OBČINA VODICE

Nadzorni odbor

Kopitarjev trg 1, 1217 Vodice
Tel.: 01/833 26 10
Fax.: 01/833 26 30

Datum: 22. 8. 2016

Na podlagi 9. člena Poslovnika Nadzornega odbora Občine Vodice (Uradno glasilo Občine Vodice, št. 10/2015) in v skladu s sprejetim Programom dela nadzornega odbora za leto 2015, št. 011-17/2014-005, z dne 16.03.2015 ter Sklepa o izvedbi nadzora Nadzornega odbora Občine Vodice, št. 900010-02/2015-001, izdanega dne 08.05.2015, kot pooblaščenec NO podajam

KONČNO POROČILO O OPRAVLJENEM NADZORU

»Nadzor varnosti in zanesljivosti informacijske tehnologije v Občini Vodice«

Pooblaščenec Nadzornega odbora:

Kot pooblaščenec Nadzornega odbora občine Vodice za izvršitev nadzora je bil s sklepom št. 90010-02/2015-001 z dne 08.05.2015 imenovan član Nadzornega odbora Občine Vodice:

- Tomaž Merše

Organ, v katerem je bil opravljen nadzor:

Občina Vodice, Kopitarjev trg 1, 1217 Vodice, odgovorna oseba župan Aco Franc Šuštar.

Predmet nadzora:

Na podlagi sklepa Nadzornega odbora Občine Vodice je bil opravljen nadzor varnosti in zanesljivosti informacijske tehnologije v Občini Vodice. Namen in cilj nadzora je bilo preveriti, ali Občina Vodice na področju uporabe IT tehnologije ravna v skladu s pravili dobre prakse in zakonodaje na področju informacijske varnosti in varovanja osebnih podatkov in vzdrževanja sistemov informacijske tehnologije.

Terminski okvir opravljanja nadzora:

Od septembra 2015 do maja 2016 z vmesnimi prekinitvami.

VSEBINA

1. UVOD

Nadzor varnosti in zanesljivosti informacijske tehnologije (v nadaljevanju IT) v Občini Vodice (v nadaljevanju: OV) je bil izveden na podlagi sklepa Nadzornega odbora OV, ki je bil določen z letnim programom dela Nadzornega odbora. Sklep o nadzoru je bil izdan 08.05.2015.

1.1. Predstavitev organa, ki je bil predmet nadzora

Nadzor je bil opravljen pri neposrednem proračunskem uporabniku OV, Kopitarjev trg 1, 1217 Vodice. OV samostojno opravlja lokalne zadeve javnega pomena, kot je določeno z akti občine in zakoni ter skrbi za gospodarski in družbeni razvoj na lokalni ravni.

Organi občine so:

- Župan
- Občinski svet
- Nadzorni odbor

S strani župana Aca Franca Šuštarja je bila določena odgovorna oseba g. Aleksander Gantar, ki je v postopku nadzora priskrbel in predstavil vse zahtevane podatke in informacije.

1.2. Obrazložitev nadzora

Delovanje občinske uprave je danes v veliki meri odvisno od sistemov informacijske tehnologije, kjer se obdelujejo in so shranjeni pomembni podatki in dokumenti občine ter tudi različni osebni podatki, za katere je tudi zakonsko zahtevano posebno varstvo. Zato je za varno in zanesljivo poslovanje občine pomembno, da pri uporabi sistemov IT sledi pravilom dobre prakse na področju zagotavljanja informacijske varnosti.

Informacijska varnost pomeni varstvo podatkov in informacijskih sistemov pred nezakonitim dostopom, uporabo, razkritjem, ločitvijo, spremembo ali uničenjem. S tem v zvezi se uporabljajo pojmi kot informacijska varnost, varovanje računalniških sistemov, varstvo informacij, ki se medsebojno prepletajo in si delijo skupne cilje varstva zaupnosti, neokrnjenosti in razpoložljivosti informacij.

