, zapiše tudi v krovni varnostni politiki organizacije.

2.3 Spremljanje delovanja SUVI

Spremljanje vpeljanega SUVI je pomemben vidik zagotavljanja varnosti informacijskih virov, čeprav mu navadno v zaključevanju procesa varovanja posvečamo premalo pozornosti. Običajno se po vpeljavi varnostnih nadzorstev, ki izhajajo iz analize informacijskih tveganj, domneva, da je proces varovanja

zaključen. Pri tem pa organizacije pozabljajo, da vpeljana nadzorstva zahtevajo neprestano spremljanje, ki zagotavlja, da le-ta delujejo in bodo še naprej delovala na zahtevan in pravilen način, kljub vsem spremembam okolja. Usmerjenost v nadzor nad učinkovitostjo izvajanja sistema vodenja varovanja informacij se kaže v zahtevi standarda ISO/IEC 27001 – potrebno je vzpostaviti in vzdrževati dokumentirane postopke za načrtovanje in izvajanje notranjih presoj, postati morajo sestavni del vsakega programa vzpostavitve, vzdrževanja in razvoja sistema vodenja varovanja informacij. Vpeljana varnostna nadzorstva delujejo učinkovito le pod pogojem njihovega preverjanja v realnem poslovnem življenju. Pri spremljanju varnostnega sistema je potrebno aktivnosti preverjanja sistematično načrtovati, odkrivanje zastarelih varnostnih nadzorstev oziroma tistih, ki delujejo v neskladju s predvidenimi zahtevami, pa ne prepuščati naključju.

V prvi fazi spremljanja SUVI gre za zagotavljanje ustrezne funkcionalnosti varnostnih nadzorstev, kasneje pa tudi za spremljanje učinkovitosti ali šibkosti storitev in vpeljanih zaščit. Spremljanje vpeljanega varnostnega sistema mora tovrstne šibkosti odkriti in omogočiti ustrezne akcije za odpravo oziroma izboljšanje le-teh. Standard ISO/IEC 27001 zajema spremljanje vpeljanega SUVI v tako imenovani fazi »preveri« (Check), kjer določa načine njegovega spremljanja. Ta faza zagotavlja akcije za uspešno delovanje varnostnih nadzorstev, opis postopkov za upravljanje in delovanje teh nadzorstev in opis procesov za sprotno pregledovanje tveganj glede na spremembe tehnologije ali pojavitev novih groženj. Prihodnje spremembe je možno predvidevati le ob pozornem spremljanju tehnologije, poslovnih zahtev in pojavu novih groženj in tveganj. V krogu PDCA sodi torej notranja presoja v fazo »preveri«, hkrati pa, upoštevajoč popravne ukrepe, ki iz nje izhajajo, tudi v fazo »ukrepaj« (Do).

Poleg notranje presoje obstajajo še drugi načini preverjanja, kot so: rutinsko preverjanje, samoupravljalni postopki in vodstveni pregledi. Pri rutinskem preverjanju gre za spremljanje SUVI kot del običajnega poslovnega procesa, na primer preverjanje, da ne pride do nenamernih ali nepooblaščenih sprememb v nastavitvah, podatkih in podobno. Samoupravljanje je vrsta nadzora, ki omogoča zaznavo kakršne koli napake med delovanjem opreme ali izvajanjem nekega procesa, namen vodstvenih pregledov pa je, da se najmanj enkrat letno preveri, ali je SUVI učinkovit, ali obstajajo možnosti za njegove izboljšave in morebitne dodatne ukrepe.

3 VPELJAVA VARNE HRAMBE E-GRADIVA

Elektronsko oziroma digitalno gradivo je v dokumentu Enotne Tehnološke Zahteve (v nadaljevanju: ETZ), izdal ga je Arhiv Republike Slovenije, definirano kot elektronsko gradivo, ki je izvorno ustvarjeno s pomočjo informacijske tehnologije ali pa z njeno pomočjo ustvarjeno iz drugih oblik dokumentarnega gradiva. Poleg besedila so v elektronsko gradivo lahko vključeni tudi drugi podatki, kot so slike, programi, filmi, zvočni posnetki ipd. Enotne tehnološke zahteve podrobneje opredeljujejo poslovne, organizacijske in tehnološke pogoje za izpolnjevanje ZVDAGA in podzakonskih predpisov, izdanih na njegovi podlagi. Pravna oseba mora glede hrambe svojega elektronskega gradiva sprejeti notranji pravni akt, ki vsebuje pravila zajema in hrambe gradiva v digitalni obliki. Obstoj notranjih pravil je bistvenega pomena pri presojanju veljavnosti dokumentarnega gradiva v elektronski obliki. Pri vzpostavitvi sistema za varno hrambo elektronskega gradiva je potrebno upoštevati varnostna določila, ki se nanašajo na:

- infrastrukturo, njeno varnost in zanesljivost,
- prostore in osebje, pristojnosti in naloge osebja in zunanjih sodelavcev,
- fizično varovanja infrastrukture - predvsem glede dostopa v prostore (vstopne pravice, avtentikacijski sistem …),
- ravnanja s strojno in programsko opremo,
- elektronsko oziroma programsko varovanje (varnostne nastavitve strežnikov, uporaba telekomunikacijskih sredstev in opreme ter prijave v sistem, varnostne kopije ...),
- notranji nadzor (operativna izvedba in spremljanje dogodkov: kontrola fizičnega dostopa, kontrola pooblastil, poročanje o varnostnih problemih ...),
- ukrepe ob nepredvidenih dogodkih ter vodenje dnevnikov in sestave zapisnikov,
- aktivnosti v zvezi s tehnološkim staranjem strojne in programske opreme, propadanjem za dolgoročno hrambo elektronskega gradiva uporabljenih nosilcev zapisa in zastaranjem oblik zapisov.

Ključni elementi pri zajemu in hrambi gradiv v elektronski obliki so:

- uporaba ustrezne informacijske infrastrukture,
- strokovno upravljanje in
- dosledno upoštevanje uveljavljenih pravil s področja varovanja informacij (zagotavljanje zaupnosti, celovitosti in razpoložljivosti).

Za zagotovitev ustrezne stopnje informacijske varnosti in upravljanja z informacijsko tehnologijo se je priporočljivo nasloniti na mednarodni standard ISO/IEC 27001 (Informacijska tehnologija - Varnostne tehnike – Sistemi za upravljanje varovanja informacij – Zahteve) in ISO/IEC 27002 (Informacijska tehnologija - Varnostne tehnike – Kodeks za upravljanje varovanja informacij). Ta par standardov celovito pokriva zahteve določil ZVDAGA. Za dosego ustrezne informacijske varnosti in upravljanja informacijske tehnologije pa se, kot zapisano, lahko organizacija drži tudi drugih standardov ali priporočil (npr.: ITIL, COBIT …), ki pokrivajo postavljene zahteve.

Enotne tehnološke zahteve v poglavju 2.2 INFORMACIJSKA INFRASTRUKTURA in poglavja 3.2 NADZOR IN VARNOST med drugim opredeljujejo naslednje zahteve, ki jih mora izpolniti organizacija:

- politika varovanja informacij,
- organiziranost varovanja informacij,
- upravljanje informacijskih sredstev,
- varnost in človeški viri,
- fizično in tehnično varovanje opreme in storitev,
- upravljanje komunikacijske infrastrukture in operativno delovanje,
- obvladovanje dostopa do sistemov,
- razvoj in vzdrževanje (aplikacijskih) informacijskih sistemov,

- upravljanje varnostnih dogodkov,
- zagotavljanje neprekinjenega delovanja,
- zagotavljanje skladnosti na področju varovanja informacij,
- dostop (nadzor nad dostopom, prikaz metapodatkov pri iskanju),
- revizijske sledi (sledenje vsem akcijam uporabnikov),
- rezervna kopija in obnova,
- sledenje gibanju dokumentov,
- avtentičnost in celovitost,
- vrste in stopnje tajnosti.

Iz navedenih zahtev je razvidno, da organizacija z vpeljanim in delujočim sistemom upravljanja varovanja informacij (SUVI), skladnim s standardom ISO/IEC 27001, izpolnjuje tudi določila ETZ s področja varovanja. Organizacija mora vzpostaviti in voditi tak sistem upravljanja varovanja informacij, ki ima zagotovljeno ustrezno dokumentacijsko podporo, ki je lahko del splošnih pravil organizacije ali notranjih pravil v zvezi z izvajanjem zajema in hrambe.

Delovanje SUVI mora temeljiti na izvedeni oceni tveganj, ki je podlaga za izbor ustreznih nadzorstev (organizacijske strukture, postopki, ukrepi, razdelitve nalog…). Metoda analize tveganj je predpisana in se izvaja redno, najmanj enkrat letno in ob večjih spremembah. Seveda morajo biti izpolnjene tudi zahteve poglavja, ki se nanaša na skladnost z zakonodajo in drugimi pravnimi predpisi.

