

Na podlagi prvega odstavka 80. člena Uredbe o upravnem poslovanju (Uradni list RS, št. 20/2005, 106/2005, 30/2006, 86/2006, 32/2007, 63/2007, 115/2007, 31/2008 in 35/2009)
generalna direktorica Statističnega urada Republike Slovenije izdaja naslednji

Pravilnik o zaščiti pred zlonamerno programsko opremo

VSEBINA

1	NAMEN PRAVILNIKA	83
2	ZLONAMERNA PROGRAMSKA OPREMA.....	83
2.1	Vrste zlonamerne programske opreme	83
2.2	Najpogostejši načini okužbe.....	84
2.3	Posledice uporabe zlonamerne programske opreme.....	84
3	TEHNIČNA ZAŠČITA PRED ZLONAMERNO PROGRAMSKO OPREMO	84
3.1	Požarni zid.....	84
3.2	Zaščita internetnega prometa	84
3.3	Zaščita strežnikov elektronske pošte	85
3.4	Zaščita delovnih postaj in strežnikov	85
3.5	Povezovanje v internet preko drugih omrežij.....	85
3.6	Razvoj novih programskih rešitev.....	85
4	UPORABNIŠKE AKTIVNOSTI	86
5	ODZIV NA OKUŽBO Z ZLONAMERNO PROGRAMSKO OPREMO	86
6	KONČNE DOLOČBE	86

1 NAMEN PRAVILNIKA

Pravilnik zaščite pred zlonamerno programsko opremo je sprejet z namenom varovanja vseh informacijskih virov Statističnega urada Republike Slovenije (v nadaljevanju: Urad), predvsem pa tistih, ki se nanašajo na povezavo z internetom, storitve elektronske pošte in varovanje delovnih postaj ter strežnikov.

Ta pravilnik določa pravila za nameščanje in uporabo tehničnih sredstev pri zaščiti pred zlonamerno programsko opremo ter pravila uporabniških aktivnosti pri preprečevanju okužbe in razširjanja zlonamerne programske opreme. Pravilnik so dolžni upoštevati vsi zaposleni na Uradu ter vse tretje osebe (v nadaljevanju uporabniki), ki jim je omogočen dostop do informacijskih virov Urada.

Pravilnik je zasnovan na standardu informacijske varnosti ISO/IEC 27001:2005 in predstavlja izvedbeno politiko v sklopu krovne varnostne politike Urada.

Cilj aktivnosti zaščite pred zlonamerno programsko opremo je preprečevanje škode, ki bi nastala zaradi okužbe z zlonamerno programsko opremo.

2 ZLONAMERNA PROGRAMSKA OPREMA

2.1 Vrste zlonamerne programske opreme

Zlonamerna programska oprema (angl. malware) se uvršča v eno ali več naslednjih skupin:

- 🔑 **virusi:** samostojni programi, ki se lahko sami razmnožujejo in okužijo računalnik brez vednosti uporabnika; običajno delujejo tako, da poškodujejo ali uničujejo datoteke;
- 🔑 **črvi** (angl. worms): samostojni programi, ki se lahko sami razmnožujejo preko telekomunikacijskih sredstev; običajno ne škodujejo drugim datotekam, vendar obremenijo računalniško omrežje do te mere, da je delovanje močno oteženo ali nemogoče;
- 🔑 **trojanski konji** (angl. trojan horses): programi, ki navidezno opravljajo koristno funkcijo, a hkrati omogočijo nepooblaščen oddaljen dostop in nadzor nad uporabnikovo delovno postajo;
- 🔑 **rootkit** (v orig.): programi, ki neopazno prevzamejo nadzor nad operacijskim sistemom, zato jih je izjemno težko odkriti; podobno kot trojanski konji omogočajo predvsem oddaljen dostop in nadzor nad delovno postajo ali strežnikom;
- 🔑 **vohumnska programska oprema** (angl. spyware): programi, ki nadzirajo in zbirajo osebne podatke uporabnikov ter jih posredujejo tretjim osebam brez uporabnikove vednosti ali odobritve;
- 🔑 **oglasna programska oprema** (angl. adware): programi, ki samodejno prenašajo in predvajajo oglasna sporočila uporabniku brez njegove privolitve;
- 🔑 **zločinska programska oprema** (angl. crimeware): programi, ki so namenjeni kraji (digitalne) identitete z namenom pridobivanja neposredne finančne koristi (nakupovanje v tujem imenu, uporaba tujega bančnega računa ipd.).

