Manja Konkolič[1]
(Slovenia)

METODOLOGIJA UPRAVLJANJA S TVEGANJI NA PODROČJU E-HRAMBE

ABSTRACT

Purpose: *This paper will define and study risk factors and risk management in the field of e-storage. The aim is to identify individual risks and vulnerabilities for information security and e-storage.*

Method / approach: *We used a systematic review and analysis of existing literature and sources.*

Results: *The results show that it is important for each organization to make a risk assessment in order to manage the risk in accordance with law, organization, business, environment, technology and human resources. It must be based on a documented methodology.*

Conclusions / practical applicability: *The results are useful in further research in this field.*

Key words: *e-storage, risks, uniform technological requirements, security*

SINTESI

Scopo: *In questo documento, definiremo e studieremo i fattori di rischio e la gestione del rischio nel campo dell'e-storage. Scopo di questo documento è identificare i rischi individuali e le vulnerabilità per la sicurezza delle informazioni e l'archiviazione elettronica.*

Metodo / approccio: *Abbiamo utilizzato una revisione e un'analisi sistematiche della letteratura e delle fonti esistenti.*

Risultati: I *risultati mostrano che è importante per ogni organizzazione una valutazione del rischio che gestisca il rischio legalmente, organizzativamente, ed aziendale, ambientale, tecnologico e delle risorse umane. Deve basarsi su una metodologia documentata.*

Conclusioni / applicabilità pratica: *I risultati sono utili per ulteriori ricerche in questo campo.*

Parole chiave: *e-storage, rischi, requisiti tecnologici uniformi, sicurezza.*

ABSTRAKT

Namen: *V prispevku bomo opredelili in proučevali dejavnike tveganja in upravljanje s tveganji na področju e-hrambe. Cilj prispevka je ugotoviti posamezna tveganja in ranljivosti za informacijsko varnost in e-hrambo.*

Metoda/pristop: *Uporabili smo sistematičen pregled in analizo obstoječe literature in virov.*

Rezultati: *Rezultati kažejo, da je pomembo, da vsaka organizacija izdela oceno tveganja, s katero se obvladuje tveganje tako pravno, organizacijsko, poslovno, okoljsko, tehnološko kot tudi s človeškimi viri. Temeljiti mora na dokumentirani metodologiji.*

Sklepi/praktična uporabnost: *Rezultati so uporabni pri nadaljnjih raziskavah na tem področju.*

Ključne besede: *e-hramba, tveganja, enotne tehnološke zahteve, varnost.*

1 Manja Konkolič, mag. var., manja.konkolic@gmail.com.

1 UVOD

Področje elektronskega arhiviranja ureja Zakon o varstvu dokumentarnega in arhivskega gradiva in arhivih (ZVDAGA). Gre za zadnji sistemski zakon, ki je bil potreben, da bi bilo področje elektronskega poslovanja celovito zaokroženo. Tehnična infrastruktura za elektronsko poslovanje in arhiviranje obstaja že nekaj časa (infrastruktura javnih ključev, overitelji digitalnih certifikatov, overitelji časovnih žigov itd.), s sprejemom ZVDAGA pa je odpadla zadnja sistemska ovira za praktično uvajanje elektronskega poslovanja in elektronskih arhivov v podjetja.

Zakon zahteva od vseh organizacij, ki bodo vzpostavile elektronski arhiv, vzpostavitev celovitega sistema načrtovanja, izvajanja in spremljanja elektronskega arhiviranja, predvsem sprejem notranjih pravil za zajem in hrambo dokumentarnega gradiva, izdelavo drugih dokumentov v zvezi s pripravo na zajem in hrambo gradiva v digitalni obliki, periodično dopolnjevanje notranjih pravil zaradi spremembe veljavnih predpisov, tehnološkega napredka in spoznanj stroke ter izvedbo drugih aktivnosti (Inštitut za ekonomijo, pravo in informatiko, 2020).

Strategija in izvedbeni narčt razvoja slovenskega elektronskega arhiva 2016-2020 navaja, da slovenski elektronski arhiv predstavlja skupno storitev dolgoročnega ohranjanja elektronskega arhivskega gradiva, katere skrbnik so slovenski javni arhivi. Storitev vključuje prevzem elektronskega arhivskega gradiva od ustvarjalcev, dolgoročno ohranjanje po načelih varne dolgoročne hrambe, kot jih določa ZVDAGA (dostopnost, uporabnost, celovitost, avtentičnost, trajnost) in zagotavljanje nadaljnje dostopnosti do tega gradiva vključno z možnostjo njegove ponovne uporabe za bodoče uporabnike. Vendar pa dolgoročno ohranjanje elektronskega arhivskega gradiva z možnostjo njegove nadaljnje uporabe ni enostavno primerljivo z dolgoročnim ohranjanjem gradiva v fizični obliki. Zahteva aktivnosti skozi celoten življenjski cikel elektronskega ahrivskega gradiva, ki se začne s kreiranjem (ali prejemom) posameznega dokumenta - kot enoto gradiva - pri ustvarjalcu pa vse do prevzema v elektronskih arhivih. Posamezni elektronski dokument v svojem življenjskem ciklu praviloma zamenja več informacijskih okolij, kontekstov in tudi skrbnikov.

