1.08 Objavljen znanstveni prispevek na konferenci
1.08 Published Scientific Conference Contribution

Sanja ANDROIĆ, Boštjan ŠPEHONJA***

POSLEDICE PREMALO SKRBNEGA RAVNANJA Z ELEKTRONSKIM IN PAPIRNIM GRADIVOM

Izvleček:

Ustrezno in dovolj skrbno ravnanje z elektronskim in papirnim dokumentarnim in arhivskim gradivom je bistvenega pomena za poslovanja posamezne organizacije ali pa ima veliko osebno vrednost v primeru fizičnih oseb. Kadar gre za arhivsko gradivo, ki ima trajen pomen za znanost in kulturo in obstaja zgolj v enem izvodu, je le-to še veliko bolj pomembno. Z raziskovanjem in predstavitvijo teoretičnih izhodišč, ponazorjenih tudi s pomočjo primerov iz prakse, bodo prikazane možne posledice premalo skrbnega ravnanja z elektronskim in papirnim dokumentarnim in arhivskim gradivom. Avtorja želita prikazati predvsem možnosti poškodb, sprememb in celo izgub gradiva v elektronski ali papirni obliki. Dotakneta se tudi metod, ki bi jih lahko zlonamerni heker izkoristil za nepooblaščeni dostop in morebitni poseg v elektronsko gradivo.

Ključne besede:

elektronsko gradivo, papirno gradivo, poškodbe gradiva, spremembe gradiva, nepooblaščen dostop

Abstract:

Electronic and Paper Records - Consequences of Negligent Handling

Proper and attentive handling of electronic and paper archives and records is of significant importance to all trading organisations. Likewise, it represents a great personal value in case of a natural person. The significance of attentive handling is even greater regarding archival documents, which have a long-lasting value for science and culture and only exist in a single copy. In the paper, we will portray the consequences of careless handling of electronic and paper records and archives, based on a thorough theoretical and practical research. Principally, we wish to present the damage, changes and even loss of electronic or paper documents. We will also touch upon different methods, which could be exploited by a malicious hacker to illegally gain access and interfere with electronic materials.

Key words:

electronic materials, paper materials, damage of materials, changes of materials, illegally gain access

1 UVOD

Ustrezno in dovolj skrbno ravnanje z elektronskim in papirnim dokumentarnim in arhivskim gradivom je bistvenega pomena za poslovanja posamezne organizacije. Le-to je še toliko bolj pomembno pri arhivskem gradivu, ki ima trajen pomen za znanost in kulturo ter obstaja večinoma zgolj v enem izvodu. Lahko ima tudi veliko osebno vrednost, če je ustvarjalec gradiva fizična oseba.

V raziskavi bomo najprej predstavili teoretična izhodišča glede ravnanja z dokumentarnim in arhivskim gradivom v elektronski in papirni obliki z metodo deskripcije, za to bomo uporabili sekundarne podatke iz strokovne literature. Obenem

* *Sanja Androić, vodja sprejemne pisarne, Mariborski vodovod, javno podjetje, d. d., Jadranska cesta 24, 2000 Maribor, Slovenija, kontakt: sanja.androic@mb-vodovod.si.*

** *Boštjan Špehonja, etični hacker, Nova Gorica, Slovenija, kontakt: bostjan.spehonja@gmail.com.*

bomo na podlagi izkušenj iz prakse prikazali možne posledice premalo skrbnega ravnanja z elektronskim in papirnim dokumentarnim in arhivskim gradivom. Prikazati želimo predvsem možnosti poškodb, sprememb in celo izgub gradiva v elektronski ali papirni obliki. Opisali bomo tudi nekaj najpogostejših metod socialnega inženiringa, ki bi jih zlonamerni heker lahko izkoristil za nepooblaščeni dostop in morebitni poseg v elektronsko gradivo.

Z raziskavo želimo prikazati, kakšne so možnosti poškodb, sprememb ali celo izgub gradiva elektronski in papirni obliki, predvsem pa opozoriti na vrste nevarnosti. Z raziskavo teoretičnih izhodišč, ki jih bomo povezali z izkušnjami iz prakse, bomo naredili nekakšen povzetek zakonskih zahtev in priporočil iz prakse za ustrezno ravnanje z dokumentarnim in arhivskim gradivom v elektronski in papirni obliki.

2 ZAKONSKE ZAHTEVE GLEDE RAVNANJA Z GRADIVOM V ELEKTRONSKI IN PAPIRNI OBLIKI

23. člen Zakona o varstvu dokumentarnega in arhivskega gradiva ter arhivih (2014, v nadaljevanju ZVDAGA-A) predpisuje glede varovanja dokumentarnega in arhivskega gradiva naslednje:

»(1) Dokumentarno gradivo se hrani v ustreznih prostorih in opremi, v ustreznih klimatskih pogojih, zavarovano pred vlomom, požarom, vodo, biološkimi, kemičnimi, fizikalnimi in drugimi škodljivimi vplivi, ter zagotavlja dostopnost, kar pomeni varovanje pred izgubo in stalno zagotavljanje dostopa zgolj pooblaščenim uporabnikom ves čas trajanja hrambe, in celovitost, kar obsega nespremenljivost in neokrnjenost ter urejenost tega gradiva.

(2) Vlada Republike Slovenije predpiše podrobnejše pogoje hrambe dokumentarnega gradiva.«

Glede hrambe arhivskega gradiva pa ZVDAGA-A v 36. členu določa naslednje:

»(1) Javno arhivsko gradivo ne glede na obliko ali nosilec zapisa prevzemajo v hrambo izključno pristojni arhivi, razen če ta zakon ne določa drugače.

(2) Arhivsko gradivo v fizični obliki se trajno in strokovno neoporečno hrani v ustreznih prostorih in opremi, v ustreznih klimatskih pogojih, zavarovano pred vlomom, požarom, vodo, biološkimi, kemičnimi, fizikalnimi in drugimi škodljivimi vplivi (materialno varstvo).

(3) Hramba arhivskega gradiva v digitalni obliki je dovoljena samo kot dolgoročna hramba zajetega gradiva v skladu z notranjimi pravili.

