m. sc. Milan Selan
media.doc

Ocena tveganj pri zagotavljanju avtentičnosti arhivskega gradiva v tradicionalnih in elektronskih arhivih

Izvleček:
Življenjski cikel dokumenta se ne razlikuje glede na nosilec, saj tako elektronski (e-), kot dokument na papirju, nastaja, se dopolnjuje in spreminja, dobi dokončno podobo, se ga razmnoži in avtorizira, razpošlje naslovnikom, izvirnik pa shrani, najprej v postopkovni, nato v tekoči in stalni zbirki. E-dokumenti omogočajo le večjo učinkovitost v vseh fazah življenjskega cikla – se pa v Javni upravi razlikuje zakonodaja, ki vpliva na obravnavo dokumentov na različnih nosilcih.

Medtem, ko se s papirnatimi dokumenti, do predaje v stalno zbirko organa, ukvarja predvsem Uredba o upravnem poslovanju (UUP), se z e-dokumenti in pretvorbo (digitalizacijo) v že zelo zgodnji fazi *ukvarja* Zakon o varstvu arhivskega in dokumentarnega gradiva in arhivih (ZVDAGA). Ne glede na pravno podlago, pa v procesu ravnanja z dokumenti nastajajo trenutki, ko lahko podvomimo v avtentičnost obravnavanega dokumenta. V članku avtor razmišlja o takih situacijah in kako jih z organizacijskimi in tehničnimi sredstvi kar se da učinkovito odpraviti.

Ključne besede:
Klasični arhivi, elektronski arhivi, dokumentarno in arhivsko gradivo (DAG), upravljanje tveganj, ocena tveganj, informacijski sistemi za upravljanje dokumentov (ISUD).

Abstract:
The Document Lifecycle does not, by any means, depend on media, as the electronic (e-) document, as well as the paper document are being created, upgraded and modified in the process of the shaping-up of the final version, copied and authorized, distributed to the addresses, while the original is being saved first in the working collection and then in the current and permanent collection. What should be pointed out is, that with the e-documents a higher level of efficiency in all the Lifecycle is guaranteed – taking into account that in the Public Administration the legislation, that has an impact on the document processing on different media, is different.

While the Decree on Administrative operations (DAO) is dealing with paper documents till their handing-over to the permanent collection, the e-documents and digitalization of paper documents, is a subject, in its very first phase, of the Protection of Documents and Archives and Archival Institution Act (PDAAIA). Notwithstanding the legislative basis, there are, however, moments/phases in the document processing, when a doubt could arise as to the authenticity of a certain document. The author's intention in elaborating this paper, is to reflect about such possible situations and to foresee the organizational and technical means with which to be able to overcome them in the best possible way.

Keywords:
Classic Archives, Electronic Archives, Documentary and Archive Documents (DAD), Risk Management, Risk Assessment, Electronic Document Management Systems (EDMS).

Uvod

Čeprav se bo zdel prispevek lahkotnejši (vsaj moj namen je bil tak), je tema, ki jo obravnava, še kako pomembna. Skrbnik določenega procesa, pa naj bo ta kakršenkoli, je odgovoren za sprotno analiziranje tveganj in njihov kvaren vpliv, ki ga imajo za delovanje procesa, pri predvidevanjih pa mora biti skrbnik nemalokrat tudi malo paranoičen. Dokaz za to je prirejanje sodnih spisov nekaj let nazaj in vsaj dva varnostna incidenta v bližnji preteklosti, ki sodita prav v kategorijo paranoičnega ocenjevanja tveganj, eden od teh je bilo brisanje (razmagnetenje) vseh varnostnih kopij celotnega informacijskega sistema (IS) na rezervni lokaciji, drugi pa v javnosti nemalokrat netočno predstavljena *afera* fotokopiranja arhivskih dokumentov, oba dogodka, ki sta se dogodila v Generalnemu sekretariatu vlade (GSV) v prvem Janševem mandatu, pa naj ne bi imela posledic na celovitost IS GSV in Vlade.

