

Na podlagi 80. člena Uredbe o upravnem poslovanju (Uradni list RS, št. 20/05, 106/05, 30/06, 86/06, 32/07, 63/07, 115/07, 31/08, 35/09, 58/10, 101/10 in 81/13), Priporočil informacijske varnostne politike javne uprave (št. 386-2/2008/23 z dne 28. 10. 2010), 51. in 89. člena Statuta Mestne občine Ljubljana (Uradni list RS, št. 24/16 – uradno prečiščeno besedilo) in 4. člena Odredbe o varnostni politiki št. 386-1/2010-19 z dne ~~14. 4. 2018~~ izdaja župan Mestne občine Ljubljana

PRAVILNIK O VAROVANJU PRED ZLONAMERNO KODO

I. SPLOŠNE DOLOČBE

1. člen

S tem pravilnikom Mestna občina Ljubljana (v nadaljnjem besedilu: MOL) določa postopke za preprečitev vstopa zlonamerne kode v informacijski sistem. Ta pravilnik upošteva vse naprave, namenjene obdelavi podatkov, ki jih uporabljajo zaposleni v Mestni upravi MOL (v nadaljnjem besedilu: mestna uprava), drugi uporabniki v MOL in zunanji izvajalci, ki uporabljajo sredstva MOL (v nadaljnjem besedilu: zunanji izvajalci).

2. člen

Namen tega pravilnika je preprečitev nenačrtovanih prekinitev poslovnih procesov mestne uprave, razkritja informacij, nepooblaščenega dostopa do podatkov ter odprava motenj v poslovanju, ki jih lahko povzroči zlonamerna koda.

3. člen

Naloga zaposlenih v mestni upravi, drugih uporabnikov v MOL in zunanjih izvajalcev (v nadaljnjem besedilu: uporabniki) je, da ravnajo v skladu s tem pravilnikom in se, po potrebi, posvetujejo s Centrom za informatiko (v nadaljnjem besedilu: CI), z namenom zagotavljanja čim boljše zaščite pred zlonamerno kodo na vseh napravah, ki jih uporabljajo pri svojem delu.

Zunanje izvajalce se k ravnanju skladno s tem pravilnikom zaveže s pogodbo oziroma izjavo, kot to določa 5. člen Odredbe o varnostni politiki.

II. ZAŠČITA

4. člen

Na sredstvih za obdelavo podatkov je lahko nameščena le programska oprema, ki jo odobri CI. CI uporabnike obvešča o grožnjah, delovanju in učinkih zlonamerne kode ter jih prek rednih izobraževanj ali internih obvestil sistematično seznaja o tveganjih, povezanih z zlonamerno kodo.

5. člen

CI spremlja trende pojavljanja zlonamerne kode na spletnih straneh protivirusne programske opreme. Glede na ocenjeno stopnjo trenutne ranljivosti, CI poda priporočila, ki zagotavljajo varno poslovanje MOL.

Uporabniki naprav za obdelavo podatkov:

- v primeru suma ali ugotovitve, da sistem za protivirusno zaščito ne deluje ali ni ustrezno posodobljen, morajo takoj obvestiti CI,
- ne smejo nameščati zlonamerne kode v računalnik,
- ne smejo posredovati naprej okuženih datotek preko različnih medijev in elektronske pošte,
- ne smejo zaganjati programov, če ne vedo, čemu služijo,
- ne smejo odpirati nepoznanih datotek, za katere ne vedo, čemu služijo.

III. ODKRIVANJE IN PREGLEDOVANJE VSEBIN

6. člen

Za nadzor pred zlonamerno kodo se uporablja večnivojska programska oprema na strežniški infrastrukturi ter na uporabniških odjemalcih.

Uporabniki, ki dostopajo do sistemov v lasti MOL, morajo obvezno sami poskrbeti za ustrezno raven zaščite pred zlonamerno programsko opremo. Kot ustrezna raven zaščite se šteje licenčna protivirusna programska oprema s požarnim zidom, ki je nameščena na delovni postaji ali prenosnem računalniku, ki se uporablja za dostop.

Dostop za zunanje uporabnike CI omogoči po presoji ustreznosti zaščite pred zlonamerno kodo na podlagi predloženih tehničnih dokazil.