(4) Vlada Republike Slovenije predpiše podrobnejše pogoje hrambe arhivskega gradiva.«

26. člen Zakona o varstvu dokumentarnega in arhivskega gradiva ter arhivih (2014) predpisuje glede hrambe dokumentarnega gradiva v digitalni obliki naslednje:

»Varna hramba izvirnega dokumentarnega gradiva v digitalni obliki mora ves čas trajanja hrambe omogočati:

- *dostopnost izvirnega gradiva, kar pomeni varovanje pred izgubo in stalno zagotavljanje dostopa zgolj pooblaščenim uporabnikom ves čas trajanja hrambe;*

- *uporabnost, kar pomeni zmožnost reprodukcije in primernost reprodukcije za uporabo ves čas trajanja hrambe;*
- *celovitost, kar obsega nespremenljivost in neokrnjenost reprodukcije vsebine glede na vsebino izvirnega gradiva.«*

Glede hrambe zajetega dokumentarnega gradiva v digitalni obliki pa 27. člen ZVDAGA-A) predpisuje naslednje:

»Varna hramba zajetega dokumentarnega gradiva v digitalni obliki mora ves čas trajanja hrambe omogočati reprodukcijo vsebine izvirnega dokumentarnega gradiva, ki izpolnjuje naslednje pogoje v enaki meri, kot bi jih to izvirno gradivo:

- *dostopnost, kar pomeni varovanje pred izgubo in stalno zagotavljanje dostopa zgolj pooblaščenim uporabnikom ves čas trajanja hrambe;*
- *uporabnost, kar pomeni zmožnost reprodukcije in primernost reprodukcije za uporabo ves čas trajanja hrambe;*
- *avtentičnost, kar pomeni dokazljivost povezanosti reproducirane vsebine z vsebino izvirnega gradiva oziroma izvorom tega gradiva;*
- *celovitost, kar obsega nespremenljivost in neokrnjenost ter urejenost reprodukcije vsebine glede na vsebino izvirnega gradiva.«*

Seveda pa lahko področna zakonodaja predpisuje tudi strožje pogoje hrambe in varovanja gradiva.

Dokumentarno in arhivsko gradivo je potrebno varovati pred poškodbami, uničenjem, izgubo ali pred nedovoljeno uporabo oziroma posegom. V nadaljevanju se bomo omejili na materialno varstvo stalnih zbirk, ki jih hranimo v arhivskih skladiščih. Vendar bi te pogoje in ukrepe morali že delno upoštevati tudi pri tekočih zbirkah gradiva, ki se hranijo v pisarnah in drugih poslovnih prostorih. Zakonodaja določa javnopravnim osebam, da morajo le-te skrbeti za ohranitev in materialno varnost dokumentarnega gradiva, dokler ni iz tega gradiva odbrano arhivsko gradivo. Zavezanost za strokovno neoporečno hrambo pa še naprej velja za dokumentarno gradivo, ki se hrani trajno. Glede tega se morajo javnopravne držati osebe strokovnih navodil pristojnega arhiva. Potrebno je opozoriti, da je dolžnost glede strokovno neoporečnega varovanja dokumentarnega in arhivskega gradiva zakonska obveza javnih in zasebnih ustanov ter posameznikov, saj je morebitno poškodovanje ali uničenje gradiva po kazenski zakonodaji kaznivo dejanje (Žumer, 2001, str. 267).

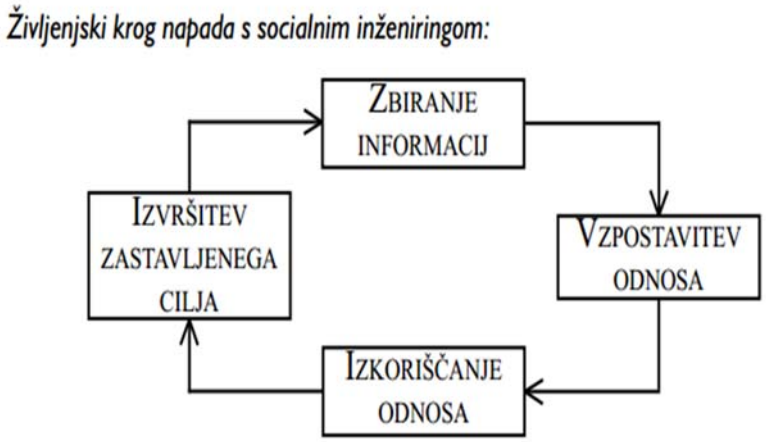
3 RAVNANJE Z ELEKTRONSKIM GRADIVOM

Živimo v dobi, ko nas na vsakem koraku spremlja informacijska tehnologija. Ta se nezadržno razvija, proizvajalci izdelkov informacijske tehnologije pa nas skoraj vsak dan presenetijo s kakšno novostjo. Na korak s časom se pripravlja tudi področje elektronskega arhiviranja, vendar je potrebno biti pri tem prehodu pazljiv. Pomisliti je potrebno tudi na vse več ranljivosti med informacijskimi tehnologijami in se vprašati, ali so sistemi dovolj varni, da se zlonamerni napadalec oziroma heker ne bi prikopal do nepooblaščenih podatkov in dokumentov ter jih poškodoval ali celo za vedno izbrisal oziroma uničil. To bi seveda naredilo nepopravljivo škodo. Spekter varnosti elektronskega arhiviranja dokumentarnega in arhivskega gradiva se začne že pri ustvarjalcu gradiva. Zlasti če gre za arhivsko gradivo v elektronski obliki, ki bo tako tudi predano pristojnemu arhivu po elektronski poti. Potrebno je razčleniti, po

kakšnem protokolu se bo gradivo pošiljalo, ali je le-ta varen pred prisluškovanjem napadalcev, kaj se zgodi, če na poti izgubi USB ali mikrofilm s pomembnimi podatki, ter kako je varovano gradivo v samem arhivu. Pri vseh korakih pa je izredno pomemben človeški vir, saj se večina napadov na informacijske sisteme zgodi ravno zaradi napak zaposlenih, s tako imenovano tehniko socialnega inženiringa, katere nekaj metod bomo predstavili v nadaljevanju.

3.1 Socialni inženiring

Socialni inženiring je tehnika napada, s katerim se manipulira zaposlene z namenom pridobivanja informacij podjetja. Po podatkih, objavljenih na spletu, bi naj bilo kar 66 % vseh vdorov povezanih s človeško napako. Zato je potrebno zaposlene izobraževati o računalniški varnosti (Social-Engineer.Org., b. l.). Vsak napad s socialnim inženiringom je lahko opisan v štirih stopnjah.



Slika 1: Življenjski krog napada s socialnim inženiringom (Informacijski pooblaščenec, 2009)

V kolikor bi se odločili uporabiti socialni inženiring nad katerim od arhivov, bi v prvem koraku po spletu in ostalih imenikih iskali vse podatke o arhivu. Predvsem imena in priimke zaposlenih, elektronske naslove, aktivnosti podjetja in tudi arhitekturo informacijskega sistema. V drugi fazi bi se odločili, kako bi stopili v kontakt z osebo, zaposleno v arhivu. Slednjo bi lahko poklicali po telefonu, ji poslali elektronsko pošto ali se osebno sprehodili do arhiva. V tej fazi moramo biti za dosego cilja čim bolj prepričljivi in dobro odigrati svojo vlogo, da si pridobimo zaupanje zaposlenega. V tretji fazi, ko imamo določen odnos z zaposlenim, sledi faza izkoriščanja. V tej fazi poizkušamo pridobiti čim več podatkov o arhivu, ki smo si jih predhodno zadali in ki nam primanjkujejo za uspešno izvedbo napada. V zadnjem koraku pa napadalec izkoristi pridobljene podatke in uspešno izvede napad. Na tak način zaobidemo vso elektronsko varnostno politiko in uspešno zaobidemo kakršen koli požarni zid ali antivirusni program.