Za naļrtovanje varnega delovanja IS (dostopnost, celovitost in zagotavljanje javne vere dokumentarnega in arhivskega gradiva (DAG)) in seveda zagotavljanja javne vere DAG v ne-elektorski obliki, je bilo treba oba dogodka temeljito prouļiti in predlagati ustrezne ukrepe, ki bi odstraniti nevarnost za morebitno ponovitev. Ļe je skrbnik odgovoren za predvidevanje moģnih scenarijev in prelaganje ukrepov za prepreļevanje incidentov, pa se od vodstva priļakuje, da bo, glede na verjetnost, stroģke in velikost ģkode ob morebitnem udejanjenju incidenta, izbral in predlagal le smiselne ukrepe. Ļe v prvem primeru ni ģlo za ģkodovanje IS, ampak je naroļnik incidenta, glede na poznavanje delovanja varnostnega kopiranja, ģelel le izbris *pomotoma* varnostno kopirane brisane elektronske poģte (ko v okolju Lotus Notes iz svojega poģtnega predala briģeģ prejeto ali odposlano poģto, se ta izbriģe le iz pregleda (mehko brisanje ï *sotf delete*), dejansko pa ģele ļez nekaj ļasa, odvisno od sistemskih nastavitev ï kdo je (*seveda ni*) naroļil (ļe so v ***l**istilni akciji* sodelovali tedanji vodja sektorja za informatiko, vodja sluģbe za obrambne priprave in tajne dokumente in svetovalec za tuje obveģļevalne sluģbe, je nabor potencialnih nalogodajalcev zelo ozek) in kdaj, lahko hitro ugotovimo tudi zakaj, saj je dovolj, ļe pregledamo objave ļasopisja zadnjih tednov pred incidentom), pa je drugi incident kompleksnejši.

Da povzamem na kratko: po zamenjavi oblasti in po tem, ko je nov sekretar vrnil arhivarska pooblastila vodji arhiva, ki so mu bila odvzeta (skupaj s kljuļi do prostorov z DAG), so v arhivu odkrili fotokopirni stroj z zabeleģenimi preko 30.000 fotokopiranji. Ugotovljeno je bilo, da je bila v arhiv pol leta prej postavljena nova fotokopirna naprava (da o tem, da fotokopirna naprava v arhivu nima kaj iskati, niti ne razpravljam, niti tega, da so po tem dnevu v arhivu delali izkljuļno ljudje brez ustreznega strokovnega arhivskega znanja), po ogledu servisne knjige pa je bilo ugotovljeno, da je bila polovica kopij opravljena ģe po volitvah, je Vlada glede na poroļilo o incidentu smatrala, da je ģlo za neupraviļeno odtujevanje informacij (glede na najdeno *reorganizirano* gradivo, urejeno po vsebini in zadevah, v personalne mape vidnejših politikov (ģlo naj bi za *ugotavljanje* t.i. privilegijev)), o tem pa so bili obveģļeni tudi ustrezni organi. Ker kriminalistiļna policija ni odkrila fotokopij (prav *pretirano* jih tudi ni iskala), se moramo vpraģati, kaj se je (hipotetiļno) v arhivu GSV pravzaprav dogajalo. Imam veļ razlag:

a) malo za ģalo: glede na to, da nam je servis zaraļunaval storitve servisiranja glede na opravljeno ģtevilo kopij, je nekdo *navil* ģtevec;

b) neupraviļena uporaba delovnih sredstev: ģtudentje, ki so v arhivu *uradno* urejali arhivsko gradivo iz Ministrstva za pravosodje, so imeli v kleti zasebni fotokopirni servis za kopiranje ģtudentskega gradiva, seminarskih in diplomskih nalog, itd;

c) neupraviļeno odtujevanje informacij: sum ni bil potrjen, za to se vpraģamo, ali je morda ģlo za:

d) diverzijo ï ponarejanje DAG.