Obveznsoti in pristojnosti slovenske javne ahrivske službe glede prevzemanja arhivskega gradiva ne glede na njegov nastanek (v papirni ali elektronski obliki), zagotavljanja njegove dolgoročne hrambe in omogočanja njegove uporabe, so določene v varstvu dokumentarnega in arhivskega gradiva ter arhivih (ZVDAGA). Zakonska določila podrobneje opredeljuje tudi Uredba o varstvu arhivskega gradiva in arhivih (UVDAG). ZVDAGA in UVDAG urejata upravljanje dokumentarnega in arhivskega gradiva na splošnem nivoju, upravljanje gradiva v elektronski obliki in njegovo varno hrambo pa v praksi natančneje določajo enotne tehnološke zahteve.

Upravljanje dokumentarnega gradiva je za organe državne uprave, uprave samoupravnih lokalnih skupnosti ter druge pravne in fizične osebe, kadar na podlagi javnih pooblastil opravljajo upravne naloge, določeno z Uredbo o upravnem poslovanju. Za upravljanje oziroma varstvo dokumentarnega in arhivskega gradiva v elektronski obliki sta pomembna tudi Zakon o elektronskem poslovanju in elektronskem podpisu in Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje.

1.1 Enotne tehnološke zahteve

Enotne tehnološke zahteve (ETZ), ki jih je sprejel Arhiv Republike Slovenije, podrobneje opredeljujejo poslovne, organizacijske in tehnološke pogoje za izpolnjevanje Zakona o varstvu dokumentarnega in arhivskega gradiva ter arhivih (ZVDAGA) in na njegovi podlagi izdanih podzakonskih predpisov. ETZ so povezovalni element med zakonskimi zahtevami, ki izhajajo iz temeljnih načel zagotavljanja varne e-hrambe, in hitro spreminjajočimi se potrebami prakse.

Spremenjena arhivska zakonodaja predvideva določitev vsebine zahteve za potrditev notranjih pravil, certificiranje strojne in programske opreme, storitev zajema in hrambe gradiva v elektronski obliki ter spremljevalnih storitev, registracijo ponudnikov in storitev digitalne hrambe v skladu s Pravilnikom o enotnih tehnoloških zahtevah. Ker slednji še ni sprejet, ostajajo v veljavi ETZ (verzija 2.1) iz leta 2013 (Ministrstvo za kulturo, 2020).

Zahteve za e-hrambo opredelimo kot pravne, tehnološke in poslovne. Predpisane so predvsem v ZVDAGA, UVDAG, ETZ in področni zakonodaji (npr. glede rokov hrambe). Poslovne zahteve se npr. nanašajo na razpoložljivost, varnost in zanesljivost sistema e-hrambe (opreme, storitev, gradiva) ter na skladnost s predpisi (Ministrstvo za kulturo, 2013).

ETZ so torej povezovalni element med zakonskimi zahtevami, ki izhajajo iz temeljnih načel (dostopnost, uporabnost, celovitost, avtentičnost, trajnost) zagotavljanja varne e-hrambe, in hitro se spreminjajočimi se potrebami prakse (Hajtnik, 2011).

1.2 Tveganje in ocena tveganja

Murphyev zakon pravi: »Če lahko gre kaj narobe, bo narobe tudi šlo.« Mednarodna organizacija za standarde (ISO) tveganje opredeljuje tveganje kot kombinacijo verjetnosti dogodka in njegovo posledico. SIST EN ISO 12100 definira tveganje, da je zaradi neke nevarnosti kombinacija verjetnosti, da se bo pojavila škoda zaradi te nevarnosti ter največje možne razsežnosti te škode oziroma tveganje je kombinacija največje možne razsežnosti škode zaradi neke nevarnosti in verjetnosti, da se bo ta škoda pojavila. Ukrepi in postopki informacijske varnosti morajo temeljiti na oceni tveganja, ki jo mora organizacija izdelati že v predhodni pripravi na zajem in e-hrambo. Ta ocena je zgolj podlaga za izvajanje zajema oz. vzpostavitev varnega sistema e-hrambe ter podlaga za poznejše upravljanje tveganja, zato da se gradivo ustrezno zavaruje med hrambo. Tveganje je možnost (verjetnost), da bo informacijski vir ali skupina virov ogrožena zaradi svoje ranljivosti in da bo povzročena izguba oz. škoda na njih.

Tveganja so lahko različna:

- Pravna in poslovna tveganja (najem zunanjih izvajalcev, tveganja, ki izvirajo iz notranje in zunanje organizacije, tveganja, povezana s skladnostjo s predpisi, itd.). Glede ocene pravnega tveganja organizacija določi zakone in druge predpise, ki jih mora spoštovati pri zajemu oz. e-hrambi glede na vrsto gradiva oz. vrsto podatkov, ki jih to gradivo vsebuje.
- Tveganja, povezana s človeškimi viri (nenamerna/namerna dejanja, usposobljenost osebja, pristojnosti in odgovornosti osebja itd.).
- Tveganja, povezana z okoljem:
- ne tehnološka tveganja (požar, izlitje vode, naravne ujme - poplava, neurje, potres, požar v okolju, vihar, vročina, strela, teroristični napad itd.),
- tehnološka tveganja (povezana z informacijsko tehnologijo, npr. odpoved delovanja, zastaranje strojne in programske opreme, zastaranje nosilcev podatkov, zastaranje oblik zapisa itd.).
- Druga tveganja, povezana tudi z informacijsko varnostjo in izvajanjem e-hrambe (tveganja, povezana z upravljanjem sprememb informacijske tehnologije in sistemov, itd.).