3.1.1 Najpogostejše vrste socialnega inženiringa

3.1.1.1 Pridobivanje informacij po telefonu

V tem primeru napadalec vzpostavi kontakt z uslužbencem podjetja in se želi skozi telefonski pogovor prikopati do uporabnih podatkov podjetja. Lahko se predstavlja kot nadrejena oseba, kot oseba za tehnično pomoč, kot študent, ki izpolnjuje anketo za diplomsko nalogo, itd. Rezultati raziskave iz leta 2014 kažejo, da je 90 % ljudi posredovalo svoje ime ter elektronsko pošto, brez da bi poznali identiteto sogovornika (Social-Engineer. Org., 2014). S tem podatkom pa napadalec lahko pridobi uporabniško ime zaposlenega ter elektronsko pošto, ki jo uporabi v nadaljnjem napadu.

3.1.1.2 Pošiljanje elektronske pošte

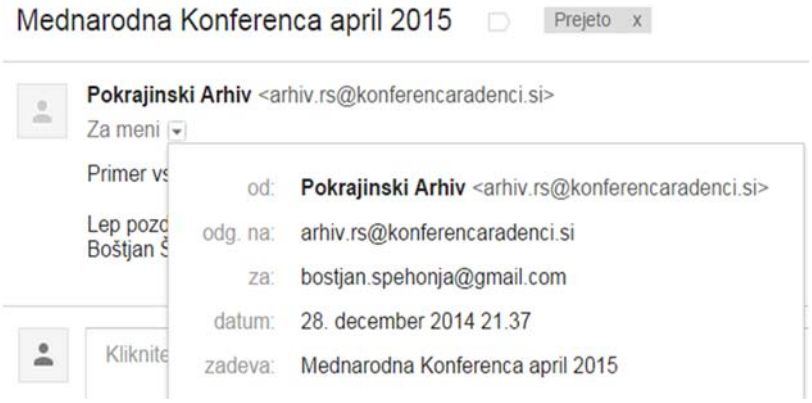
Vsako leto se odpošlje 107 trilijonov sporočil, kar pomeni 294 bilijonov sporočil na dan. 90 % vseh je tako imenovana vsiljena pošta (Social-Engineer.Org., 2014). To je pošta z reklamno vsebino, na katero se nismo naročili. V veliko primerih pa zahtevajo v sporočilih od nas tudi vpis osebnih podatkov. Najnevarnejšo plat teh sporočil predstavljajo povezave v sporočilu ter priponke. Če uporabnik ne posodablja operacijskega sistema ter spletnih brskalnikov, lahko pride do okužbe samo prek brskanja po okuženih spletnih straneh. Včasih je veljalo, da se okužimo, če brskamo po manj znanih straneh z neprimerno vsebino. Danes temu ni tako, saj je lahko okužena vsaka stran, ki nima pravilnega vzdrževanja in posodobitev. Tako napadalci izkoristijo varnostne pomanjkljivosti na spletni strani in na njo namestijo zlonamerno kodo brez naše vednosti. V vsiljeni pošti so velikokrat tudi povezave, ki nam ob kliku na njo odprejo okuženo spletno stran. Iz izkušenj lahko potrdimo, da se za uspešno izvedbo napada največkrat pošiljajo elektronska sporočila s priponko. V teh primerih gre velikokrat za okužene datoteke. Če tako priponko od neznanega avtorja z neznano vsebino odpremo in celo kaj namestimo, smo najverjetneje postali okuženi in naš informacijski sistem obvladuje napadalec. Pri tovrstnih napadih je cilj napadalca različen. Lahko uporablja vaš informacijski sistem za nadaljnje zlonamerne aktivnosti po internetu, lahko pa si na svoj strežnik pošilja podatke o vašem sistemu, vključno s krajo bančnih podatkov, zbira vaša uporabniška imena ter gesla in krade podatke, do katerih nima pooblastil.

Posebna vrsta napadov preko elektronske pošte je tudi ribarjenje. Pri tem napadalec postavi svojo lažno spletno stran, ki je po vsebini in videzu identična strani določene organizacije oziroma podjetja. Na spletni strani zahteva od nas prijavo z osebnimi podatki ter geslom, in na ta način posredujemo svoje podatke napadalcu. Iz prakse lahko potrdimo, da veliko ljudi uporablja isto geslo tako v službene kot zasebne namene, kar ni v skladu s primeri dobre prakse.

3.1.1.2.1 Tehnični problem elektronske pošte

Zaradi same arhitekture ter tehničnega delovanja SMTP-protokola, ki je odgovoren za prenos elektronske pošte, lahko kdorkoli pošlje sporočilo v imenu kogarkoli. Na vsak SMTP-strežnik se lahko povežemo s protokolom telnet, na vrata 25. V tem primeru lahko pošiljamo elektronsko pošto v sklopu domene. Strežniki, ki so pravilno varnostno konfigurirani, ne dopuščajo pošiljanja elektronske pošte na druge domene. Po drugi strani pa lahko preko svojega strežnika ali spletnih storitev pošiljamo elektronsko pošto v imenu kogarkoli, vendar je to vidno v izvorni kodi elektronskega sporočila. Če je zaznava vsiljene pošte pravilno konfigurirana, bi sistem moral zaznati,

da gre za prevaro. V nekaterih podjetjih smo celo opazili, da si zaposleni natisnejo elektronsko pošto in jo hranijo v registrih. Tak dokument je v praksi, sploh na sodišču, popolnoma brez vrednosti, saj jih je zelo enostavno ponarediti. Za dokaz potrebujemo originalno elektronsko pošto, ki je shranjena v našem elektronskem predalu, forenziki pa lahko v nekaterih primerih ugotovijo, ali gre za lažno elektronsko sporočilo.