4 PRAVNI VIDIKI VARNE HRAMBE E-GRADIVA

Osnovne pravne norme vzpostavitve varnih sistemov za dolgoročno hrambo gradiva v elektronski obliki najdemo v Zakonu o varstvu dokumentarnega in arhivskega gradiva ter arhivih (Ur. l. RS, št. 30/2006, v nadaljevanju: ZVDAGA), v Uredbi o upravnem poslovanju, Uredbi o pogojih za elektronsko poslovanje in elektronsko podpisovanje in v drugih sorodnih predpisih ter v varnostnih standardih družine ISO/IEC 27000. ZVDAGA pravno veljavnost dokumentarnega gradiva pogojuje z načinom njegovega zajema in hrambe, saj ravno v času zajema in hrambe dokumentarnega gradiva obstaja možnost, da je avtentičnost in celovitost gradiva okrnjena. Zakon zato določa tri različne scenarije, po katerih se pravna veljava takšnega gradiva presoja (ETZ, 2006 str. 11).

Na podlagi zakona se tistemu dokumentarnemu gradivu, ki je bilo zajeto in varno hranjeno v skladu s strani državnega arhiva potrjenimi notranjimi pravili subjekta, ki je hrambo in zajem gradiva izvajal, prizna enakost izvirnemu gradivu, posledica tega pa je, da je tudi pravna veljavnost takega gradiva enaka pravni veljavnosti izvirnika. Takšno gradivo torej deli usodo uzvirnika že po samem zakonu, kar pomeni, da njegove pravne veljavnosti ni potrebno posebej dokazovati.

Druga možnost je, da je bilo gradivo varno hranjeno in zajeto pri subjektu, ki sicer deluje po nekih zapisanih notranjih pravilih, vendar takšna pravila niso bila potrjena s strani državnega arhiva. V takšnem primeru je dokumentarnemu gradivu lahko priznana enakost z izvirnikom, vendar je potrebno pred tem dokazati, da so

notranja pravila subjekta skladna z zakonom, podzakonskimi predpisi ter enotnimi tehnološkimi zahtevami, za katere bo poskrbel državni arhiv.

Tretja možniost pa je, da je bilo določeno gradivo hranjeno ali zajeto pri subjektu, ki tega nima urejenega z notranjimi pravili ali ki pravila sicer ima, vendar se jih v konkretnem primeru ni držal, ali pa gre za primer, ki ga potrjena pravila ne urejajo. V vseh teh primerih se enakost elektronskega gradiva z izvirnim presoja v vsakem posameznem primeru, kar pomeni, da mora izpolnjevati enake pogoje varne hrambe kot izvirno gradivo.

4.1 Varna hramba e-gradiva z vidika Zakona o varstvu osebnih podatkov

Pri vzpostavitvi sistema zajema in hrambe gradiv v elektronski obliki, ki vsebujejo osebne podatke, je potrebno upoštevati in zagotoviti tudi skladnost z Zakonom o varstvu osebnih podatkov (ZVOP-1, 2005). S tem zakonom se določajo pravice, obveznosti, načela in ukrepi, s katerimi se preprečujejo neustavni, nezakoniti in neupravičeni posegi v zasebnost in dostojanstvo posameznika oziroma posameznice pri obdelavi osebnih podatkov (1. člen ZVOP-1). Poleg načela zakonitosti in poštenosti je eno izmed temeljnih načel tega zakona tudi načelo sorazmernosti, ki določa, da morajo biti osebni podatki, ki se obdelujejo, ustrezni in po obsegu primerni glede na namene, za katere se zbirajo in nadalje obdelujejo. Za samo razumevanje zakona je pomembno poznati in razumeti osnovne pojme, ki jih opredeljuje navedeni zakon, med drugim kako so določeni pojmi osebni podatek, zbirka osebnih podatkov, obdelava osebnih podatkov.