Vrednost informacije izvira iz treh glavnih lastnosti ali kvalitet: zaupnost, neokrnjenost in razpoložljivost. Informacijski sistem je sestavljen iz treh glavnih delov: strojne opreme, programske opreme in standardov informacijsko varnostne industrije, ki se uporablja kot mehanizem zaščite in preprečitve na treh ravneh: fizičnem, osebnostnem in organizacijskem. Pravilna izvedba vseh treh področij lahko zagotavlja ustrezno raven informacijske varnosti znotraj organizacije.

V obravnavanem nadzoru smo se osredotočili na informacijsko varnost kot zaupnost, neokrnjenost in razpoložljivost podatkov v informacijskem sistemu Občine Vodice.

Poleg tega smo preverili ravnanje z osebnimi podatki pri uporabi sistemov IT v OV ter gospodarnost pri zagotavljanju storitev vzdrževanja sistemov IT v Občini Vodice.

Za dosego tega cilja je bilo izvedeno:

- Pregled dokumentacije o strojni opremi in arhitekturi sistemov IT v Občini Vodice.
- Pregled postopkov zagotavljanja varnostnih kopij strežniškega datotečnega sistema.
- Pregled zaščite sistema IT pred virusi in drugo zlonamernimi programi.
- Pregled nadzora dostopa do naprav, programov in podatkov, ki jih uslužbenci potrebujejo pri svojem delu in so zanje pristojni ter pooblaščeni.
- Pregled načina uporabe najpomembnejših programov programske opreme, ki se uporabljajo v občinski upravi.
- Pregled zagotavljanja sledljivosti sprememb podatkov in dokumentov v najpomembnejših programskih orodjih, ki jih uporablja občinska uprava.
- Pregled postopkov varovanja osebnih podatkov v elektronski obliki pri uporabi sistemov IT v Občini Vodice in pregled Pravilnika o zavarovanju osebnih podatkov, št. 104-24/2014-001, z dne 27. 11. 2014.
- Pregled postopkov upravljanja in vzdrževanja informacijskega sistema ter upravljanje sprememb v njem.

2. UGOTOVITVE

2.1. Strojna oprema in arhitektura sistema IT v Občini Vodice

Pregled seznama z opisom naprav v sistemu IT Občine Vodice pokaže, so izbrane ustrezne naprave primerne zmogljivosti za delo, ki se na njih opravlja. Izjema je le prenosni računalnik, za katerega nisem dobil informacije, kakšne naloge se na njem opravlja, da bi bila potrebna tako zmogljiva naprava, ki je primerna za zahtevne grafične ali video aplikacije ali igranje zahtevnejših računalniških iger, tako da ocenjujem, da bi bil za opravila občinske uprave lahko tudi manj zmogljiv in zato cenejši.

Interno računalniško omrežje OV ima standardno zasnovo:

- z usmerjevalnikom, ki skrbi za povezavo s svetovnim spletom, usmerjanje prometa po internem omrežju, ter požarno pregrado z blokiranimi zunanjimi dostopi, razen za elektronsko pošto.
- ethernet stikalom, ki povezuje vse ostale naprave v omrežju,
- Strežnikom, ki deluje kot tiskalniški, datotečni, poštni strežnik (Microsoft Exchange 2003), DHCP (angleško Dynamic Host Configuration Protocol) strežnik, interni DNS strežnik za mrežo (DNS je kratica za Domain Name System/Service/Server oziroma za sistem domenskih imen) in SQL strežnik (Structured Query Language ali strukturirani povpraševalni jezik) za delo s podatkovnimi bazami.

Konfiguracija omrežja omogoča ethernet TCP/IP protokol s privatnim naslovnim prostorom 192.168.0.x, lokalno domeno Windows AD, domena vodice.local. Dostop do interneta je vzpostavljen preko ADSL povezave s stalnim IP naslovom. Ponudnik dostopa je Telekom Slovenije.

Za stalno visoko razpoložljivost strežnika je zanj zagotovljen sistem brezprekinitvenega napajanja (UPS), tako da lahko nemoteno deluje tudi ob izpadih električne energije. Sistem UPS pa strežnik varuje tudi pred potencialno nevarnimi nihanji in napetostnimi »špicami« v električnem omrežju.