Izdelava ocene tveganja mora temeljiti na metodologijah, ki omogočajo naknadno preverjanje ugotovitev ocene in njeno poznejše posodabljanje (Ministrstvo za kulturo, 2013).

Organizacija mora pri pripravi oz. organiziranju zajema in e-hrambe izpolniti vse predpisane varnostne zahteve, bistvene za posamezno vrsto gradiva (npr. dokumentarno gradivo; arhivsko gradivo; gradivo v fizični ali digitalni obliki) oz. vrsto podatkov, ki jih bo vsebovalo zajeto oz. hranjeno gradivo (osebni, tajni, zaupni, javni ipd. podatki).

Iztočnica za načrtovanje, organiziranje in izvajanje varovanja gradiva je ocena tveganja pri zajemu oz. e-hrambi. Na njeni podlagi organizacija določi, vzpostavi in izvaja ukrepe ter postopke varovanja gradiva in delovnih postopkov ter opreme za zajem oz. e-hrambo.

Organizacija mora zagotavljanje informacijske varnosti urediti z notranjimi pravili. Pri tem mora upoštevati predpise, ki določajo način varovanja podatkov v zajetem oz. hranjenem gradivu. Med pomembnejšimi predpisi je Zakon o varstvu osebnih podatkov (ZVOP–1) , saj pravzaprav ni organizacije, pri kateri vsaj del zajetega oz. e-hranjenega gradiva ne bi vseboval tudi osebnih podatkov. Sprejetje notranjega akta kot podlage za organiziranje sistema informacijske varnosti zahteva 25. člen ZVOP-1 (npr. Pravilnik o postopkih in ukrepih za zavarovanje osebnih podatkov), poleg njega pa številni drugi predpisi, ki urejajo obdelavo manj pogostih ali na določena področja omejenih vrst podatkov (npr. 38. člen Zakona o tajnih podatkih za tajne podatke, 42. člen Zakona o državni statistiki za statistično tajnost, 54. člen Zakona o maturi za izpitno tajnost).

Določbe za organiziranje, vzpostavitev in upravljanje sistema informacijske varnosti v organizaciji morajo temeljiti na določbah ZVDAGA in drugih pravnih predpisov, ki se morajo upoštevati glede na vrsto zajetega oz. hranjenega gradiva. Pri pripravljanju ukrepov in postopkov informacijske varnosti ter aktov o ureditvi sistema te varnosti si organizacije lahko pomagajo s standardi, priporočili in dobrimi praksami s tega področja (npr. ISO 27001 in ISO 27002) (Ministrstvo za kulturo, 2013).

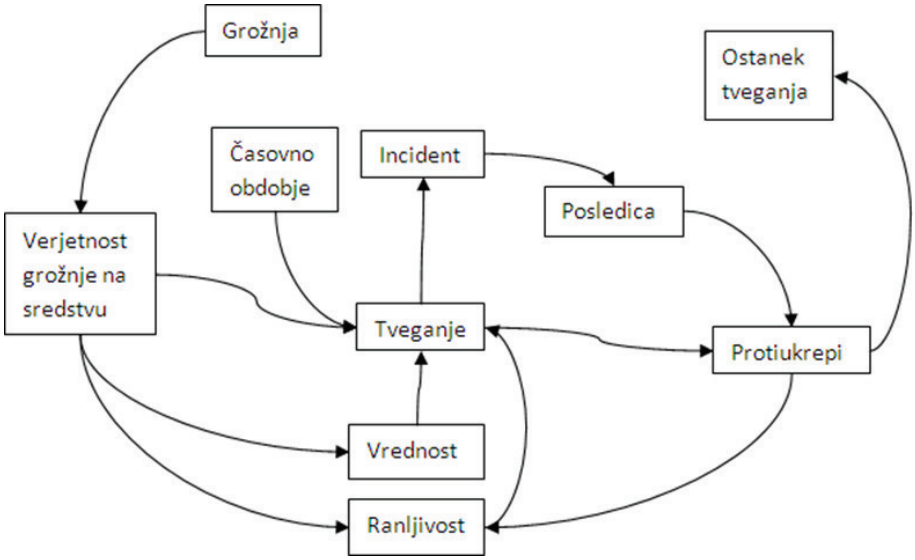
Organizacija mora izdelati oceno tveganja, s katero prepoznava in obvladuje tveganje, povezano s človeškimi viri, ter pravno, poslovno, organizacijsko, okoljsko in tehnološko tveganje, vezano na zajem oz. e-hrambo gradiva. Če organizacija vloži zahtevek za potrditev notravnjih pravil v državni arhiv, mora k vlogi priložiti tudi poročilo o izvedeni oceni tveganja. Ocena tveganja mora temeljiti na dokumentirani metodologij in mora biti najmanj enkrat na leto in ob spremembah, ki vplivajo na tveganje, posodobljena tako, da izraža dejansko stanje. Enako velja za izbrana nadzorstva (ukrepe), ki izhajajo iz ocene tveganja (Ministrstvo za kulutro, 2013).