Po mojem mnenju je sicer ģlo za kombinacijo druge in tretje moģnosti, ker pa je (vsaj tretjo) policija ovrgla, in ker smo bili priļe *kreativnosti* tedaj vladajoļe stranke (ponarejeni izvirniki v aferi Depala vas, sestavljanje izvirnika iz razliļnih dokumentov (primer Türk), lahko upraviļeno pomislimo tudi na ļetrto moģnost.

Precej let so se tiskani dokumenti podpisovali le na koncu, parafiranje vmesnih pa je ponovno uvedel ģele generalni sekretar v Pahorjevi vladi. Zamenjava vmesnih strani je mogoļa in teģko ugotovljiva. Problem se bo sicer pokazal ģele ob predaji arhivskega gradiva v Arhiv RS, in ļe se bosta Arhiv RS in GSV v interesu javnosti odloļila tako, bo treba preveriti pristnost vsake od okrog 500.000 strani z gradivom na mikrofilmu. Do konca mandata leta 2000 je GSV, ko je bil DAG ģe na papirju, sproti snemalo na mikrofilm (vzporedno na dva mikrofilma) celotno DAG. V praksi GSV uporablja staro gradivo le z mikrofilma, ļeprav se izvirno DAG ģe nahaja v arhivu GSV in tam ļaka na predajo v Arhiv RS.

Ļe gre v prvih dveh primerih zgolj za obiļajno kaznivo dejanje ali zgolj prekrģek, pa je v drugih dveh za odloļitev vodstva in sodi v kategorijo *paranoje* pri ugotavljanju tveganj.

Çivljenjski cikel dokumentarnega in arhivskega gradiva (DAG)

V ļlanku se ukvarjam le s problemi javne vere (zaupanja) v DAG, ne pa tudi s pomembnimi sestavinami upravljanja tveganj, dostopnostjo, zaupnostjo (neupraviļena seznanitev z vsebinami) in celovitostjo (uniļenje ali delno uniļenje DAG na papirju ali v e-obliki). S problemom potvarjanja vsebine se sreļujemo v celotnem ģivljenjskem ciklu dokumenta ne glede na vrsto nosilca, z uporabo novih tehnologij in nosilcev se menjajo le moģnosti in potencialni ponarejevalci ter naļin vplivanja na vsebino. V analizi moģnih incidentov je mnogo

takih, ki se v praksi (že) niso in verjetno se niti ne bodo zgodili (verjetnost dogodka je blizu nič), vseeno pa obstaja teoretična oziroma hipotetična nevarnost. Sicer pa, pri analizi tveganj pri zagotavljanju izvirnosti dokumenta ugotavljamo, da za DAG na papirju nevarnosti preživijo v organu ustvarjalca (OU) in s strani ljudi, ki izkazujejo upravičen dostop do DAG (*insider*), le pri elektronskih dokumentih obstaja nevarnost nepooblaščenega dostopa s poskusi uničenja ali potvarjanja vsebine od zunaj (*outsider*), s tem problemom pa se ukvarjamo v sklopu analize neupravičenega dostopa.

Do predaje DAG v Arhiv RS je za izvirnost/istovetnost odgovoren OU, po predaji v Arhiv pa arhiv, ki tudi ni imun na številne nevarnost, čeprav so te bolj v zvezi z celovitostjo (požari, poplave) kot z izvirnostjo.