2.2. Zagotavljanje varnostnih kopij strežniškega datotečnega sistema

Vsi za občino pomembni podatki in datoteke se hranijo na strežniku, zato je nujno zagotavljati redno varnostno kopiranje vsebine datotečnega sistema le za strežnik.

Za varnostne kopije je poskrbljeno s programsko opremo, ki je nameščena na strežniku Symantec Backup Exec 12. Varnostne kopije se zapisujejo na trak na vgrajeni tračni enoti v strežniku. Varnostne kopije podatkov na strežniku se izdelujejo in shranjuje dnevno. Kopije, ki se naredijo od ponedeljka do četrtka, se v naslednjem tednu prepisujejo, kopije, ki se naredijo v petek, pa se shranjujejo za obdobje 4 tednov. Podatke (BACK-upe) se shranjuje na kasete, za katere skrbi zaposleni v sprejemni pisarni, kjer se kasete hranijo v zaklenjenem predalu mize.

Sistem zagotavljanja varnostnih kopij datotečnega sistema strežnika je primeren.

Predal, kjer se shranjujejo kasete z varnostnimi kopijami strežniškega datotečnega sistema, je lesen in ni ognjevaren, kar pomeni, da bi v primeru požara v prostorih občinske uprave lahko prišlo do hkratnega uničenja strežnika in varnostnih kopij podatkov na njem.

Priporočilo:

Glede na to, da je v prostorih občinske uprave na voljo tudi jeklena ognjevarna omara, predlagamo, da se kaseta z vsakokratno dnevno kopijo (zadnja varnostna kopija) hrani v tej ognjevarni omari. Tako bi zagotovili, da bi tudi v primeru požara v prostorih občinske uprave in morebitnega uničenja strežnika oziroma podatkov na njem vedno imeli na razpolago največ en dan stare podatke s strežnika.

Rok izvedbe: takoj in v nadaljevanju stalna naloga.

Občina Vodice v odgovoru na osnutek poročila o nadzoru z dne 20.6.2016 navaja, da to priporočilo že izvaja.

2.3. Zaščita pred virusi in drugo zlonamernimi programi

Za zaščito pred virusi je na strežniku nameščena protivirusna programska zaščita Trendmicro Client and Server Messaging Security, protivirusna zaščita delovnih postaj se posodablja s strežnika. Protivirusna zaščita je Trend Micro Line.

Neodvisni testi zaščitno programsko opremo Trendmicro ocenjujejo kot dobro do zelo dobro, pri čemer zelo pohvalijo predvsem njeno učinkovito zaščito pred virusi.

Zaščito pred virusi in zlonamerno kodo lahko ocenimo kot primerno.

2.4. Dostop do naprav, programov in podatkov

2.4.1. Politika gesel za dostop do računalnikov

Dostop do vseh računalnikov občinske uprave je možen le z uporabniškim imenom in geslom, za katerega veljajo naslednja pravila:

- sestavljeno mora biti iz najmanj 6 znakov, in sicer kombinacije velikih in malih črk in drugih znakov,
- geslo nima neomejenega trajanja ampak poteče po 6 mesecih,
- pred ali ob poteku gesla mora uporabnik sam spremeniti geslo,
- geslo ne sme biti enako zadnjemu uporabljenemu geslu,
- uporabnik je z geslom dolžan skrbno ravnati in ga ne razkriti nikomur drugemu.

Gesla vsakega uporabnika se hranijo v zapečateni kuverti v zaklenjeni ognjevarni omari. Pri menjavi gesla se uporabniku računalnikov vrne zapečateno kuverto s starim geslom, ta pa referentu za splošne zadeve in finance predloži kuverto z novim geslom. Kuverte se lahko odpre le v izrednih primerih (smrt uporabnika oziroma v primerih, ko je nujen dostop do vsebin podatkov uporabnika). Odpiranje kuverte in prijava v računalnik se v takem primeru izvede komisijsko.

Politika spreminjanja in zahtevnosti uporabniških gesel je podrobneje opisana v Organizacijskem predpisu – Navodilo za sistem varovanja podatkov na fiksnih in prenosljivih elektronskih medijih, št. 104-22/2014-002, z dne 25. 11. 2014.