Ocenjevanje tveganja je prvi korak pri obvladovanju tveganj. Organizacije uporabljajo ocene za določitev obsega potencialnih groženj in tveganj, povezanih z IT sistemi. Rezultat tega procesa pomaga identificirati primerne kontrole za zmanjšanje ali odpravo tveganja (Žvanut, 2011).

1.3 UPRAVLJANJE S TVEGANJI

Upravljanje s tveganji je temelj vsake informacijske varnostne politike kot tudi dolgoročne e-hrambe in e-arhiviranja. Upravljanje s tveganji mora biti stalen proces (Hajtnik, 2020).

Standardni postopek za opravljanje z tveganji poteka tako, da poskušamo identificirati tveganje, oceniti kako veliko je tveganje, poskušati odpraviti ali zmanjšati tveganje in kot zadnje narediti poročilo. Konstantno poskušamo najdi tveganja in se spopasti z njimi, saj v nasprotnem primeru lahko pride, da tveganje izkoristi ranljivost in tako pride do izgube. Poleg analize tveganj se uporablja za uspešno zaščito še protokole, standarde, varnostne politike in dobre praske. Najbolj znani standardi, ki se uporabljajo pri informacijski varnosti so ISO, ANSI, OASIS, OMG, 3GPP, ENISA, ITU-T, IEEE, Cloud Security Alliance in drugi (Hribar, 2015).



Slika 1: Upravljanje s tveganji (vir: Žvanut, P., 2011)

Pri upravljanju s tveganji se gibljemo v okviru sredstev in groženj. Sredstvo predstavlja določeno vrednost organizaciji in grožnja pomeni vsak možen vzrok za incident. Tveganje je posledica interakcije med njima in pomeni možnost, da dana grožnja izkoristi ranljivost sredstva ter tako povzroči škodo. Ranljivost v tem primeru pomeni slabost, ki jo lahko izkoristi grožnja. Za zmanjšanje tveganja je potrebno ocenjevanje tveganja, kar pomeni identifikacijo tveganj, njihovo jakost in protiukrepe. predstavlja določeno tveganje. Če se grožnja uresniči, pomeni to incident (dogodek), ki ima določene posledice. Za odpravo te ranljivosti in posledično grožnje, je potrebno uveljaviti pravilne protiukrepe. Po uveljavitvi protiukrepov še zmeraj ostane določeno tveganje (ostanek tveganja), ker ne moremo vedno 100 % odpraviti ranljivosti (Žvanut, 2011).

Upravljnje s tveganji vsebuje in opredeljuje ustrezne ukrepe, vire, odgovornosti in prioritete za upravljanje s tveganji. Vzpostavljen mora biti v kontekstu notranjih pravil in informacijske varnostne politike z jasno opredeljenim pristopom k tveganjem in merili za njihovo sprejemanje (Hajtnik, 2019).

Ranljivost informacijskega sistema je vsaka pomanjkljivost informacijskega sistema, ki jo lahko določena grožnja izrabi. Je posledica slabe zaščite informacijskega sistema zoper določeno grožnjo ali aktivnosti napadalca. Ranljivost sama po sebi ne povzroča škode, je zgolj stanje ali serija stanj, ki dopušča, da grožnja vpliva na informacijski sistem (Koščak, 2011).

Obvladovanje tveganj je proces prepoznavanja ranljivosti in grožnje za informacijske vire, ki jih uporabljajo organizacije za doseganje poslovnih ciljev, in odločanje o nasprotnih ukrepih, če so ti potrebni za zmanjševanje tveganj na sprejemljivo raven, osnovano na vrednotah informacijskih virov organizacije. Proces obvladovanja tveganj je ponavljajoč proces, ki je neomejen. Poslovno okolje se neprestano spreminja in nove grožnje ter ranljivost se pojavljajo vsakodnevno. Izbira nasprotnih ukrepov (kontrole) z obvladovanjem tveganj mora oblikovati ravnovesje med produktivnostjo, ceno, učinkovitostjo nasprotnih ukrepov, in varovanje vrednosti informacijske pridobitve.

Tveganje je verjetnost, da se zgodi nekaj slabega, kar povzroči podjetju materialno ali nematerialno škodo. Ranljivost je šibkost, ki lahko ogrozi ali povzroči podjetju materialno ali nematerialno škodo. Grožnja je nekaj, kar ima potencial za povzročitev škode.

Tveganje ustvarja verjetnost, da bo grožnja izrabila ranljivost za povzročitev škode. Posledice nastopijo kadar grožnja izrabi ranljivost ter povzroči škodo. V kontekstu informacijske varnosti, je posledica izguba razpoložljivosti, neokrnjenosti ter zaupnosti in morda še drugih izgub (izguba dobička, izguba življenja, izguba lastninske pravice). Ugotovimo lahko, da ni možno identificirati vsa tveganja, niti jih izločiti. Ostalo tveganje je imenovano preostalo tveganje. Z ukrepi je možno tveganja zmanjšati na sprejemljivo raven.

Skladno z ISO/IEC 27002:2005 postopek za upravljanje informacijske varnosti zahteva oceno tveganja, ki zahteva sledeča preverjanja:

- varnostna politika,
- organizacija informacijske varnosti,
- upravljanje dobička, varnost človeških virov,
- fizična in okoljska varnost,
- komunikacijsko in operacijsko upravljanje,
- kontrola dostopa,
- pridobitev informacijskega sistema,
- razvoj in vzdrževanje,
- informacijska varnost obvladovanja incidentov,
- upravljanje neprekinjenega poslovanja in
- normativna skladnost.