Oblikovanje izvirnika DAG

Danes težko najdemo kakšno tveganje v fazi oblikovanja (*create*) novega dokumenta, saj ga podpisnik, če že ni avtor sam, dobo pregleda, korigira in podpiše popravljeno verzijo (upam tudi, da prebere tudi celo novo verzijo ☺ poznam sicer primer, ko je nekdo v zadnji verziji uradno *popravil* le vejico v pogodbi, v resnici pa je napravil že nekaj *tiskarskih* napak (npr.: ni odvezan plačila bančne garancije é → ni obvezen plačati bančno garancije é). Precejšnje tveganje se pojavi v primeru prevajanja izvirnika, saj podpisnik po navadi ni tako vešč v tujem jeziku, da bi povsem razumel vse podtone prevoda. V preteklosti se je v tej fazi potvarjanje dogajalo neukim podpisnikom, ki so pisanje zaupali pisarjem, dogajalo pa se tako neukim kmetom kot vladarjem, če verjamemo nekaterim filmom in knjigam.

Podvajanje DAG

O izvirniku dokumenta govorimo šele, ko da podpiše podpisnik, pa naj gre za podpis na papirju ali e-podpis. Dokler rokujemo le z enim dokumentom, in dokler je le ta še v rokah podpisnika, nas kaj hudega res ne more doleteti. Problemi se začno, ko rabimo več izvodov istega dokumenta. Problemi so se začeli že v času, ko so zapriseženi pisarji prepisovali dokumente in to še pred Plinijem st. in njegovo *Naturalis historia*. Sicer je le vic, ampak primeren za ponazoritev problema ☺ že pri prepisovanju biblije je prepisovalec napravil *tiskarsko* napako in namesto *celebrato* (slaviti) zapisal *celibato* (celibat) ☺ v cirilični verziji te napake niso naredili in popje slavijo in se hkrati veselo šenijo še naprej. V času klasičnih pisalnih strojev brez spomina (na take spet prisega ruska tajna služba), ko si v valj vstavil pet in več tankih listov papirja z indigom in natipkal dokument, je bilo vsaj naporno če še ne nemogoče, natipkati novo, lažno verzijo dokumenta, ki bi po videzu dajala vtis izvirnika. Zaznavna nevarnost se pojavi s pisalnimi stroji z dovolj spomina in pojavom oblikovanja besedil na računalniku ☺ izjemno lahko je iztiskati dve verziji dokumenta, ki se na videz ne razlikujeta. Se vam je kdaj zazdelo, da je vaš šef prebral vse izvode istega dokumenta? Pravi izvod gre naslovniku, potvorjen pa po postopku na koncu stalno/arhivsko zbirko DAG, ali obratno, odvisno od namena? Tveganje enostavno odpravimo tako, da podpisnik sam izpiše ustrezno število izvodov dokumenta in jih takoj tudi popiše, vse vmesne strani pa tudi parafira.

V elektronskem svetu (se pravi, ko dokument nastane v e-obliki, e-obliko pa ohranja cel življenjski cikel, vse do e-hrambe), se potencialni ponarejevalci selijo v sfero ljudi, ki v OU zagotavljajo informacijsko podporo ISUD, za potvarjanje vsebine pa se zahteva neprimerno več znanja, administratorskih pooblastil in tehnične spretnosti. ISUD mora zagotavljati, da se dokument, ki je označen kot dokončen, ne more več popravljati (seveda se ga da še vedno popraviti z določenimi sistemskimi (oblikovalskimi) pravicami, ki lahko *prelisičijo* ISUD), za elektronsko podpisan dokument (najbolje je kar podpisna kartica, ki podpis obravnava tridimenzionalno (pritisk kot globino), pa zagotoviti ustrezno preverjanje podpisa, oziroma ugotavljanje, da se dokument po podpisu ni spreminjal.

Ob upoštevanju nekaterih osnovnih zahtev informacijske varnostne politike (IVP; ravnanje z gesli (npr. podpisnik ne sme *posoditi* svojega gesla ali podpisne kartice), načela čiste mize (podpisnik se odjavi s sistema, če zapusti sobo, gesla so v primernih omarah in zaklenjena), načela dveh ključev (ločena administratorska pooblastila za sistemske in uporabniške programe) in zagotavljanje revizijske sledi, se možnost neopaznega potvarjanja dokument skrči na minimum.