Slika 2: Vsiljena pošta - lažno sporočilo

Slika 2 prikazuje primer vsiljene pošte, ki pa na prvi pogled ne izgleda tako. Iz enega od pokrajinskih arhivov smo dobili elektronsko pošto, ki bi lahko vsebovala tudi okuženo datoteko ali povezavo na okuženo spletno stran. Ko pogledamo izvorno kodo sporočila, pa ugotovimo, da je bila poslana s spletne strani, namenjene za pošiljanje lažne pošte, kar je razvidno iz slike 3. Kot že rečeno, veliko sistemov takšno pošto zazna in jo označi kot vsiljeno. Iz praktičnih primerov pa ugotovimo, da ta metoda še vedno predstavlja eno resnejših groženj.

```
Delivered-To: bostjan.spehonja@gmail.com
Received: by 10.107.30.144 with SMTP id e138csp2598367ioe;
        Sun, 28 Dec 2014 12:32:40 -0800 (PST)
X-Received: by 10.194.71.45 with SMTP id r13mr99722034wju.128.
        Sun, 28 Dec 2014 12:32:39 -0800 (PST)
Return-Path: <arhiv.rs@konferencaradenci.si>
Received: from emkei.cz ([2a01:5e0:36:5001::1e14:cf7b])
        by mx.google.com with ESMTP id uz6si64447676wjc.127.2(
        for <bostjan.spehonja@gmail.com>;
        Sun, 28 Dec 2014 12:32:39 -0800 (PST)
Received-SPF: none (google.com: arhiv.rs@konferencaradenci.si
Authentication-Results: mx.google.com;
       spf=none (google.com: arhiv.rs@konferencaradenci.si doe
Received: by emkei.cz (Postfix, from userid 33)
        id 7C28BD5586; Sun, 28 Dec 2014 21:37:45 +0100 (CET)
To: bostjan.spehonja@gmail.com
Subject: Mednarodna Konferenca april 2015
```

Slika 3: Izvorna koda lažnega sporočila

3.1.1.3 Anketiranje

Enak scenarij kot preko telefona se lahko zgodi tudi v živo. V podjetje pride oseba, ki se predstavlja kot tehnična pomoč, kot nemočen uporabnik ali kot nadrejena oseba in poizveduje po določenih informacijah. Poznamo tudi primere brskanja po smeteh, iz katerih lahko pridobimo uporabne informacije podjetja in zaposlenih.

Tu pridemo do točke, ko se vprašamo, kako osveščeni so uslužbenci v našem podjetju. Iz prakse lahko povemo, da za uporabnika ni dovolj, da se mu samo pove, na kaj mora biti pozoren, saj je računalniška varnost velikokrat nezanimiva tema. Pomembno je, da se zaposleni izobražujejo o informacijski varnosti in varni uporabi interneta, predvsem pa da se jim predstavi konkretne primere iz prakse, primere škode, ki lahko nastanejo zaradi človeške napake itd. Včasih se priporoča celo preverjanje zaposlenih, na koncu pa predstavitev rezultatov testiranja. Pošlje se jim sumljivo elektronsko pošto ali nastavi okužen USB-ključek. Ta podjetju prav tako predstavlja veliko grožnjo, saj se lahko na njem skriva okužena datoteka, ki jo žrtev odpre in s tem okuži informacijski sistem.

3.2 Prenos podatkov od uporabnika do gradiva

Za prenos podatkov iz posamezne organizacije do arhiva je možnih več poti. Prva pot je preko medijev (USB, zunanji disk, mikrofilmi …), to zahteva fizično pot. Pri tej poti obstaja nevarnost odtujitve ali izguba medija. Medij je potrebno ustrezno zavarovati in uporabiti naprave, ki so namenjene prenosu občutljivih podatkov. Prvi način je enkripcija oziroma šifriranje medija. To pomeni, da se podatki na ključku spremenijo v tako obliko, da nepooblaščena oseba iz njih ne more razbrati koristnih informacij. Še močnejša oblika zaščite pa je na napravah, ki imajo šifriranje vgrajeno v strojni opremi in kjer je potrebno za vklop medija poznati pravi pin. Po nekaj zaporednih napačnih pin-geslih se naprava ponastavi in avtomatsko izbriše vse podatke. To sta načina, ki omogočata, da kljub odtujitvi ali izgubi medija podatki niso vidni in jih ni mogoče prebrati. Nekoliko lažji, vendar nevarnejši način je pošiljanje podatkov preko internetnega omrežja. Tukaj lahko razdelimo grožnje v dve podskupini:

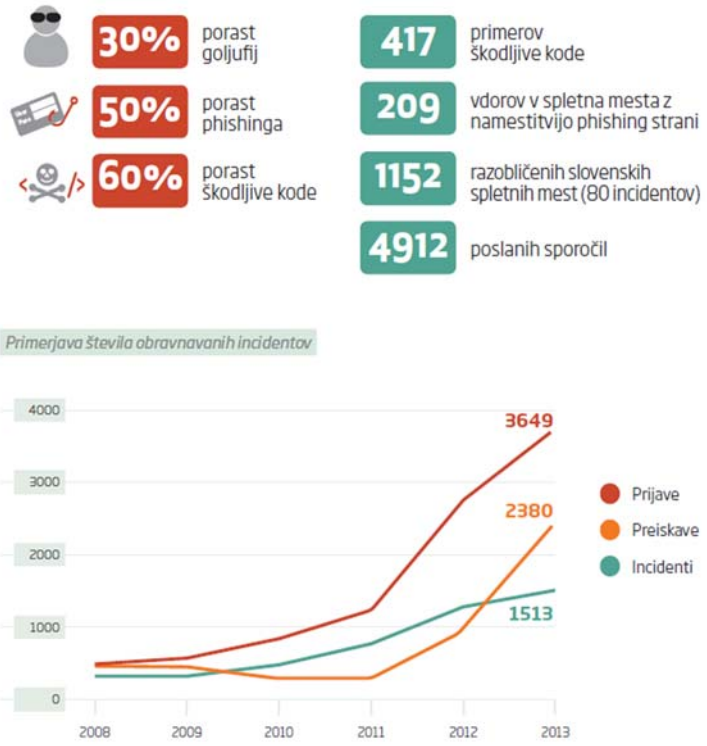
- grožnje v lokalnem omrežju (LAN),
- grožnje v prostranem omrežju (WAN).

3.2.1 Grožnje v prostranem omrežju (WAN)

»Prostrano omrežje, lahko tudi globalno omrežje WAN (wide area network) je omrežje računalnikov, ki se razprostira na velikih razdaljah. Nekatere povezave na prostranih omrežjih potekajo po telefonskih linijah ali celo preko satelitov. Prostrana omrežja pogosto povezujejo več lokalnih omrežij v eno samo.« (Pedagoška fakulteta Maribor, b. l.).

Napadov iz prostranega omrežja ni mogoče napovedovati. Lahko se zgodijo praktično kadarkoli. Vsaka odprta vrata na strežniku, ki so vidna navzven, omogočajo napadalcu morebitno zlorabo. Prav tako omogoča zlorabo neposodobljen operacijski sistem ali morebitne pozabljene administratorske datoteke na strežnikih, ki vsebujejo občutljive podatke podjetja. Zato je potrebno, da vsaka organizacija vsaj enkrat na leto opravi penetracijski test, navadno v sodelovanju z administratorji organizacije.