Proces upravljanja z tveganji je sestavljen iz:

- Identifikacije premoženjskega stanja in ocene vrednosti. Vsebuje: ljudi, stavbe, računalniško strojno opremo, programsko opremo, podatke (digitalne, tiskane, ostalo), sredstva za oskrbo.
- Ocene tveganja. Vsebuje: vplivi narave, posledice vojne, nesreče, zlonamerno delovanje, ki izvira iz notranje in zunanje organizacije.
- Ocene ranljivosti in verjetnost, da bo le-ta izkoriščena. Vrednotenje politike, postopkov, standardov, izobraževanja, fizične varnosti, kvalitete kontrole, tehnične varnosti (Housing, 2020).

2 INFORMACIJSKA VARNOST

Informacijska varnost je vedno spreminjajoča in razvijajoča se aktovnost, ki pomeni varstvo podatkov in informacijskih sistmov pred nazkonitim dostopom, uporabo, razkritjem, ličitvijo, spremembo ali uničenjem (Von Sloms, 2009 v Bernik in Selan, 2011). Glavni elementi informacijske varnosti, poznani kot CIA model, so zaupnost, celovitost in razpoložljivost. Informacijska varnost ni le tehnični izziv, ampak tudi izziv celotne organizacije in vodenje le-te, ki zajema tvegani management, poročanje in odgovornost (Bernik in Selan, 2011).

Informacijska varnost obsega organizacijske in tehnične ukrepe ter postopke varne hrambe izvirnega, zajetega ali pretvorjenega gradiva. Namen izvajanja ukrepov in postopkov informacijske varnosti je:

- varovanje gradiva pred njegovo izgubo, nepooblaščenimi spremembami ali nepooblaščenim razkritjem,
- omejevanje dostopa do shranjenega gradiva na pooblaščene uporabnike,

- zagotavljanje varnosti in razpoložljivosti informacijskih sistemov za zajem in e-hrambo oz. s tem povezane spremljevalne storitve,
- zagotavljanje pravne veljavnosti e-hranjenega gradiva, kar omogoča uporabo tega gradiva kot dokazila v različnih uradnih postopkih.

Za doseganje načel varne e-hrambe moramo zagotoviti ukrepe in postopke, s katerimi bomo varovali gradivo pred njegovo izgubo in okrnitvijo ter dokazovanjem celovitosti:

- Prvo zahtevo, ki se nanaša na preprečevanje izgube, izpolnjujemo z ustreznim številom varnostnih kopij gradiva na različnih mestih, s prepisovanjem njegove vsebine na nove nosilce zapisa, preden obstoječi propadejo, s stalnim preverjanjem nosilcev zapisa in s pravočasno pretvorbo gradiva iz ene obliko zapisa v drugo pred zastaranjem oblike, v kateri je hranjeno.
- Drugo zahtevo, ki se nanaša na varovanje pred okrnitvijo in dokazovanjem celovitosti gradiva ter obsega zagotavljanje njegove točnosti, nespremenljivosti in popolnosti oz. reprodukcije njegove vsebine in dokazljivosti njegovega izvora ves čas hrambe, pa izpolnjujemo s tvorbo in hrambo ustreznih metapodatkov in revizijskih sledi o zajemu, pretvorbi, popravkih ali dopolnitvah hranjenega gradiva.
- Gradivo oz. reprodukcija njegove vsebine sme biti ves čas trajanja hrambe dostopno (le) pooblaščenim uporabnikom. Zahteva po omejevanju dostopa obsega tudi:
- omejevanje dostopa do prostorov, v katerih sta oprema in infrastruktura informacijskega sistema za zajem in e-hrambo,
- omejevanje dostopa do prostorov, v katerih se hranijo nosilci zapisov gradiva oz. v katerih je nameščena oprema informacijskega sistema za zajem in e-hrambo,
- varnostne ukrepe in postopke v zvezi z osebjem, ki sodeluje pri zajemu in e-hrambi.

Za delovanje informacijskega sistema za zajem in e-hrambo je pomembno tudi zagotavljanje potrebne okoljske varnosti.

Zgornje navedbe o hrambi arhivskega gradiva oz. gradiva javnopravnih oseb spadajo v t. i. materialno varstvo gradiva (Ministrstvo za kulturo, 2013).

2. 1 Pravna ureditev informacijske varnosti

Odločitev o formalni obliki notranje pravne ureditve informacijske varnosti je odvisna predvsem od ugotovitev ocene pravnega tveganja, po katerih se organizacija odloči, ali bo to področje uredila:

1. neposredno z notranjimi pravili oz. s posebnim aktom o (za)varovanju zajema oz. e-hrambe (npr. s pravilnikom, poslovnikom, navodilom, politiko informacijske varnosti);

2. z ustrezno dopolnitvijo obstoječih aktov organizacije s področij:

- (za)varovanja podatkov (npr. pravilnika o zavarovanju osebnih podatkov, o zavarovanju tajnih podatkov, o zavarovanju poslovnih skrivnosti),
- urejanja drugih varnostnih vprašanj (npr. požarne varnosti, hišnega reda ipd.),
- organiziranosti ter opisa del in nalog zaposlenih (npr. akt o organizaciji in sistemizaciji delovnih mest),
- upravljanja dokumentarnega gradiva (npr. pravilnik o pisarniškem poslovanju) ipd.