Pomemben element preprečevanja potvarjanja dokumenta je prav program, ki beleži vse posege do določenega dokumenta ☺ kdo in kdaj je posameznik dostopal do dokumentov, kaj je pri tem počel (branje, spreminjanje, zamenjava, brisanje), od kje je dostopal (v lokalnem območju, oddajen dostop ☺ dovoljen ali piratski), koliko časa se je zadrževal na posameznem dokumentu itd., seveda pa je zbirka revizijskih sledi, nadzor in analiza v rokah ljudi, ki niso neposredno vezani na informacijsko podporo, npr. zaposleni v strokovnih službah, ki pripravljajo

izvirne dokumente, saj se za nadzor ne zahteva prav posebnega znanja s področja informacijske stroke. Zanimivo je analizirati dostope do *zanimivih* dokumentov pred seznanitvijo zaposlenih o nadzornem programu in po seznanitvi število *firbcev* zelo upade (to sicer ni namen tega programa)! O upravičenem in neupravičenem dostopu se ukvarja analiza tveganj s področja zaupnosti dokumentov, s tem v zvezi pa so povezani predvsem problemi odtekanja informacij (npr.: strojepiska na sodišču je posredovala kriminalni združbi o načrt tajnih prisluhov).

Razpošiljanje DAG

Če smo v prejšnji fazi zagotovili enakost vseh izvodov dokumenta na papirju, potem pri pošiljanju DAG, za OU, niso odkrite potencialne nevarnosti potvarjanja dokumenta. Ko OU zapečati kuverto in jo preda kurirju ali na pošto, se problemom neupravičenega posega v dokument na poti ukvarja prenosnik pošte, po prejemu pošte pa prejemnik. V elektronskem svetu mora biti informacijski sistem oblikovan tako, da je dokument odposlan vsem naslovnikom takoj, ko ga podpisnik elektronsko podpiše. Z analizo razlikovanja časov podpisa in odpreme na poštnem strežniku lahko ugotavljamo, če se je kakšen dokument v OU *valjal* predolgo, s tem pa potencialnemu ponarejevalcu, v OU, omogočil svoj namen. Dodatno varnost lahko zagotovimo tudi tako, da podpisan dokument izvozimo preko enosmerne podatkovne diode v poseben zaprt sistem, dostop do teh zbirk pa je pod posebnim režimom, zanj pa skrbijo ljudje, ki v OU ne nudijo redne IT podpore (načelo dveh ključev) ‒ seveda so pri obeh zbirkah, ob ustreznem ISUD (najmanj kar je, mora meti ustrezno akreditacijo Arhiva RS), pomembne le upraviteljske, sistemske in oblikovalske pravice. Dostop do dokumentov od zunaj ni mogoč, vendar po potrebi lahko vedno primerjamo dokumente v rednih zbirkah z dokumenti v varnostni coni. Analiza tveganj vdorov v sistem od zunaj sicer sodi že v področje zaupnosti dokumentov.

Hramba DAG v postopkovni ali tekoči zbirki dokumentov

Ob ustrezno deljenih pravicah, omenjenih v prejšnjem poglavju, neopazno potvarjanje elektronskih dokumentov ni več mogoče, ob vzpostavitvi varnostne zbirke (pri tem ne govorim o standardnih varnostnih kopijah ‒ dnevnih, tedenskih, trajnih, delnih ali celovitih ‒, in možnostjo restavriranja potvorjenih dokumentov), pa lahko trajno zagotovimo njihovo avtentičnost.