Ta zajema varnostni pregled strežnikov, javnih IP-naslovov, spletne strani, spletnih aplikacij, test propustnosti požarne pregrade, preizkus varnosti oddaljenih povezav, iskanje datotek ter dokumentov, ki naj ne bi bili javno dostopni, ter pregled ustrezno nastavljenih pravic na napravah. S takšnim pregledom se najbolj približamo resničnemu napadu, rezultat poročila pa je dokument, v katerem je podrobno opisan postopek izvedbe testa, dobljene ranljivosti, klasifikacija groženj posamezne ranljivosti ter mnenja in priporočila za odstranitev ranljivosti. Da je zgoraj opisani test več kot dobrodošel, prikazuje tudi naslednja slika.



Slika 4: Primerjava števila obravnavanih incidentov (SI-CERT, 2013)

Slika prikazuje porast števila incidentov, ki jih je obravnaval SI-CERT – Nacionalni odzivni center za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij. V primerjavi z letom 2012 je bilo za 30 % več goljufij, za 50 % več primerov ribarjenja ter 60 % več primerov škodljive kode.

Splet je živ, po njem se vsako minuto pretoči ogromna količina podatkov, med njimi je tudi zlonamerna vsebina. Po spletu neprestano krožijo programi, ki preiskujejo javne IP-naslove. Če tak program avtomatsko ugotovi, da vaš sistem ni posodobljen in da na njem obstaja varnostna ranljivost, jo avtomatsko izkoristi – s tem je vaš strežnik prevzel napadalec. Ta lahko uporabi strežnik za nadaljnje napade in vam s tem povzroči precej težav ali pa vam krade podatke iz notranjega omrežja, kot je opisano v naslednjem poglavju.

Iz večletnih izkušenj izvajanja penetracijskih testov ter preverjanja varnosti tako večjih kot manjših podjetij lahko zagotovimo, da je na spletu ogromno slabo vzdrževanih sistemov ter ranljivih spletnih strani/aplikacij, osveščenost o računalniški varnosti administratorjev ter uporabnikov pa še vedno precej premajhna.

3.2.2 Grožnje v lokalnem omrežju

»Lokalno omrežje (LAN) je osnovni gradnik vsakega računalniškega omrežja. Lokalno omrežje lahko sega od enostavnega (dva računalnika, ki sta povezana preko medija) do kompleksnega (na stotine povezanih računalnikov in perifernih enot). Značilnost lokalnih omrežij je v tem, da so to zasebna omrežja, ki se nahajajo znotraj neke stavbe ali območja na razdalji nekaj kilometrov. Običajno imajo enotno administracijo. V lokalnih omrežjih je tudi malo napak pri prenosu podatkov. Večinoma se uporabljajo za skupno rabo datotek in tiskalnikov. Pogosto pa tudi za skupno administracijo (domena), za zaščito pred zunanjim omrežjem, sporočanje.« (Breščak, b. l.).

Iz definicije lahko ugotovimo, da grožnjo pri odtujitvi podatkov v prvi vrsti predstavljajo zaposleni, ki imajo dostop do podatkov, pa tudi tisti zaposleni, ki na nelegalen način pridobijo dostop do nepooblaščenih podatkov. V tem primeru je vse odvisno od same konfiguracije omrežne opreme, konfiguracije strežnikov, zavedanja administratorjev o računalniški varnosti ter ozaveščenosti arhivarjev o varni uporabi interneta. V notranjem omrežju je zelo enostavno izvesti napade, s katerimi prisluškujemo prometu, ki se pretaka po mreži. Primer napada je MITM (man in the middle), ki se ga lahko izvede s tehniko zastrupljanja ARP-poizvedb. Na ta način prepričamo vse računalnike v omrežju, da smo mi naprava, s katero želijo ostali računalniki komunicirati, posledično se preusmeri celotni promet skozi naš - napadalčev računalnik. Prestrežene podatke lahko kopiramo, modificiramo ali blokiramo in s tem sami kontroliramo pretok podatkov v omrežju. V primeru uspešnega napada lahko pridobimo vsa nekriptirana gesla, uporabniška imena, seje uporabnikov in promet, ki ga uporabnik pošilja skozi internet. Na ta način lahko uporabniku ukrademo identiteto. Drugi način je, da postavimo svoj strežnik DNS (domenski strežnik), s katerim preusmerjamo zahtevke zaposlenih na druge spletne strani. Posebno pozornost je potrebno posvetiti tudi omrežnim napravam (usmerjevalniki, stikala, požarna pregrada), saj je varnost notranjega omrežja odvisna tudi od teh. Zato mora biti osveščenost administratorjev o računalniški varnosti na visoki ravni, sploh ker gre za upravljanje z visoko občutljivimi podatki. Potrebno je zagotoviti tudi dodatno varovalo, da se podatki iz arhivov ne bi nekontrolirano pretakali izven arhiva preko elektronske pošte, USB-ključkov, ftp-protokolov in ostalih metod. Za ta namen je potreben sistem, ki bi nadziral pretok podatkov iz arhiva ter vanj. Zgoraj opisane nevarnosti so možne v vsaki organizaciji, torej tudi v arhivih.

3.2.3 Tehnična izvedba

Naslednja težava, ki se lahko pojavi, je v sami tehnični izvedbi oziroma shranjevanju podatkov. Določene organizacije so razvile svoj datotečni sistem, v katerem shranjujejo podatke v formatu, kot ga določi proizvajalec datotečne storitve. Arhivi bi morali imeti univerzalni program, ki bi prepoznal datotečne sisteme vseh proizvajalcev. Če to ni mogoče, pa nekakšen vmesnik za pretvorbo podatkov v format, ki je uporabljen v elektronskih gradivih. Isto pretvorbo bi arhiv potreboval, če bi organizacija želela svoje podatke iz arhiva. V vsaki pretvorbi lahko pride do napak in s tem posledično celo do izgube podatkov.

4 RAVNANJE Z DOKUMENTARNIM IN ARHIVSKIM GRADIVOM V PAPIRNI OBLIKI

Skrb za ustrezno ravnanje z dokumentarnim in arhivskim gradivom se prične že pri ustvarjalcu gradiva, v primeru arhivskega gradiva pa se nadaljuje pri pristojnem arhivu. Ne glede na vse pogostejšo uporabo elektronskega poslovanja je še vseeno največ pomembne dokumentacije oziroma gradiva ustvarjenega in hranjenega v papirni obliki. Zakonodaja s področja varovanja dokumentarnega in arhivskega gradiva določa kar veliko zahtev glede ravnanja z gradivom, slednjih se bomo na kratko lotili v nadaljevanju.

4.1 Zakonske zahteve glede materialnega varstva gradiva

Uredba o varstvu dokumentarnega in arhivskega gradiva (2006) v 39. členu arhivom, javnopravnim osebam in imetnikom zasebnega arhivskega gradiva določa, da »morajo zagotavljati pogoje za materialno varstvo arhivskega in dokumentarnega gradiva, da se pri hrambi, urejanju, popisovanju, uporabi, prevozu in razstavljanju gradivo ne poškoduje, uniči ali kako drugače izgubi«.