Zbirka osebnih podatkov je v ZVOP-1 določena posredno, s pomočjo termina *osebni podatek*, ki je določen v prvi točki 6. člena ZVOP-1, kot *katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen*. Nadalje druga točka 6. člena ZVOP-1 določa, da je posameznik *določena ali določljiva fizična oseba, na katero se nanaša osebni podatek; fizična oseba je določljiva, če se jo lahko neposredno ali posredno identificira, predvsem s sklicevanjem na identifikacijsko številko ali na enega ali več dejavnikov, ki so značilni za njeno fizično, fiziološko, duševno, ekonomsko, kulturno ali družbeno identiteto, pri čemer način identifikacije ne povzroča velikih stroškov, nesorazmerno velikega napora ali ne zahteva veliko časa. Zbirka osebnih podatkov* je tako določena v peti točki 6. člena ZVOP-1 kot vsak *strukturiran niz podatkov, ki vsebuje vsaj en osebni podatek, ki je dostopen na podlagi meril, ki omogočajo uporabo ali združevanje podatkov, ne glede na to, ali je niz centraliziran, decentraliziran ali razpršen na funkcionalni ali geografski podlagi; strukturiran niz podatkov je niz podatkov, ki je organiziran na takšen način, da določi ali omogoči določljivost posameznika*. Pojem obdelave osebnih podatkov je določen v 3. točki 6. člena ZVOP-1 kot kakršnokoli delovanje ali niz delovanj, ki se izvaja v zvezi z osebnimi podatki, ki so avtomatizirano obdelani ali ki so pri ročni obdelavi del zbirke osebnih podatkov ali so namenjeni vključitvi v zbirko osebnih podatkov, zlasti zbiranje, pridobivanje, vpis, urejanje, shranjevanje, prilagajanje ali spreminjanje, priklicanje, vpogled, uporaba, razkritje s prenosom, sporočanje, širjenje ali drugo dajanje na razpolago, razvrstitev ali povezovanje, blokiranje, anonimiziranje, izbris ali uničenje; obdelava je lahko ročna ali avtomatizirana (sredstva obdelave). Pojem »obdelava osebnih podatkov« je eden izmed najpomembnejših terminov s področja varstva osebnih podatkov, saj je v 1. členu ZVOP-1 določeno, da se določbe tega zakona uporabljajo le, kadar gre za obdelavo osebnih podatkov. Definicija obdelave osebnih podatkov je postavljena zelo široko, saj v definiciji pojma obdelave z besedo »zlasti« le primeroma našteva možne

oblike obdelovanja, iz česar izhaja, da tudi kakršnokoli drugo ravnanje z osebnimi podatki pomeni njihovo obdelovanje. Tako je npr. poleg hranjenja tudi nepooblaščen vstop v zbirko osebnih podatkov in njihovo kopiranje obdelava osebnih podatkov.

Z vidika zakonsko skladne hrambe gradiva pa je bistveno upoštevanje določil 24. člena ZVOP-1, ki določa, da zavarovanje osebnih podatkov obsega organizacijske, tehnične in logično-tehnične postopke in ukrepe, s katerimi se varujejo osebni podatki, preprečuje slučajno ali namerno nepooblaščeno uničevanje podatkov, njihova sprememba ali izguba ter nepooblaščena obdelava teh podatkov tako, da se varujejo prostori, oprema in sistemsko programska oprema, vključno z vhodno-izhodnimi enotami, varuje aplikativna programska oprema, s katero se obdelujejo osebni podatki, preprečuje nepooblaščen dostop do osebnih podatkov pri njihovem prenosu, vključno s prenosom po telekomunikacijskih sredstvih in omrežjih, zagotavlja učinkovit način blokiranja, uničenja, izbrisa ali anonimiziranja osebnih podatkov in omogoča poznejše ugotavljanje, kdaj so bili posamezni osebni podatki vneseni v zbirko osebnih podatkov, uporabljeni ali drugače obdelani in kdo je to storil, in sicer za obdobje, ko je mogoče zakonsko varstvo pravice posameznika zaradi nedopustnega posredovanja ali obdelave osebnih podatkov.