Vsebina aktov oz. dokumentov, s katerimi organizacija uredi informacijsko varnost, je odvisna od ugotovitev ocene tveganja, varnostne razvrstitve informacijskih virov ter organiziranosti in področja poslovanja organizacije.

Če organizacija sprejme politiko informacijske varnosti kot samostojno dokumentacijo, je ta sestavni del notranjih pravil. Navadno jo sestavljajo krovni dokument na najvišji ravni in področne varnostne politike na drugi ravni, ki jih dopolnjujejo različna navodila, obrazci in notranji standardi na tretji ravni.

V krovnem dokumentu politike informacijske varnosti se zapišejo obvezujoča pravila in predpisi, ki se nanašajo na splošna načela upravljanja informacijskega sistema, npr.:

- namen in cilj varnostne politike,
- odgovornosti (vodstva, zaposlenih, tretjih oseb),
- odgovorne osebe za informacijsko varnost in njeno izvedbo,
- usklajenost (npr. s predpisi, tehnologijo),
- način in pogostost preverjanja in dopolnjevanja varnostne politike,
- način obravnavanja varnostnih incidentov pri varovanju informacij (kršenje politike in disciplinski ukrepi),
- organizacija dokumentacije, ki predstavlja politiko informacijske varnosti in se nanaša na posamezna področja,
- veljavnost.

V področnih varnostnih politikah pa so natančneje opredeljene zahteve po uvedbi varnostnih ukrepov in postopkov varovanja na posameznih področjih, ki morajo izhajati iz ocene tveganja ter odgovornosti za izvedbo, način uvedbe in nadzor nad njimi. Z vidika zahtev po varovanju, kakršne določa ZVDAGA, lahko opredelimo področne varnostne politike, ki se npr. nanašajo na: varovanje v zvezi z osebjem, upravljanjem informacijskih virov in informacijske infrastrukture ter operativnega delovanja, s fizičnim in tehničnim varovanjem, z upravljanjem dostopnih pravic, naročanjem storitev pri zunanjih izvajalcih in neprekinjenim poslovanjem.

Za organiziranje in izvajanje ukrepov ter postopkov informacijske varnosti mora organizacija imenovati odgovorno osebo (vodjo informacijske varnosti), katere naloge so predvsem:

- nadzor stanja informacijske varnosti,
- odrejanje ukrepov za zagotavljanje informacijske varnosti,
- nadzor nad upravljanjem in izvajanjem varnostnih ukrepov in postopkov pri zagotavljanju informacijske varnosti,
- vodenje razvida informacijskih varnostnih incidentov,
- vodenje seznamov oseb, pooblaščenih za samostojen vstop v prostore, v katerih so nameščene ključne naprave sistema za zajem oz. e-hrambo,
- vodenje seznamov oseb, pooblaščenih za dostop do hranjenega gradiva,
- sodelovanje pri sistemih za upravljanje identitet in dostopnih pravic uporabnikov sistema za zajem oz. e-hrambo.

Zaposleni v organizaciji (redno in začasno) in morebitni zunanji sodelavci morajo podpisati izjavo o zaupnosti oz. varovanju informacij. S podpisom te izjave potrdijo, da so seznanjeni s predpisi in akti, ki v organizaciji urejajo varovanje gradiva in njegove vsebine kot predmeta zajema in e-hrambe (Ministrstvo za kulturo, 2013).

3 ISO STANDARDI

Standardi za informacijsko varnost se področno razlikujejo, vendar je najboljši pristop še vedno v centraliziranem upravljanju pri implementaciji varnostnih mehanizmov (SUVI – Sistem upravljanja varovanja informacij).

ri razvoju e-hrambe je smiselno implementirali različne standarde s področja dolgoročnega ohranjanja elektronskega gradiva, predvsem pa:

- ISO 14721 Space data and information transfer systems - Open archival information systems - Reference model.
- ISO 15489-1 Information and documentation - records management.
- ISO 27001 Information technology - Security techniques - Information security management systems – Requirements.
- ISO 27002 Information technology - Security techniques - Information security management systems - Code of Practice.
- ISO 13008 Information and documentation - Digital records conversion and migration process.
- ISO 20652 Space data and information transfer systems – Producer–archive interface – Methodology abstract standard.
- ISO 27005 Information technology – Security techniques – Information security risk management.
- ISO 18128 Information and documentation – Risk assessment for records processes and systems.
- ISO 27002 Information technology – Security techniques – Code of practice for information security controls.

4 UKREPI IN ZAŠČITNI MEHANIZMI

Za zagotavljanje informacijske varnosti je pomembno, da zagotovimo zapunost, neokrnjenost in razpoložljivost informacij. Zaupnost pomeni, da so informacije dostopne samo pooblaščenim osebam. Neokrnjenost pomeni, da je zagotovljena točnost in popolnost informacij in programske opreme (sama po sebi se ne sme spreminjati). Razpoložljvost pomeni, da so informacije in računalniške storitve na voljo pooblaščenim uporabnikom. Če vse to želimo zagotoviti, moramo vzpostaviti zaščitne mehanizme:

- fizični: zagotavljanje fizične varnosti in delovanja,
- logični: zagotavljanje tehničnih mehanizmov,
- proceduralni (organizacijski ukrepi): zagotavljanje varnostne politike, standardov, smernic.