Politiko gesel za dostop do računalnikov lahko ocenimo kot primerno.

2.4.2. Preprečevanje nepooblaščenega dostopa do računalnikov

Ko uslužbenec zapusti delovno mesto in pozabi zakleniti računalnik, se pojavi možnost nepooblaščenega dostopa do računalnika in s tem podatkov v informacijskem sistemu, ki so dostopni temu uslužbencu. Zato sistem Windows omogoča nastavitve samodejnega zaklepanja računalnika po določenem času nedejavnosti uporabnika. To pomeni, da se določen čas po odhodu uslužbenca tudi v primeru, ko sam pozabi zakleniti računalnik, le ta zaklene samodejno. Ker se to zgodi tudi v enakem času nedejavnosti, ko je uslužbenec še prisoten, ga to lahko moti in si želi nastavitev spremeniti. Zato mora biti iz varnostnih razlogov ta nastavitev možna samo z administratorskimi pravicami, da je ne more vsak uporabnik poljubno spreminjati.

V občinski upravi Občine Vodice je pri vseh zaposlenih nastavljeno, da se računalnik po 10 minutah nedejavnosti uporabnika zaklene in za ponovno uporabo zahteva geslo. Ko želi uporabnik ponovno uporabljati računalnik, se na zaslonu prikaže polje za vnos gesla za avtorizacijo, na enak način kot pri zagonu računalnika. Izklop funkcije ohranjevalnika zaslona ni možen.

Takšna ureditev je primerna in preprečuje dostop do računalnika, tudi če ga uporabnik pred odhodom z delovnega mesta ne zaklene.

2.4.3. Politika administratorskih pravic na računalnikih občinske uprave

Uslužbenci občinske uprave imajo na svojih računalnikih uporabniške račune brez administratorskih pravic, kar pomeni, da ne morejo niti hote niti ne hote spreminjati pomembnih nastavitev računalnika ter na njem spreminjati programske opreme (nameščanje in odstranjevanje programske opreme).

Administratorske pravice imata le dva uslužbenca občinske uprave, ki se ob potrebi po spreminjanju nastavitev ali programske opreme na določenem računalniku, vanj prijavita s svojim uporabniškim računom in opravita potrebne spremembe. To omogoča, da za posege,

ki jih lahko opravita ta dva uslužbenca občinske uprave, ni potrebno klicati podjetja za vzdrževanje informacijskega sistema in se s tem lahko znižujejo stroški tega vzdrževanja.

Slabost take ureditve je vtem, da imata ta dva uslužbenca tudi pri delu na svojem računalniku ves čas aktivne administratorske pravice in lahko tudi nehote (npr. ob prejemu okužene elektronske pošte) naredita spremembo na svojem računalniku.

Priporočilo: Uslužbencema, ki imata pooblastilo za uporabo administratorskih pravic na računalnikih občinske uprave, se dodeli po dva uporabniška računa. Enega z administratorskimi pravicami in enega brez njih, kakršne imajo vsi drugi uslužbenci. Pri svojem rednem delu naj uporabljata uporabniški račun brez administratorskih pravic, račun s temi pravicami pa le v primerih, ko nastane potreba po uporabi teh pravic.

Rok izvedbe: 90 dni po izdaji poročila.

Občina Vodice v odgovoru na osnutek poročila o nadzoru z dne 20.6.2016 navaja, da je tudi dodelitev dveh različnih uporabniških imen za oba uslužbenca občinske uprave, ki imata pooblastila administratorja, že v izvedbi.

2.4.4. Dostop do programov in dokumentov

Pomemben del varovanja podatkov v sistemih IT je spoštovanje načela najmanjšega privilegija, ki pomeni, da ima vsak uporabnik v informacijskem sistemu le tiste pravice ter dostop le do tistih programov in podatkov, ki jih potrebuje za opravljanje svojega dela, do drugih pa ne.