Pri dokumentih na papirju pa možnost potvarjanja dokumentov obstaja vseskozi. Dokumenti v postopkovni zbirki se nemalokrat *valjajo* v ovojih na mizi ali v nezaklenjenih omarah in predalih, do dokumentov lahko pridejo tudi zaposleni v OU, ki sicer do njih nimajo pravice, s tem pa se krog potencialnih ponarejevalcev širi. Parafirane vmesne strani in striktno upoštevanje načela prazne mize, pripomore k zmanjšanju nevarnosti, ne odpravi pa je v celoti, saj ima skrbnik zadeve (uslužbenec, ki ima zadevo v reševanju) pri sebi edini izvod izvirnega dokumenta v OU in teoretično z njim počne kar hoče, tudi potvarja ali *pomotoma* izgubi. Da se izognemo težavam oziroma skušnjavam, ne glede na to, da bo dokument končal v stalni zbirki ali v Arhivu RS v papirnati obliki, je treba dokumentu na papirju, takoj po podpisu, zagotoviti pravno veljavno kopijo, bodisi na mikrofilmu, bodisi v digitalizirani obliki, oboje pa urejeno z notranjimi pravili oziroma pravilnikom za ravnanje z DAG OU (npr.: postopki pri snemanju dokumentov na mikrofilm in zagotavljanje pravne veljavnosti posnetih dokumentov). Take kopije izvirnikov se hranijo v drugih prostorih kot izvirniki, dostop do kopij mora biti urejen s poslovnikom, dostopa do njih pa nimajo skrbniki/reševalci zadev. V primeru digitalizacije dokumentov je treba, pred vrnitvijo izvirnika skrbniku zadeve, ustrezno preveriti istovetnost digitaliziranega dokumenta in elektronsko verzijo ustrezno parafirati (e-podpisati, časovno žigosati). Podpisnik je praviloma ni oseba, ki digitalizira dokumente.

Hramba DAG v stalni zbirki (arhivu organa)

Če je vodstvo organa ocenilo, da v prejšnjih postopkih dokumentov na papirju ni treba presneti na mikrofilm (ali jim kako drugače zagotoviti njihovo verodostojnost), ker za potvarjanje ni ugotovljenih razlogov ali ne obstaja dovolj velika nevarnost, ali pa stroški ali organizacijski problemi presegajo morebitno nastalo škodo, pa je ob predaji DAG v stalno zbirko, predvsem iz razlogov tveganja izgube dokumentov (požar, poplava) ‒ o tem presodi analiza tveganj celovitosti DAG ‒, treba zagotoviti varnostno kopijo dokumentov, bodisi na papirju, bodisi na mikrofilmu ali v digitalizirani obliki. Poznani so primeri, kako so zgoreli pomembni dokumenti že v postopkovni in tekoči zbirki (*novoletno darilo* Direktorata za upravne notranje zadeve MNZ), ali kako sta vlaga in plesen uničila DAG OU že pred predajo v Arhiv RS.

Izkuđnje nas uļijo, da se tudi v arhivu OU postavljajo fotokopirni stroji in da se ustvarjajo kopije dokumentov, za katere pa ne vemo, kje se nahajajo. Za odpravo kakrđnihkoli dvomov se ob predaji gradiva iz tekoļe v stalno zbirko OU opravi prenos DAG na rezervne nosilce ï na papir (kopira), mikrofilm (mikrofilmanje) ali na elektronske nosilce masovnega spomina (digitalizacija). Kopije se, ne glede na nosilec dokumenta, shranijo na rezervni lokaciji, dostopa do jih pa nimajo ne usluđbenci glavne pisarne, ne arhiva OU.

Hramba arhivskega gradiva (AG) v Arhivu RS

Da nevarnosti pred izgubo DAG pređijo povsod in ne glede na nosilec, sem opozoril đe leta 2010 na posvetu IIAS v Trstu (Selan, 2010) in leto prej na posvetu Tehniļni in vsebinski problemi klasiļnega in elektronskega arhiviranja v Radencih (Selan, 2009), v tem ļlanku pa se bom omejil le na nevarnosti potvarjanja dokumentov v arhivih, pođari, potresi in poplave, diverzije in teroristiļni napadi pa me ne zanimajo.