Obravnavanje tveganj je odvisno od tega, kje podatke uporabljamo in koliko so za nas vredni. Tveganje lahko obravnavamo na različne načine:

- izogibanje tveganju,
- zmanjševanje tveganja,
- prenos tveganja na drugo napravo,
- sprejem tveganja (sprejmemo dejstvo, da obstaja).

Popolna varnost v realnosti ne obstaja, je pa pomembno, da uporabljamo kombinacijo naslednjih ukrepov:

- preventivni: zmanjšujejo možnost uresničitve grožnje,
- detekcijski: zaznajo grožnjo,
- korektivni: zmanjšujejo posledice napadov.

Najprej je potrebno zagotoviti zaščito strojne opreme, kar dosežemo z varovanimi prostori, zaklepanjem računalnikov, nedostopnostjo, čiščenjem in ustreznim vzdrževanjem. Programsko opremo zaščitimo z izvajanjem nadzora nad dostopi in delovanjem. S kontrolo dostopa se zaščitijo podatki, uporablja se: identifikacija, avtentikacija, avtorizacija. Gesla predstavljajo šibko zaščito, zato običajno niso primerna za visoko stopnjo zaščite. Za kontrolo dostopa in varovanje se uprablja še: požarni zidovi, antivirusni programi, programi proti vohunskim programom, sistemi za zaznavanje vdorov.

Varnostni protokoli v komunikacijskem protokolu TCP IP omogočajo vzpostavitev varne šifrirane povezave med strežnikom in odjemalcem. Najpogostejši uporabljeni protokoli za vzpostavitev varnega kanala med strežnikom in odjemalcem so:

- SSL (Secure Sockets Layer)
- TLS (Transport Layer Security)
- WTLS (Wireless Transprot Layer Security) – zasnovan na TLS in SSL, optimiziran za uporabo na ozko pasovnih komunikacijskih kanalih (Bernik, 2014).

Določiti je potrebno (organizacijski ukrep):

- postopke, odgovornosti, dokumentiranja:
- izdelati oceno tveganja, ki mora biti redno revidirana
- upoštevati načela varovanja - sprejeta, zapisana v hierarhično organizirani varnostni dokumentaciji
- določiti odgovorne osebe, ki poročajo vodostvu
- uvajanje nalog s področja varovanja informacij v poslovne procese organizacij
- dvig varnostne kulture zaposlenih in poslovnih partnerjev...

Tehnološki ukrep kot implementacija varnostnih tehnologij:

- za zaščito sistemov, dostopov, podatkov, komunikacij
- varnostno kopiranje
- oddaljene lokacije
- protivirusna zaščita
- požarni zid (firewall), ločevanje odsekov mreže
- nastavljanje varnostnih parametrov v opremi
- sistemi za nadzor dostopa do sistemov in mrež (pametne kartice, generatorji gesel za enkratno uporabo)
- varni elektronski podpis
- uvajanje sistemov fizične varnosti (alarmi, video nadzor, pristopne kontrole)
- zagotavljanje visoke razpoložljivosti sistema
- navidezno zasebno omrežje (VPN)..

Zmanjševanje tveganj, poveznih z informacijskimi sredstvi:

- popis vseh pomembnih informacijskih virov (oprema, podatki /informacije, evidence, navodila, licence, SW,...)
- varnostna razvrstitev v skladu z oceno tveganj in občutljivostjo gradiva glede na stopnjo škode škode ob izgubi
- odgovornosti za varovanje skrbniki virov ali skupin
- pravila za ravnanje; nabava, hramba, prenos, nadzor uporabe, uničenje gradiva...

Fizično in tehnično varovanje:

- zmanjševanje tveganj, poveznih s prostori in opremo:
- opredelitev varovanega območja v skladu s pomembnostjo in ranljivostjo informacijskih virov
- omejen in nadzorovan fizični dostop v posamezna varovana območja
- zaščite pred okoljskimi nevarnostmi - požar, izlitje ali vdor vode, nenadne spremembe temperature ali vlage, ... (Domanjko, 2020).

5 ZAKLJUČEK

Napredek informacijsko telekomunikacijskih tehnologij in vzporedno tudi napredno elektronsko poslovanje kažeta na motive, zaradi katerih se dokumenti, ki nastajajo pri vsaki organizaciji, vlagajo v e-hrambo. Prvi motiv je stalna dostopnost ne glede na lokacijo, drugi motiv je manjši stroški napram hrambi gradiva v fizični obliki in tretji motiv je ohranitev izvornega – digitalnega gradiva. Posledično s tem pa se pojavljajo tveganja na področju e-hrambe. Tveganja pri e-hrambi so zelo specifična; od prostorov, dostopa do prostorov, zaposlenih, vse do informacijske infrastrukture. Zato je nujno, da vsaka organizacija izdela oceno tveganja, s katero se obvladuje tveganje tako pravno, organizacijsko, poslovno, okoljsko, tehnološko kot tudi s človeškimi viri. Temeljiti mora na dokumentirani metodologiji in mora biti vsaj enkrat letno posodobljena tako, da izraža dejansko stanje. Zato je nujno zagotavljati posodobljeno informacijsko varnost v skladu z veljavno zakonodajo in predpisanimi standardi, z upoštevanjem dobrih praks, z uvedbo SUVI (učinkovitega in celovitega sistema upravljanja informacijske varnosti) in nenazadnje z organizacijskimi, tehnološkimi in fizičnimi ukrepi. Na ta način se lahko zagotovi visoka zaščita zagotavljanja varnosti.