Občinska uprava pri svojem delu uporablja različno programsko opremo, pri čemer so za poslovanje in izvajanje nalog občine najpomembnejši:

- DOKSIS je program, ki vsebuje zbirko vseh dokumentov upravnega in neupravnega poslovanja, ponuja podporo Uredbi o upravnem poslovanju ter omogoča delo z dokumenti, skladno z zakonodajo;

  Uporabnik v programsko okolje dostopa s svojim uporabniškim imenom in geslom. Dostopa lahko do zadev, ki so mu bile dodeljene v reševanje in so signirane na uporabnikovo ime. Pri svojih zadevah lahko dokumente spreminja, dodaja in briše, vse spremembe pa so v sistemu evidentirane (čas in oseba, ki je izvajala spremembe).

- CADIS je program, ki omogoča različne sisteme kot je sistem plačane realizacije (proračunski uporabniki), evidenčno knjiženje (javni zavodi, režijski obrati občin) ali poljuben drug sistem;

  V programsko okolje se dostopa na enako način kot pri programu DOKSIS. Vsak skrbnik proračunske postavke lahko v okviru svoje pravic vedno spremlja stanje proračuna (realizacija proračunske postavke, predobremenitve, prosta sredstva,...).

- PISO je prostorski pregledovalnik, ki predstavlja enotno geoinformacijsko infrastrukturo, ki je na voljo vsem občinam v državi. Občinam, podjetjem in občanom omogoča učinkovit vpogled v državne in občinske prostorske evidence. Vsebuje informacijsko podporo za izvajanje različnih poslovnih procesov vezanih na prostor.

V programsko okolje se dostopa na enak način kot pri programu DOKSIS. Zaradi varovanja osebnih podatkov je program že v zasnovi ločen na dva dela, javni in interni del. Interni dostop je omogočen zaposlenim, ki podatke iz posameznega modula potrebujejo pri izvajanju nalog v okviru svojega delovnega mesta (npr.: izdaja lokacijske informacije, podatki za izračuna nadomestila za uporabo stavbnega zemljišča,...).

V postopku nadzora je bilo preverjeno, da v programsko okolje zgoraj naštetih programov zaposleni lahko vstopajo le z uporabniškim imenom in geslom, ki mu je bilo dodeljeno s strani administratorjev posameznih programov. Programe sestavljajo različni moduli, dostop do modulov pa je uporabnikom omogočen le na podlagi njegovih pravic, ki so mu bile dodeljene po načelu najmanjšega privilegija, tako da lahko uporabnik dostopa do podatkov, če le-te potrebuje pri opravljanju nalog med delovnim procesom, kar je bilo med nadzorom nazorno prikazano in preverjeno.

Programska oprema torej omogoča, občinska uprava pa pravilno uporablja nastavitve pravic uslužbencev, tako da ima vsak dostop do podatkov in dokumentov, ki jih potrebuje, do drugih pa ne, oziroma, da lahko spreminja le dokumente in izvaja le postopke za katere je odgovoren in pristojen.

2.4.5. Zagotavljanje sledljivosti sprememb in dostopov do podatkov in dokumentov

Za zagotavljanje verodostojnosti, zaupnosti, neokrnjenosti in razpoložljivosti informacij in dokumentov ter učinkovit nadzor na varovanjem osebnih podatkov je pomembna sledljivost in evidentiranje tako dostopov kot sprememb dokumentov in podatkov v informacijskih sistemih.

V občinski upravi je sledljivost sprememb dokumentov v veliki meri zagotovljena že v programski opremi DOKSIS, KADIS in PISO. Število uporabnikov, ki lahko spreminjajo določene dokumente, je določeno po načelu najmanjšega privilegija, tako da je to število čim manjše. Spremembe se v sistem evidentirajo na podlagi uporabniškega imena pod katerim so bile izvedene.

Program PISO, ki med drugim vsebuje tudi zbirke osebnih podatkov, beleži vse dostope do podatkov, ki so bili izvedeni s posameznim uporabniškim imenom. Po preverbi katerega koli podatka v sistemu PISO se v sistem shranijo podatki, kdo je pregledoval (uporabniško ime), kdaj je pregledoval, kje je pregledoval in kaj se je pregledovalo iz zbirke osebnih podatkov, ki so vsebovane v pregledovalniku PISO.