Nadalje je določeno, da morajo strojna, sistemska in aplikativno programska oprema v primeru obdelave osebnih podatkov, ki so dostopni preko telekomunikacijskega sredstva ali omrežja, zagotavljati, da je obdelava osebnih podatkov v zbirkah osebnih podatkov v mejah pooblastil uporabnika osebnih podatkov. Navedeni postopki in ukrepi za zavarovanje osebnih podatkov morajo biti ustrezni glede na tveganje, ki ga predstavlja obdelava in narava določenih osebnih podatkov, ki se obdelujejo. Funkcionarji, zaposleni in drugi posamezniki, ki opravljajo dela ali naloge pri osebah, ki obdelujejo osebne podatke, so dolžni varovati tajnost osebnih podatkov, s katerimi se seznanijo pri opravljanju njihovih funkcij, del in nalog. Dolžnost varovanja tajnosti osebnih podatkov jih obvezuje tudi po prenehanju funkcije, zaposlitve, opravljanja del ali nalog ali opravljanja storitev pogodbene obdelave. Dolžnost zavarovanja je določena v 25. členu ZVOP-1, ki določa, da so upravljavci osebnih podatkov in pogodbeni obdelovalci dolžni zagotoviti zavarovanje osebnih podatkov na način iz 24. člena tega zakona. Upravljavci osebnih podatkov v svojih aktih predpišejo postopke in ukrepe za zavarovanje osebnih podatkov ter določijo osebe, ki so odgovorne za določene zbirke osebnih podatkov, in osebe, ki lahko zaradi narave njihovega dela obdelujejo določene osebne podatke.

V primeru, da je infrastruktura, na kateri se hranijo (in s tem obdelujejo) osebni podatki, v tretji državi, je pomembno tudi poznavanje in zagotavljanje določil o iznosu osebnih podatkov v tretje države. Prav tako je bistveno zagotavljanje ustreznih postopkov v primeru obdelave občutljivih osebnih podatkov.

5 ZAKLJUČEK

Ključni elementi pri zajemu in hrambi gradiv v elektronski obliki so uporaba ustrezne informacijske infrastrukture, njeno strokovno upravljanje in dosledno upoštevanje uveljavljenih pravil s področja varovanja informacij (zagotavljanje zaupnosti, celovitosti in razpoložljivosti). Načrtovanje in vpeljava varnosti informacijskih sistemov in z njimi povezane informacijske tehnologije pomeni za organizacijo zaščito informacijskih virov in ostalega premoženja, ki ga organizacija poseduje.

Cilj vsakega varnostnega načrtovanja je zaščititi kritično poslanstvo organizacije, odstranitev groženj ali vsaj zmanjšanje na sprejemljiv nivo ter z zmanjševanjem tveganja, skladno s pravnimi in regulativnimi predpisi, zagotavljati neprekinjeno poslovanje organizacije, neokrnjenost, razpoložljivost in zaupnost podatkov in informacij. Organizacija, ki ima vpeljan in delujoč sistem upravljanja varovanja informacij (SUVI), skladen s standardom ISO/IEC 27001, izpolnjuje tudi določila ETZ s področja varovanja. Organizacija mora vzpostaviti in voditi tak sistem upravljanja varovanja informacij, ki ima zagotovljeno ustrezno dokumentacijsko podporo, ki je lahko del splošnih pravil organizacije ali notranjih pravil v zvezi z izvajanjem zajema in hrambe.

V praksi se je pokazalo, da je za sistematično načrtovanje in upravljanje varnosti nujno potrebno dobro poznavanje varnostnih elementov, prav zaradi njihove soodvisnosti, prepletanja in dopolnjevanja. Napačna ocena njihove pomembnosti lahko vpliva na končni rezultat procesa načrtovanja in upravljanja varnosti. Dobro poznavanje teh elementov pravzaprav predstavlja osnovo, temelj kasnejšega procesa upravljanja tveganj, predvsem ocene tveganj, kjer varnostne elemente proučujemo, med seboj povezujemo, jim določamo vrednost, do končnega rezultata, ki nam podaja poročilo o stanju tveganj in groženj, ki pretijo organizaciji. Pri upravljanju tveganj moramo vedeti, kakšne možnosti, strategije, pristope ali metodologije imamo na voljo za izluščenje potrebnih informacij o stopnji tveganja in s tem izhodišč za izbiro in vpeljevanje ustreznih varnostnih kontrol za zmanjševanje ali omejevanje tveganja. Poznavanje postopkov in smernic upravljanja tveganj je v načrtovanju in upravljanju varnosti izrednega pomena tudi zato, ker so rezultati, ki jih pridobimo v tem procesu, uporabni tudi za načrtovanje neprekinjenega poslovanja ter pri opredelitvi varnostne politike.

Zavedati se moramo, da sistem upravljanja varovanja informacij in proces elektronske hrambe podatkov ne more biti uspešen brez ustreznega razvijanja varnostne kulture v podjetju, izobraževanja o varnostnih vidikih in spodbujanja motivacije za zaščito dobrin podjetja. Standard priporoča, da se tako izobraževanje zaposlenih izvede vsaj enkrat letno, bistveni namen programov varnostnega ozaveščanja, izobraževanja in urjenja pa je predvsem zagotavljanje zavedanja posameznikov (od vodstva, odločevalcev, upravljavcev in vzdrževalcev do običajnih uporabnikov), ki so vključeni v proces varovanja, o namenu in potrebnosti vpeljave in vzdrževanja varnostnega programa.