Ļe nepravilno zlaganje kopij AG (afera TŤrk) ne sodi v kategorijo potvarjanja verodostojnih AG, pa v arhivu pređijo nevarnosti tako od zaposlenih kot od zunanjih (upraviļenih ali neupraviļenih) uporabnikov.

Poglejmo si le nekaj mođnih scenarijev potvarjanja AG na papirju:

a) arhivisti lahko pri delu v arhivskih prostorih kadarkoli zamenjajo izvirnik z *izvirnikom.*

b) arhivisti lahko pri vraļanju AG iz nearhivskih prostorov (npr. iz ļitalnice) vrnejo potvorjeno gradivo ali gradivo *zalođbijo* v napaļnem fondu;

c) zunanji uporabniki lahko pri uporabi gradiva izvirnike zamenja s potvorjenimi dokumenti.

Problem ređimo tako, da posamezni arhivisti ne vnađajo ali iznađajo AG v/iz arhivskih prostorov (razen pri prevzemu novega AG, kar pa se tako ali tako opravi *komisijsko*), niti ne vstopajo ali izstopajo s kakrđnim koli papirjem, nadzor nad tem pa izvaja ustrezna sluđba. Danes take kontrole (đe) ni. Dokumente, ki jih je treba tako ali drugaļe obdelati zunaj arhivskih prostorov (ļe ne gre ravno za kađna restavratorska dela), pa se digitalizira v arhivskih prostorih, zunaj njih pa se jih obdeluje le v digitalizirani obliki. Zunanji uporabniki nimajo veļ dostopa do AG na papirju, ampak le đe v digitalizirani obliki.

In elektronskega AG:

a) arhivisti praviloma nimajo upraviteljskih, sistemskih ali oblikovalskih pravic, imajo pa jih strokovna sluđba, ki nudi IT podporo Arhivu. Obstaja nevarnost zamenjave elektronskih ali digitaliziranih dokumentov (problem se v glavnem nanađa na elektronsko nepodpisane ali ne ļasovno đigosane dokumente), kljub temu, da program to onemogoļa;

b) vdor v sistem od zunaj in zamenjava elektronskih ali digitaliziranih dokumentov.

Ređitev problema je enostavna, izdela se uporabniđka kopija elektronskega AG (vsebinsko zaokrođeni deli se posebej ļasovno đigosajo ali kako drugaļe elektronsko overijo), in dajo na uporabo notranjim in zunanjim uporabnikom, do uporabniđke kopije pa imajo vse upraviteljske, sistemske ali oblikovalske pravice tudi informatiki, ki nudijo IT podporo Arhivu in redno preverjajo veljavnost zbirke (e-podpis, ļasovni đig). Elektronski izvirniki se hranijo kot celota, elektronsko podpisana ali ļasovno đigosana, na dveh ali veļ lokacijah (lahko tudi pri dveh ponudnikih storitev e-hrambe) in brez kakrđnega koli oddaljenega e-dostopa (npr. le iz ene delovne postaje na lokaciji sami, ļe gre za stređniđki sistem, oziroma le hramba elektronskih nosilcev masovnega spomina). Informatikom arhiva se prepreļi vstop v tako e-shrambo. Pri oceni tveganj je treba razmiđljati tudi o mehanskih vdorih in *vdorih* v shrambo, kot jo praksa đe pozna. Referenļna zbirka je vedno zbirka, do katere uporabniki nimajo neposrednega dostopa. Ob ugotovitvi, da je nekdo potvoril vsebino uporabniđke kopije, se uporabniđka kopija restavrira iz elektronskega izvirnika in ponovno đigosa oziroma e-podpiđe.