Ob nadzoru smo ugotovili, da so tudi podatki o dostopih do podatkov varovani in jih ponudnik programske opreme priskrbi le ob sklepu pristojnega organa.

Na podoben način je sledljivost omogočena tudi pri **programu CADIS**. V zvezi s tem je občinska uprava za potrebe nadzora pridobila izjavo ponudnika programske opreme, v kateri ta pojasnjuje:

Vsi dostopi (prijave) in aktivnosti znotraj programske opreme se beležijo v posebni dnevniški bazi, ki je ločena od podatkov. Po potrebi (npr. pri forenzični preiskavi, reviziji) na zahtevo občine lahko to revizijsko sled izvozimo za nadaljnjo obravnavo. Beležijo se vsi vnosi in spremembe vnosov, dostopi do izpisov in uporabljeni kriteriji za izpis, prijave ... Za vsak dnevniški zapis se beleži tudi uporabnik, datum in ura. Zapisov v revizijski sledi uporabniki ne morejo spreminjati ali brisati.

Sledljivost sprememb je zagotovljena v revizijski sledi, ki je zapisana v dnevniški bazi. S tem so mišljene spremembe podatkov v naši podatkovni bazi.

Nespremenljivost listin, ki imajo status nespremenljivosti, se zagotavlja s podpisovanjem s kvalificiranimi digitalnimi potrdili (SiGen-CA). V primeru naknadnega spreminjanja dokumentov so digitalni podpisi neveljavni. V dokumentnem sistemu se hranijo različice dokumentov.

Program Doksis je v osnovi namenjen arhiviranju vseh vhodnih in izhodnih dokumentov Občine Vodice. Sistem je nastavljen tako, da vsak uporabnik lahko upravlja le z lastnimi dokumenti in dokumenti, ki so mu dodeljeni v reševanje. Sledljivost sprememb je zagotovljena s signirno oznako in datumom spremembe (dodajanja) dokumenta.

Dokumenti so shranjeni v načinu READ ONLY, tako da jih uporabniki lahko vidijo, ne morejo pa jih spreminjati. Spreminja jih lahko le uporabnik, ki je dokument ustvaril.

2.4.6. Varovanje osebnih podatkov v elektronski obliki pri uporabi sistemov IT

V zvezi z varovanjem osebnih podatkov je Občina Vodice v letu 2014 sprejela Pravilnik o zavarovanju osebnih podatkov, št. 104-24/2014-001, z dne 27. 11. 2014. Pravilnik določa ukrepe za zavarovanje osebnih podatkov pri zbiranju, obdelovanju, shranjevanju, posredovanju in njihovi uporabi na občini. Zavarovanje osebnih podatkov zajema pravne, organizacijske in ustrezne logistično-tehnične postopke in ukrepe, s katerimi se:

- varuje sistemska programska oprema naprav, na katerih se obdelujejo osebni podatki
- varuje aplikativna programska oprema, s katero se obdelujejo osebni podatki,
- zagotavlja varnost posredovanja in prenosa osebnih podatkov,
- nepooblaščenim osebam onemogoči dostop do naprav, na katerih se obdelujejo osebni podatki in do njihovih zbirk,
- omogoča naknadno ugotavljanje, kdaj so bili posamezni podatki uporabljeni in vneseni v zbirko podatkov in kdo je to storil, in sicer za obdobje, za katero se posamezni podatki shranjujejo.

Pravilnik v določa, da morajo biti računalniki ali druga strojna oprema, na kateri se obdelujejo ali hranijo osebni podatki izven delovnega časa programsko zaklenjena, dostop do osebnih podatkov hranjenih na disku računalnika, pa avtoriziran.

Določa tudi, da morajo biti v prostorih, kjer imajo vstop stranke oziroma osebe, ki niso zaposlene na občini, nosilci podatkov in računalniški prikazovalniki nameščeni v času dela na njih tako, da strankam ni omogočen poglede vanje.