Glede hrambe gradiva v skladiščih zakonodaja zahteva, da se gradivo, katerega obseg je več kot 30 tekočih metrov, hrani v arhivskih skladiščih s primerno opremo. Gradivo, ki ni v prej omenjenih skladiščih, se mora hraniti v kovinskih omarah, ki so zaklenjene in varne pred požarom in poplavami. Seveda je v prostorih, kjer se hrani gradivo, prepovedano kaditi, glede hrambe tajnih podatkov pa se uporablja zakonodaja o varovanju tajnih podatkov (Uredba o varstvu dokumentarnega in arhivskega gradiva, 2006, 41. člen).

44. člen Uredbe o varstvu dokumentarnega gradiva na podlagi druge alineje prvega odstavka 40. člena iste uredbe določa, da ukrepi za zavarovanje gradiva obsegajo predvsem:

1. *»vzdrževanje arhivskih skladišč in arhivske opreme,*
2. *izklapljanje električnega toka, kadar ni nikogar v skladiščih,*
3. *razkuževanje gradiva pred njegovim uskladiščenjem,*
4. *osušitev vlažnega gradiva pred prevzemom in preselitvijo,*
5. *vzdrževanje gradiva in prostorov v snažnem stanju,*
6. *razpraševanje vsega gradiva vsaj enkrat na leto,*
7. *stalno pregledovanje skladišč in gradiva ter odpravljanje okoliščin, ki bi lahko povzročile poškodbe gradiva,*
8. *redno prezračevanje arhivskih skladišč zato, da v njih ni škodljivih plinov,*
9. *zagotavljanje ustrezne temperature in vlage v arhivskih skladiščih,*
10. *obvezno stalno merjenje temperature in vlage ter vodenje evidence o temperaturi in zračni vlagi v vsakem arhivskem skladišču posebej.«*

Dokumentarno gradivo, ki se hrani trajno, in arhivsko gradivo je potrebno pripraviti za hrambo, kot sledi:

1. *»da se zravna oziroma zloži v format, primeren za skladiščenje,*
2. *da se ne obrezuje,*

3. *da se vloži v ustrezne arhivske škatle oziroma druge tehnične enote, ki se uporabljajo za opremo arhivskih enot in ne smejo biti nepredušno zaprte, preprečevati pa morajo vdor prahu,*
4. *da se gradivo velikih formatov polaga v kovinske predalnike in le izjemoma obeša,*
5. *da se ob urejanju odstranijo kovinski predmeti in folije (umetne snovi), ki nimajo dokumentarne vrednosti, vendar tako, da ostanejo vidne prvotne celote spisov,*
6. *da se arhivske škatle in druge tehnične enote postavljajo ali polagajo na police,*
7. *da gradivo, večje od formata A 3, leži na policah, in sicer vezano največ 3 enote druga nad drugo in nevezano največ do 5 cm,*
8. *da se zaščiti z opremo iz kemično obstojnih materialov.« (Uredba o varstvu dokumentarnega in arhivskega gradiva, 2006, 46. člen).*

4.2 Situacija v praksi

Če pogledamo izpolnjevanje zakonskih zahtev glede ravnanja z dokumentarnim in arhivskim gradivom v papirni obliki, lahko na podlagi naših dolgoletnih izkušenj iz prakse rečemo, da je situacija pri večini ustvarjalcev gradiv naslednja. Ustvarjalci gradiva svojih tekočih zbirk gradiva večinoma nimajo hranjenih v zaklenjenih kovinskih omarah, razen kakšnega bolj »delikatnega« gradiva, kot je npr. kadrovska dokumentacija in kakšne poslovne skrivnosti. Tekoče zbirke gradiva se večinoma nahajajo v omarah po pisarnah. V stalne zbirke se gradivo predaja enkrat na leto, ponavadi ob pričetku koledarskega leta ali takrat, ko zmanjka prostora v pisarni. Večina organizacij ima arhivsko skladišče v kletnih prostorih, ki žal ne zadostuje popolnoma vsem zakonskim določilom materialnega varstva gradiva. Pomembnosti primernega ravnanja z dokumentarnim in arhivskim gradivom se zaveda že večina ustvarjalcev gradiva, a še vedno nekateri premalo naredijo za to, predvsem na področju zagotavljanja primernih prostorov in ustrezne usposobljenosti zaposlenih, ki skrbijo za hrambo gradiva. Vse našteto je povezano tudi s finančnimi sredstvi, ki jih je nekako vedno premalo. Kljub velikemu zavedanju o pomembnosti ustreznega ravnanja z gradivom imajo pristojni arhivi težavo z zagotavljanjem zadostnih finančnih sredstev. Eden zadnjih odmevnih primerov je zaprtje arhivskega skladišča Pokrajinskega arhiva Maribor zaradi razširitve zdravju nevarne plesni na arhivskem gradivu zaradi neustreznih prostorskih pogojev. Posledice plesni na gradivu vidimo na spodnji sliki.

Slika 5: Plesen na arhivskem gradivu Pokrajinskega arhiva Maribor (MMC RTV SLO/STA, 2014)

Na podlagi dosedanjih izkušenj iz prakse lahko rečemo, da so najbolj pogoste poškodbe papirnega gradiva zaradi presuhih ali prevlažnih arhivskih skladišč. Pa tudi zaradi neprimerne hrambe. Za primer lahko damo npr. karte večjega formata, ki so zavite v rolo in niso hranjene v tulcu ali arhivskih omarah v predalih. Problem so tudi različne kakovosti papirja in črnil tiska, saj smo že videli tudi kakšno (k sreči) dokumentarno gradivo, s katerega je bilo oteženo branje vsebine ali se je celo ni več videlo. Velik problem so lahko tudi plastične mapice, v katerih se hrani gradivo, saj se lahko zgodi, da se pri hrambi v nekoliko toplejših in suhih prostorih črnilo in tudi del papirja zalepita na plastični del mapice. Pri suhih skladiščih se lahko prične gradivo zvijati, v prevlažnih skladiščih pa imamo lahko problem plesni ali celo mokrost papirnega gradiva. Velikokrat se zgodi, da se v neprimernih arhivskih skladiščih pojavijo glodavci, kot so npr. miši in podgane, ki lahko resno poškodujejo gradivo. V današnjih težkih časih pa je po našem mnenju tudi več ljudi, ki bi lahko videli kakšno korist ali bi zgolj želeli škodovati in bi se zato odločili za krajo ali uničenje kakšnega gradiva. Slednje pa bi se lahko zgodilo tudi zgolj zaradi nevednosti človeka ali zunanjih neugodnih vplivov.