Konec

Veliko je nevarnosti, ki pređijo na avtentiļnosti DAG, nekaj jih je v tem ļlanku ugotovljenih, zanje so nakazane tudi ređitve za njihovo prepreļevanje. Analitik tveganj mora imeti bujno domiđljijo in v vsem po malem videti

tudi teorijo zarote, saj je od takrat, ko smo bili vsi dobri in na isti strani, preteklo ğe veliko vode pod Tromostovjem. Bistvo prispevka je, kako razmiġljati o tveganjih pri kakrġnem koli procesu, pri tem pa vedno imeti v mislih znameniti Murphyjev zakon: ***Ļe gre lahko kaj narobe, bo zagotovo tudi ġlo.***

Ne glede na zapisano v ļlanku, je treba vsako ugotovljenem tveganje temeljito analizirati. Pomembni vidiki vrednotenja tveganja so verjetnost udejanjenja tveganja (uresniļljivo/neuresniļljivo, pogostost), materialna (pri kakġni stanovanjski pogodbi npr. izguba lastniġtva) ali nematerialna (npr. izguba ugleda) ġkoda, ter stroġki za zmanjġanje verjetnosti do ġe sprejemljive vrednosti verjetnosti.

Literatura in viri

Selan M. (2009): Zahteve in varnostna izhodiġġa klasiļnega in elektronskega arhiviranja, Posvetovanje Tehniļni in vsebinski problemi klasiļnega in elektronskega arhiviranja, Radenci: Pokrajinski arhiv Maribor;

Selan M. (2010): Arhivska zakonodaja z vidika zahteve po varnosti: klasiļni arhiv proti elektronskemu, Atlanti, revija za sodobno arhivsko teorijo in prakso, Trst: Mednarodni institut arhivskih znanosti Trst in Maribor;

Uredba o upravnem poslovanju

Uredba o varstvu dokumentarnega in arhivskega gradiva

Uredba o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih

Zakon o elektronskem podpisu in elektronskem poslovanju

Zakon o tajnih podatki

Zakon o varstvu dokumentarnega in arhivskega gradiva in arhivih,

Summary:

There are many dangers that lurk on the authenticity of the Documentary and Archive Documents (DAD), to a few are found in this article, and solutions to prevent them are indicated. Risk Analyst must have a vivid imagination and a little bit to see around a theory of conspiracy, because from the time we were all good and on the same side, a lot of water has passed under the *Triple Bridge*. The essence of this paper is how to think about the risks involved in any process, while always bear in mind the famous Murphy's Law: *If something can go wrong, it will certainly go.*

Notwithstanding stated in the article, each of the risks identified, should be thoroughly analyzed. Important aspects of risk assessment are the realization of the risk (realistic/unrealistic, frequency), materialistic (for example, loss of ownership of the house) or unmaterialistic (eg, loss of reputation) damage and the cost of reducing the risk probability to have an acceptable level.

O avtorju:

Milan Selan, magister informacijskih znanosti, se z informatiko ukvarja vse od leta 1972. Zadnjih deset let pred upokojitvijo je bi zaposlen Sektorju za informatiko v Generalnemu sekretariatu vlade (kot vodja sektorja v ļasu ne-Janġeve vlade) in odgovoren za informacijski sistem vlade, oblikovanje elektronskih arhivov v skladu z ZVDAGA in ETZ, informacijski sistem za podporo odloļanju o zakonodajnih in drugih aktih Sveta EU in za vzpostavitev sistema za ravnanje z elektronskimi tajnimi dokumenti v skladu z uredbo InfoSec.

About Author:

Milan Selan, m. sc. of Information Science, deals with informatics since 1972. Before his retirement, he was for ten years employed in the Informatics Department of the General Secretariat of the Government (as a Head of Department in non-Janġa Government time) and responsible for the governmental information system, creation of electronic archives in accordance with PDAAIA and UTR, for the information system to support decisions on legislative and other acts of the EU and for establishing a system for handling classified electronic documents in accordance with the regulation of InfoSec.