VIRI IN LITERATURA

- BS ISO/IEC 27001:2005: *Information Security Management Systems - Requirements.* (2005). BSI.
- BS ISO/IEC 27002:2005: *Information Technology - Security Techniques - Code of practice for information security management.* (2005). BSI.
- Enotne tehnološke zahteve (ETZ) (2006). Arhiv Republike Slovenije.
- IT Governance Institute: *COBIT* (2005). USA.
- Priročnik za upravljavce osebnih podatkov (2007). Informacijski pooblaščenec Republike Slovenije.
- Zakon o elektronskih komunikacijah (ZEKom-1) (2012). *Uradni list RS,* št. 109/2012.
- Zakon o kazenskem postopku (ZKP-UPB4) (2007). *Uradni list RS,* št. 32/2007.
- Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih (2006). Uradni list RS, št. 30.

- Zakon varstvu osebnih podatkov (ZVOP-1) (2005). *Uradni list RS*, št. 94/2007.
- Zakon o varstvu osebnih podatkov (ZVOP-1) (2006). ZVOP-1 s komentarjem. Ljubljana: Narodna in univerzitetna knjižnica.

SUMMARY

Marko POTOKAR[*]*, Igor BERNIK*[**]

IMPLEMENTATION OF AN INFORMATION SECURITY MANAGEMENT SYSTEM FOR THE E-ARCHIVES PROJECT IN COMPLIANCE WITH PDAAIA AND PDPA

Key elements in gathering and keeping materials in electronic form are the use of suitable information infrastructure, its professional management and consistent following of established rules from the field of information security (ensuring confidentiality, integrity and availability). Planning and introduction of information system security, and therewith connected information technology, means protection of information sources and other property possessed by an organization. Thus, the goal of each security planning is to protect critical mission of an organization, to remove or at least reduce threats to an acceptable level, and by reducing risk, in accordance with legal rules and regulations, ensure continuous operation of an organization, integrity, availability and confidentiality of data and information. An organization with an established and working information security management system (ISMS) which is in accordance with the ISO/IEC 27001 standard, also follows the rules of UTR from the field of security. An organization has to establish and run such an information security management system that provides suitable documentation support, which can be part of general rules of an organization or internal rules regarding gathering and keeping information.

It has been shown in practice that for systematic planning and management of security it is necessary to possess good knowledge of security elements because of their codependence, intertwinement and supplementation. Misjudgment of their importance can crucially affect the final result of security planning and management process. Good knowledge of these elements is actually the basis, the foundation of the subsequent risk management process, especially risk evaluation where security elements are studied, linked, determined by value, to the final result giving us the report of risk and threat situation in an organization. In risk management we have to know what possibilities, strategies, approaches or methodologies are available to be able to extract necessary information about risk level and thus starting points to choose and introduce suitable security controls to reduce or limit risks. In addition, knowing risk management procedures and guidelines is of utmost importance in security planning and management because the results achieved in this process can be used in planning uninterrupted operation and determining security policy.

[*] *Marko Potokar, MA, president of the council of the Institute for Security Culture; member of the Institute for Comparative Securitiy Studes; member of the professional council of the Institute for the Forensics of Information technologies, state supervisor for the protection of personal data, Information Comissioner of the Republic of Slovenia, Zaloška 59, 1000 Ljubljana, Slovenia, contact: marko.potokar@ifit.si.*

[**] *Igor Bernik, Ph. D., head of Information Security Lab and Vice Dean for Academic Affairs at the Faculty of Criminal Justice and Security, Univerity in Maribor, Kotnikova ulica 8, 1000 Ljubljana, Slovenia, contact: igor.bernik@fvv.uni-mb.si.*

However, we have to be aware of the fact that information security management system and electronic data storing process cannot be successful without adequate development of security culture in the company, education about security aspects and encouraging motivation to protect company goods. The standard recommends such education and training of employees at least once a year; the main goal of security promotion programmes, education and training is mostly to make the individuals (from leadership, decision-makers, managers, maintenance, to general users) who are included in the security process aware of the purpose and importance of introduction and maintenance of security programme.