VIRI

Bernik, I. (2014) Osnove informacijske varnosti. Univerza v Mariboru, Fakulteta za varnostne vede.

Bernik, I. in Selan, D. (2011). Upravljanje informacijske varnosti – strateški in operativni vidik. Univerza v Mariboru, Fakulteta za varnostne vede.

Domanjko, B. (2020). Strokovno usposabljanje za uslužbence javnopravnih oseb. Arhiv RS, Ljubljana. Dobljeno 20.4.2020 na spletni strani: https://www.gov.si/assets/organi-v-sestavi/Arhiv-RS/Izobrazevanja-in-usposabljanja/Uprava/Januar-2020/Predstavitve/5_eHramba.pdf

Hajtnik, T. (2019). Strokovno usposabljanje za uslužbence ponudnikov storitev zajema in e-hrambe ter spremljevalnih storitev. Ministrstvo za kulturo, Arhiv Republike Slovenije. Dobljeno 19. 4. 2020 na spletni strani: https://www.gov.si/assets/organi-v-sestavi/Arhiv-RS/Izobrazevanja-in-usposabljanja/E-hramba/December-2019/Predstavitve/THajtnik_Upravljanje-z-e-AG.pdf

Hajtnik, T. (2011). Poslovni, organizacijski in tehnološki pogoji za izpolnjevanje določil ZVDAGA: Nova verzija ETZ 2.0. V Tehnični in vsebinski problemi klasičnega in elektronskega arhiviranja. Št. 11, 419-424.

Hajtnik, T. (2020). Elektronsko arhiviranje in informacijska infrastruktura. Povzetki predavanj. Alma Mater Europaea.

Hribar, D., (2015). Informacijska varnost. Dobljeno 22. 4. 2020 na spletni strani: http://www.varensvet.si/informacijska-varnost/

Housing. (2020). Ocena tveganj. Dobljeno 19. 4. 2020 na spletni strani: https://www.housing.si/Ocena_tveganj_varnost_IS/

Inštitut za ekonomijo, pravo in informatiko. (2020). Elektronsko arhiviranje, Ljubljana. Dobljeno 22. 4. 2020 na spletni strani: http://www.ipri-zavod.si/ostalo/elektronsko-arhiviranje/

Koščak, D. (2011). Varovanje informacij v skladu s standardom ISO/IEC 27000. Diplomsko delo. Univerza v Ljubljani, Fakulteta za računalništvo in informatiko.

Ministrstvo za kulturo, Arhiv Republike Slovenije. (2020). Strategija in izvedbeni načrt razvoja slovenskega elektronskega arhiva 2016 – 2020. Dobljeno 24. 4. 2020 na spletni strani: https://www.gov.si/assets/organi-v-sestavi/Arhiv-RS/Projekt-e-ARH.si/PR-material/Strategija_e-ARH_si_2016-2020_1.0.pdf

Ministrstvo za kulturo, Arhiv Republike Slovenije. (2013). Enotne tehnološke zahteve, II. del. Ljubljana. Dobljeno 23. 4. 2020 na spletni strani: https://www.gov.si/assets/organi-v-sestavi/Arhiv-RS/Zakonodaja-2019/Enotne-tehnoloske-zahteve-2.1/0a8f-8dc882/Arhiv-RS_ETZ_-_2.1_II.-del.pdf

Ministrstvo za kulturo, Arhiv Republike Slovenije. (2020). Enotne tehnološke zahteve. Dobljeno 20. 4. 2020 na spletni strani: https://www.gov.si/zbirke/storitve/enotne-tehnoloske-zahteve-v-2-1-2013/

Pravilnik o enotnih tehnoloških zahtevah za zajem in hrambo gradiva v digitalni obliki, Uradni list RS, št. 118/2020.

Pravilnik o postopkih in ukrepih za zavarovanje osebnih podatkov, št. 020-5/2010/48.

Uredba o varstvu dokumentarnega in arhivskega gradiva (UVDAG). Uradni list RS, 86/2006.

Uredba o upravnem poslovanju (UUP). Uradni list RS, št. 20/2005, 106/2005, 30/2006, 86/2006, 32/2007, 63/2007, 115/2007, 31/2008, 35/2009).

Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje. Uradni list RS, št. 77/2000, 86/2006.

Zakon o varstvu osebnih podatkov (ZVOP-1). Uradni list RS, št. 94/07.

Zakon o tajnih podatkih (ZTP). Uradni list RS, št. 50/06 – uradno prečiščeno besedilo, 9/10, 60/11 in 8/20.

Zakon o državni statistiki za statistično tajnost (ZDSta). Uradni list RS, št. 45/95 in 9/01.

Zakon o maturi (ZMat). Uradni list RS, št. 1/07 in 46/16.

Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih (ZVDAGA). Uradni list RS, št. 30/06 in 24/14.

Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP). Uradni list RS, št. 57/2000, 61/2006.

Žvanut, P. (2011). Ocenjevanje tveganj v informacijskih sistemih na osnovi teorije omrežij. Diplomsko delo. Univerza v Ljubljani, Fakulteta za računalništvo in informatiko.

Typology: 1.04 Professional Article