Vzdrževanje in popravilo strojne računalniške in druge opreme, s katero se obdelujejo osebni podatki, je dovoljeno samo z vednostjo in odobritvijo pooblaščene osebe (direktor občinske uprave), izvajajo pa ga lahko samo pooblaščeni servisi in njihovi vzdrževalci, ki imajo z občino sklenjeno pogodbo o servisiranju računalniške oziroma strojne opreme. Ti so v pogodbi zavezani tudi k varovanju vseh podatkov v opremi, ki jo servisirajo.

Občina Vodice vodi osebne podatke v zbirkah osebnih podatkov – stalne zbirke. Te zbirke so določene z Internim seznamom katalogov zbirk osebnih podatkov.

V primeru, da osebne podatke iz zbirk osebnih podatkov posreduje drugim upravičencem, se to vpiše v knjigo evidenc o ravnanju z osebnimi podatki.

Brisanje osebnih podatkov na računalniških medijih se opravi na način, po postopku in metodi, ki onemogoča restavriranje brisanih podatkov. Uničevanje in brisanje zbirke osebnih podatkov se opravi komisijsko (Župan imenuje tričlansko komisijo s trajnim mandatom, ki prisostvuje in protokolira vsak izbris in uničenje nosilcev osebnih podatkov z zapisnikom.).

V praksi se to nanaša na primere, ko občina prejme osebne podatke v papirnati obliki oziroma na računalniškem mediju (CD, disketa, ipd,...). Pri brisanju podatkov iz baze podatkov v računalniškem sistemu, je te podatke še vedno mogoče restavrirati v času hranjenja varnostnih kopij strežniškega datotečnega sistema, kar pomeni, da se ob uporabi take kopije lahko v sistemu ponovno pojavijo podatki, ki so že bili izbrisani in jih tam ne bi več smelo biti. Temu se je včasih nemogoče izogniti, dobro pa se je tega zavedati.

Za brisanje datotek v računalnikih se ne uporablja posebna programska oprema. Brisanje z običajnim ukazom za brisanje ali delete pomeni, da je te datoteke s forenzičnimi metodami vsaj še nekaj časa po brisanju mogoče restavrirati, saj ta pobriše le informacije o lokaciji datoteke na datotečnem sistemu, same vsebine datoteke pa ne.

Pri zbirkah osebnih podatkov, ki se vodijo s programi, ki vsebujejo tudi potrebno zaščito osebnih podatkov in zagotavljajo sledljivost dostopov do osebnih podatkov tega problema ni, saj tam ob brisanju podatkov ne gre za brisanje datotek, ampak za brisanje podatka v podatkovni bazi, torej za spremembo vsebine datoteke.

Če se vse zbirke osebnih podatkov razen Kataloga evidence videoposnetkov in Zbirke zvočnih zapisov sej občinskega sveta vodijo v takšnih programih, lahko ugotovimo, da je za njihovo varovanje in tudi brisanje ustrezno poskrbljeno.

Ob prenosu osebnih podatkov po elektronski pošti morajo biti le-ti zavarovani z geslom za identifikacijo upravičenca do njih. Vsebina zbirke ali zbirk podatkov, ki se prenašajo po komunikacijskih kanalih, po elektronski pošti ali fizično na računalniških medijih izven prostorov občine, se mora med prenosom napraviti nečitljiva z ustreznimi standardnimi kriptografskimi metodami.

Na vprašanje glede programskih orodij, ki se uporabljajo za kriptiranje osebnih podatkov za pošiljanje po elektronski pošti, predstavnik občine pojasni, da v praksi osebni podatki po elektronski pošti ne pošiljajo.

Župan, direktor občinske uprave, delavci, ki upravljajo z osebnimi podatki, ter referent v vložišču, so pooblaščeni, da za potrebe svojega dela vpogledajo in uporabijo osebne podatke, vsebovane v zbirkah osebnih podatkov vodenih v občini.

Za inšpekcijski nadzor nad varovanjem osebnih podatkov je pristojen informacijski pooblaščenec.

Upoštevanje vseh določb Pravilnika o zavarovanju osebnih podatkov zagotavlja ustrezno varovanje osebnih podatkov v informacijskih sistemih in postopkih Občine vodice.