Narodna in univerzitetna knjižnica je leta 2006 v okviru raziskovalnega projekta »PaperTreat« (6. okvirni program Evropske komisije) pregledala zbirko monografij NUK in ugotovila, da je bila večina knjig med letoma 1870 in 1990 natisnjenih na zelo neobstojnem papirju. Spremenjen postopek izdelave papirja po letu 1850 je razlog za slabšo obstojnost papirja iz tega obdobja, saj ima le-ta nizek pH, ki pospešuje njegovo razgradnjo. Ocenjena doba uporabnosti t. i. »kislega papirja« je samo sto let. Tako ogroženemu gradivu lahko podaljšamo njegovo življenjsko dobo »s hranjenjem pri nižji temperaturi ali s postopkom razkislinjenja, s katerim papirju dvignemo pH in posledično upočasnimo njegovo razgradnjo« (Malešič in Sešek, 2014, str. 6). Na spodnji sliki lahko vidimo gradivo, ki je že poškodovano in krhko zaradi kislinske razgradnje papirja.

Slika 6: Primer gradiva, ki je že krhko zaradi kislinske razgradnje papirja (Malešič in Sešek, 2014, str. 6)

Na naslednji sliki lahko vidimo poškodovano gradivo, ki je bilo hranjeno v izjemno vlažnih prostorih.

Slika 7: Poškodovanost Oklicne knjige župnije Rodik zaradi hrambe v izjemno vlažnih prostorih (Grkman, 2012)

Na sliki 8 pa lahko vidimo, kako so poškodovano Oklicno knjigo župnije Rodik z zgornje slike rešili s konzerviranjem in restavriranjem.

Slika 8: Konzervirana in restavrirana Oklicna knjiga župnije Rodik (Grkman, 2012)

Menimo, da je največji problem glede morebitnih poškodb dokumentarnega in arhivskega gradiva v papirni obliki predvsem neprimernost nekaterih arhivskih prostorov, premajhna kakovost papirja in črnil za dolgotrajno hrambo in včasih tudi premajhna usposobljenost oseb za ravnanje z gradivom. Kar se tiče sprememb gradiva so lahko razlogi enaki, a bi tukaj lahko dali kot glavni razlog zlonamernost človeka. Gradivo v papirni obliki se lahko izgubi zaradi požara, poplave, kraje ali uničenja s strani človeka itd.

5 ZAKLJUČEK

V prispevku smo prikazali zakonske zahteve glede ravnanja z dokumentarnim in arhivskim gradivom v elektronski in papirni obliki, ki smo jih povezali z izkušnjami iz prakse. Pri ravnanju z gradivom v elektronski obliki smo predstavili nekaj tehnik socialnega inženiringa, s katerimi bi lahko zlonamerni napadalec z manipulacijo zaposlenih ali drugih ranljivosti sistema nepooblaščeno dostopal do informacij, jih poškodoval, spremenil ali celo uničil dokumentarno ali arhivsko gradivo v elektronski obliki. Nekaj tehnik socialnega inženiringa bi se lahko uporabilo tudi za zlonamerne namene glede gradiva v papirni obliki. Predstavili smo tudi grožnje v prostranem ter lokalnem omrežju in tehnične težave, s katerimi se lahko srečamo v prihodnosti ob predaji arhivskega gradiva v elektronski obliki. Opisali smo tudi zahteve za materialno varstvo dokumentarnega in arhivskega gradiva v papirni obliki. Nevarnosti in poškodbe gradiva v papirni obliki smo predstavili s pomočjo svojih izkušenj iz prakse in prikazov nekaterih primerov.

Zakonodaja predpisuje, kako moramo ravnati z dokumentarnim in arhivskim gradivom, da bi le-to ostalo dostopno, uporabno, avtentično in celovito. Menimo, da so pri elektronskem gradivu največje nevarnosti zlonamerni posegi napadalcev. Slednji lahko pridobijo nepooblaščen dostop do arhivskega gradiva preko ranljivosti v strežniških sistemih zaradi slabega vzdrževanja, neposodobljenih strežnikov ali napak na ostalih aplikacijah, spletnih straneh itd. Na ta način je lahko nepooblaščeni osebi omogočen ne samo dostop do gradiva, temveč lahko ta oseba gradivo tudi uniči, poškoduje ali modificira, kar je v nasprotju z zakonodajo. Veliko grožnjo predstavljajo tudi zaposleni, saj je človek vedno bil in bo najšibkejši člen v sistemu varnosti. Seveda ne smemo pozabiti tehničnih omejitev elektronskih dokumentov, kot so formati zapisov, ki se nenehno spreminjajo, čemur se je potrebno prilagajati s pravočasnimi in ustreznimi pretvorbami formata zapisov. Ena od velikih nevarnosti so tudi prostrana in lokalna omrežja, ki se jih z vdori radi lotijo zlonamerni napadalci. Največja nevarnost današnje moderne tehnologije je internet. Pri elektronskem gradivu se pojavlja tudi vprašanje, kako bo potekala predaja arhivskega gradiva ustvarjalca gradiva pristojnemu arhivu. Največji problem bodo najverjetneje kanali oziroma elektronske poti, preko katerih bo potekala predaja. Obstaja tudi vprašanje povezljivosti različnih dokumentnih ali datotečnih sistemov ustvarjalcev gradiva z omenjenimi kanali oziroma elektronskimi potmi in s sistemom pristojnega arhiva. Pri papirnem gradivu so največja nevarnost premalo ustrezni prostorski pogoji hrambe gradiva in kvaliteta materialov. Velika nevarnost za gradivo v papirni in elektronski obliki so tudi zaposleni, ki so premalo strokovno usposobljeni za ustrezno ravnanje z gradivom.

Ocenjujemo, da je gradivo v papirni obliki največkrat poškodovano zaradi neustreznih prostorskih pogojev arhivskega skladišča. Gradivo se tako lahko poškoduje zaradi plesni, glodavcev, se prične zvijati zaradi toplote in suhosti prostorov itd. Veliko poškodb gradiva v papirni obliki nastane zaradi preslabe kvalitete papirja, ta povzroča kislinsko razgradnjo. Problem so lahko tudi požari, vdori vode itd. Za poškodbe,

spremembe ali celo uničenje gradiva je velikokrat lahko kriv tudi človek zaradi nezadovoljivega strokovnega znanja ali zlonamernih namenov.

Menimo, da se ustvarjalci gradiva in arhivi premalo zavedajo nevarnosti za nastanek poškodb, sprememb in celo izgub gradiva v papirni in še bolj elektronski obliki, saj vsi s preveliko hitrostjo hitimo v svet elektronskega poslovanja in hrambe. Velik problem vidimo v tem, da je za varno in ustrezno hrambo gradivo zagotavljenih premalo finančnih sredstev s strani organizacij kot ustvarjalcev gradiva in tudi s strani državnih organov, ki so pristojni za arhive. Drugi veliki problem je premajhno zavedanje o tem, da se mora z dokumentarnim in arhivskim gradivom ustrezno ravnati že od njegovega nastanka. To lahko pripišemo premajhni strokovni usposobljenosti večine zaposlenih pri ustvarjalcih gradiva, saj le-ti pošljejo na izobraževanje zgolj tisto osebo ali osebe, ki so zadolženi za arhiv organizacije. Predvsem pa se bodo vodstva organizacij in arhivov morala pričeti zavedati pomembnosti ustrezno izobraženih in motiviranih zaposlenih, saj je prav človek najšibkejši člen varnosti. Lahko imamo najsodobnejšo in najvarnejšo tehnično opremo, a nam ne bo prav nič pomagala pri zaščiti dokumentarnega in arhivskega gradiva, če bo človek še vedno možni šibki člen.