7. člen

Obstoj in delovanje zlonamerne kode v sistemu nadzira CI. Naloge CI pri tem so:

- nadzor strežnikov pred zlonamerno kodo,
- nadzor delovnih postaj in prenosnih računalnikov pred zlonamerno kodo,
- nadzor nad nezaželeno elektronsko pošto na poštnem strežniku,
- nadzor omrežnega prometa v lokalnem omrežju MOL in javno dostopnem delu omrežja MOL.

V primeru odkritih neskladnosti na sredstvih MOL, CI sredstvo pregleda ter po potrebi odpravi vzrok nepravilnega delovanja. V primeru anomalij na zunanjem omrežju, CI tveganega uporabnika blokira.

Uporabniki, ki za dostop uporabljajo sredstva v lasti MOL, morajo ta sredstva najmanj enkrat mesečno priključiti v interno omrežje MOL.

V primeru, da uporabnik za dostop uporablja sredstva, ki niso v lasti MOL, mora sredstvo ustrezno zaščititi.

8. člen

V primeru odkritja zlonamerne kode CI s pregledom sistemskih dnevnikov določi izvor ali razlog pojavitve in ukrepa v skladu z opredeljenimi postopki.

9. člen

Prenosni nosilci podatkov se med uporabo na sredstvih MOL avtomatsko preverjajo s protivirusnim programom, ki je nameščen lokalno na delovni postaji ali prenosnem računalniku. V primeru, da so na nosilcu datoteke sumljivega izvora, jih uporabniki ne smejo odpirati ali zaganjati.

10. člen

Protivirusna programska oprema se na delovnih postajah in prenosnih računalnikih nadgrajuje avtomatsko.

IV. ODKRIVANJE VDOROV

11. člen

Zaposleni v CI o vsakem vdoru v informacijski sistem MOL obvestijo vodjo CI. Ta skupaj z ostalimi oceni kritičnost incidenta. V primeru, da ima incident hude posledice, oziroma če gre za sum prekrška ali kaznivega dejanja, vodja CI o tem obvesti direktorja mestne uprave. Ta odloči, ali se pripravi prijava incidenta pristojnemu organu. V primeru prijave se sredstva, na katerih je prišlo do incidenta, ne uporabljajo. CI pripravi zapisnik o varnostnem incidentu, ki je priloga prijave pristojnemu organu, ki jo podpiše župan.

V. ODSTRANJEVANJE ZLONAMERNE PROGRAMSKE OPREME

12. člen

Protivirusni program, ki se uporablja, mora imeti aktivirano funkcijo preverjanja in prepoznavanja morebitne nove zlonamerne kode. Protivirusni program v primeru odkritja o tem obvesti uporabnika in administratorja CI ter zlonamerno kodo samodejno izolira in odstrani. Dogodek se zabeleži v CI.

13. člen

CI je pristojen za vzdrževanje in konfiguracijo protivirusnega sistema.

14. člen

V primeru hujšega incidenta, CI izolira uporabnika oziroma segment mreže, kjer se nahaja okužba.

15. člen

Če uporabnik odkrije zlonamerno kodo, ki je protivirusni program ni zaznal, mora takoj prekiniti vse aktivnosti na okuženi delovni postaji ali prenosnem računalniku in o tem nemudoma obvestiti CI. Pri tem beleži simptome in kakršna koli sporočila, ki se pojavijo na zaslonu.

CI poskuša prepoznati zlonamerno kodo, jo odstraniti, obnoviti sistem in določiti vzrok okužbe. Prenosnih nosilcev podatkov, ki so se uporabljali na okuženem računalniku, se ne sme uporabljati na ostalih računalnikih.

16. člen

CI v primeru suma, da se na določeni delovni postaji, prenosnem računalniku ali strežniku nahaja zlonamerna koda, opravi analizo te naprave.

VI. POROČANJE O ZLONAMERNI KODI

17. člen

CI pripravi poročilo v primeru odkritja varnostnega incidenta, slabostih varovanja pred zlonamerno kodo ter motnjah delovanja programske opreme ter opredeli korektivne ukrepe.

VII. KONČNA DOLOČBA

18. člen

Ta pravilnik začne veljati naslednji dan po objavi na intranetni strani MOL.

Številka: 386-1/2010-24

Datum:

24-04-2018

Župan
Mestne občine Ljubljana
Zoran Janković