2.4.7. Upravljanja in vzdrževanja informacijskega sistema ter sprememb v njem

Za varnost in zanesljivost je pomembno tudi njegovo vzdrževanje in upravljanje, redno posodabljanje programske opreme, odpravljanje napak, ...

- Informacijski sistem Občine Vodice vzdržuje ENA d.o.o.
- Vzdrževalec odpravlja napake na strojni in programski opremi, pregleduje sistemske LOG datoteke, opravlja nadzor nad izvajanjem varnostnih kopij, izvaja redno vzdrževanje programske in stojne opreme.
- Vzdrževalec je bil izbran preko javnega naročila (evidenčni postopek), vsa dela se izvajajo na podlagi pogodbe št. 430-04/2015-005, z dne 13. 5. 2014 in Aneksa k pogodbi št. 1, št. 430-04/2014-007, z dne 1. 12. 2014. Občina mesečno plačuje izvedena dela, na podlagi potrjenega e-računa po dejansko opravljenih količinah.
- Vzdrževanje poteka fizično na računalniku ali drugi strojni opremi v prostorih občine, v nujnih primerih, pa tudi preko oddaljenega dostopa, ob prisotnosti zaposlenega. Oddaljen dostop se vedno vzpostavi le za potrebe in čas trajanja posameznega posega. Vzdrževalna dela se pričnejo po predhodni odobritvi s strani Občine Vodice. Vsi dostopi preko oddaljenega dostopa se beležijo v evidenco dostopov pri zaposlenem v občinski upravi.
- Vsi predvideni posegi se vpisujejo v delovni nalog, ki je pripravljen na podlagi predlogov s strani zaposlenih občinske uprave. Nalog podpiše vzdrževalec in pristojna oseba naročnika. Podpisan nalog je podlaga za pričetek izvajanja del.
- Vzdrževalec v delovnih nalogih dokaj izčrpno opiše opravljena dela in posege, tako da je iz njih dovolj jasno razvidno, za kaj je šlo pri posameznem posegu oziroma opravilu.
- Ocena zaračunanega obsega dela za posamezne posege in primernost cen storitev (v primerjavi z drugimi izvajalci) niso predmet tega nadzora.

3. MNENJE

Občina Vodice ima urejena pravila ter postopke in opremo za zagotavljanje varnosti in zanesljivosti informacijskega sistema, ki ga uporablja občinska uprava. Za svoje poslovanje in delovanje uporablja programska orodja, ki zagotavljajo selektiven dostop do podatkov in dokumentov ter sledljivost dostopov in sprememb podatkov in dokumentov. Občina ima sprejet Pravilnik o zavarovanju osebnih podatkov, ki zagotavlja dobro varstvo osebnih podatkov. Prav tako ima za vzdrževanje informacijskega sistema sklenjeno pogodbo z usposobljenim izvajalcem.

Ob pregledu postopkov in ravnanj sem podal nekaj priporočil za njihovo izboljšanje, v nobenem primeru pa ni šlo za večje napake ali nepravilnosti.

Nadzorni odbor glede varnosti in zanesljivosti informacijske tehnologije v Občini Vodice izdaja **pozitivno mnenje.**

Povzetek priporočil:

- Zadnja dnevna varnostna kopija datotečnega sistema strežnika naj se hrani v jekleni ognjevarni omari.
- Uslužbencema, ki imata pooblastilo za uporabo administratorskih pravic na računalnikih občinske uprave, se dodeli po dva uporabniška računa. Enega z administratorskimi pravicami in enega brez njih.

Predlagamo, da se priporočila, navedena v tem poročilu izvedejo v rokih in se v prihodnosti trajno upoštevajo.

Občina Vodice v odgovoru na osnutek poročila o nadzoru z dne 20.6.2016 navaja, da obe priporočili v praksi že upošteva.

Nadzor izvedel:
Tomaž Merše, član Nadzornega odbora

Predsednica Nadzornega odbora
Andreja Rahne

OBČINA VODICE NADZORNI ODBOR

Prejemnik poročila:
Aco Franc Šuštar, župan Občine Vodice