VIRI IN LITERATURA

- Breščak, B. (b. l.): *Lokalno omrežje*. Pridobljeno 18. 12. 2014 s spletne strani: http://www.s-sers.mb.edus.si/gradiva/rac/moduli/upravljanje_ik/21_lan/01_datoteka.html.
- Grkman, S. (2012): *Konserviranje in restavriranje Oklicne knjige župnije Rodik*. Ljubljana: Arhiv Republike Slovenije. Pridobljeno 20. 12. 2014 s spletne strani: http://www.arhiv.gov.si/nc/si/medijsko_sredisce/novica/article/1244/5540/.
- Informacijski pooblaščenec (2009): *Socialni inženiring in kako se pred njim ubraniti?* Pridobljeno 10. 12. 2014 s spletne strani: https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/socialni-inzeniring-in-kako-se-pred-njim-ubraniti.pdf.
- Malešič, J. in Sešek, I. (2014): Masovno razkislinjenje knjig: ohranjanje kulturne dediščine v Narodni in univerzitetni knjižnici. *Knjižničarske novice 24 (1/2)*, str. 6. Pridobljeno 20. 12. 2014 s spletne strani: http://www.nuk.uni-lj.si/knjiznicarskenovice/v2/podrobnostClanek.aspx?id=820. .
- MC RTV SLO/STA (2014): Pokrajinski arhiv Maribor zaradi plesni ostal brez skladišča. Pridobljeno 22. 12. 2014 s spletne strani: http://www.rtvslo.si/kultura/drugo/pokrajinski-arhiv-maribor-zaradi-plesni-ostal-brez-skladisca/335555.
- Pedagoška fakulteta (b. l.): Pridobljeno 10. 12. 2014 s spletne strani: http://splet-stari.fnm.uni-mb.si/pedagoska/didgradiva/nastopi/didrac2/00/2/racunalnisko_omrezje.htm.
- SI-CERT (2013): *Poročilo o omrežni varnosti za leto 2013*. Pridobljeno 18. 12. 2014 s spletne strani: https://www.cert.si/porocilo-o-omrezni-varnosti-za-leto-2013/.
- Social Engineer, Org. (2014): *The Social Engineering Infographic*. Pridobljeno 08. 12. 2014 s spletne strani: http://www.social-engineer.org/social-engineering/social-engineering-infographic/.
- Social Engineer, Inc. (b. l.): Pridobljeno 08. 12. 2014 s spletne strani: www.social-engineering.org.
- Uredba o varstvu dokumentarnega in arhivskega gradiva (2006). Uradni list RS, št. 86.
- Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih (2014). Uradni list RS, št. 51.
- Žumer, V. (2001): *Arhiviranje zapisov. Priročnik za ravnanje z dokumentarnim in arhivskim gradivom*. Ljubljana: GV založba.

SUMMARY

Sanja ANDROIĆ, Boštjan ŠPEHONJA***

ELECTRONIC AND PAPER RECORDS - CONSEQUENCES OF NEGLIGENT HANDLING

Based on practical experience and research, the authors demonstrate legal demands regarding handling electronic and paper records and archives. The authors displaye several social engineering techniques, which a malevolent attacker could use to damage, change or even destroy electronic records and archives. This illegal access to gain important information is often done either via employee manipulation or by abusing a vulnerable system. Furthermore, some of these social engineering methods could also be abused regarding paper documents. Additionally, the authors illustrate wide and local area network threats and what technical difficulties one may face in the future when transfering electronic archives. Demands for material protection of paper records and archives are also described. Hazards and damages concerning paper materials are presented with a few examples based on practical experiences.

Legislation defines how records and archives should be handled to remain accessible, useful, authentic and complete. The authors believe that the biggest threats to electronic records are wrongful intrusions. These attackers can gain unlawful access to archives by abusing a vulnerable server system due to poor maintenance, non updated servers or errors on web pages or applications. In this manner, an unauthorised person does not only have access to records, but can also destroy, damage or modify them, which contradicts legislation. Employees also represent a great risk, since people have and always will be the weakest link regarding security. Of course, we must not forget technical limits of electronic documents, such as different formats, which are constantly changing and as such we must adapt on time and with suitable format conversions. One of the biggest threats are also wide and local area networks, which are a common target of attackers. Naturally, the greatest danger in current modern technology is the internet. The question with electronic records is also how the archives of the creator will be transfered to the competent archive. The main difficulty will most likely be the channels or electronic paths, which will be used for the transfer. There is also a question of connectivity between various documents or file systems of the creator's documents with the stated channels or electronic paths and system of the competent archive. The greatest threats regarding paper documents are inadequate storage capacity and poor material quality. Furthermore, one of the hazards are also the employees that are not sufficiently trained to correctly handle the documents.

The authors estimate that the paper documents are mostly damaged due to inappropriate archival storage. Consequently, dcouments can be damaged due to mould, rodents, folding, due to high temperatures and dry environment, etc. A large amount of paper documents are damaged due to poor quality of the paper, which leads to acid decomposition. As hazards one can also mention fire, floods and other natural catastrophes. Some damages are also due to incorrect handling of documetns by no other than people and their lack of professional knowledge or even deliberate attempts to vandalize the material. The authors believe that creators of the records and archives

* *Sanja Androić, head of reception office, Mariborski vodovod, javno podjetje, d. d., Jadranska cesta 24, SI-2000 Maribor, Slovenia, contact: sanja.androic@mb-vodovod.si.*

** *Boštjan Špehonja, ethical hacker, Nova Gorica, Slovenia, contact: bostjan.spehonja@gmail.com.*

are often not aware of the damages, changes or even losses of the paper and even more so electronic documents that can occur, especially due to the great desire to rush into the world of electronic trading and storage. The biggest worry the authors see, is the lack of financial support from organisations, such as creators of documets and state institutions responsible for archives, for a safe and appropria storage of archives.

The second biggest problem is the lack of awareness that records and archives have to be appropriately handled since their creation. This can be attributed to inadequate professional qualifications of most people employed by creators of documents, which only send a selected few, who are responsible for archives, to attend educational conferences.

As mentioned, an unqualified person can be a great risk in this area, therefore organisations and their leaders will have to start paying attention to the importance of suitably educated and motivated employees. The latest technical equipment will have no protection over records and archives whatsoever, if a person still remains the weakest link due to inappropriate education and lack of knowledge.