Zgornje skupine zlonamerne programske opreme predstavljajo le splošni okvir, pogosto namreč lahko posamezen program uvrstimo v več skupin hkrati.

2.2 Najpogostejši načini okužbe

Najpogostejši načini okužbe z zlonamerno programsko opremo so:

- 🔑 odpiranje okužene e-pošte ali okuženih pripetih dokumentov;
- 🔑 klikanje na spletne povezave, ki navidezno kažejo na spletne naslove uradnih institucij (npr. bank) v e-poštnih sporočilih, ki so sumljivega izvora;
- 🔑 obiskovanje sumljivih spletnih strani (npr. pornografske strani, strani z nelegalnimi vsebinami) in klikanje na sumljive spletne reklame;
- 🔑 uporaba zasebnih USB ključkov, CD/DVD medijev in drugih prenosnih medijev.

2.3 Posledice uporabe zlonamerne programske opreme

Posledice uporabe zlonamerne programske opreme so:

- 🔑 razkritje osebnih in/ali zaupnih informacij;
- 🔑 nedelovanje oz. upočasnjeno delovanje omrežnih komunikacij;
- 🔑 poškodovanje ali uničenje dokumentov, baz podatkov in drugih elektronskih oblik podatkov;
- 🔑 odtujitev finančnih sredstev preko spletnega bančništva, spletnega nakupovanja ipd.;
- 🔑 kraja (digitalne) identitete.

3 TEHNIČNA ZAŠČITA PRED ZLONAMERNO PROGRAMSKO OPREMO

S tehničnimi sredstvi za zagotavljanje zaščite pred zlonamerno programsko opremo upravljajo izključno zaposleni sektorja, pristojnega za informacijsko infrastrukturo in tehnologijo (v nadaljevanju tudi »SIIT«). Zaposleni SIIT se morajo kontinuirano izobraževati na področju varnosti informacijskih sistemov.

Posamezne nastavitve delovanja teh sredstev so prepuščene presoji zaposlenih tega sektorja, vendar morajo biti skladne tako s krovno varnostno politiko kot tudi s tem in vsemi ostalimi pravilniki, ki se nanašajo na informacijsko varnost.

3.1 Požarni zid

Požarni zid predstavlja ključno tehnično sredstvo za filtriranje elektronskega prometa z internetom ter posledično zaščito pred zlonamerno programsko opremo. Pooblaščen osebe iz SIIT izvedejo ustrezno nastavitve požarnega zidu tako z vidika vhodnega, kot tudi z vidika izhodnega prometa.

3.2 Zaščita internetnega prometa

Poleg požarnega zidu, ki omogoča določene stopnje filtriranja elektronskega prometa z internetom, Urad lahko dodatno filtrira promet tudi na podlagi vsebine, dovoljenih spletnih strani, časa dostopa ipd, skladno s pravilnikom o uporabi interneta. Na ta način pregleduje promet za morebitno zlonamerno programsko opremo, ki je ne bi zaznal in zaustavil požarni zid. Vsa elektronska komunikacija delovnih postaj in strežnikov mora biti preusmerjena na vmesni strežnik (angl. proxy server) z uporabo ustreznih nastavitev domenske politike. Vmesni strežnik je upravljan s strani MJU v skladu s svojo varnostno politiko.

Vse delovne postaje, ki niso v upravljanju Urada (npr. prenosniki, ki so last gostov) in so priključene na LAN omrežje, dostopajo do interneta preko vmesnega strežnika.

3.3 Zaščita strežnikov elektronske pošte

Strežnik elektronske pošte v Uradu je del sistema elektronske pošte v okviru HKOM, ki ga upravlja MJU v skladu s svojo varnostno politiko. Lokalni strežnik, ki skrbi predvsem za lokalno hrambo elektronske pošte in za hitrejše delovanje storitve, je v upravljanju Urada.

3.4 Zaščita delovnih postaj in strežnikov

Na vseh delovnih postajah, prenosnikih in podobnih napravah in topološko izpostavljenih strežnikih mora biti nameščena protivirusna programska oprema, ki se redno posodablja s centralnega strežnika protivirusne programske opreme ter stalno in v rednih presledkih preverja delovne postaje in strežnike za prisotnost zlonamerne programske opreme. Centralni strežnik se redno posodablja.

Za dostop do interneta se uporablja zadnja verzija spletnega brkljalnika, ki se redno posodablja, promet mora biti usmerjen preko vmesnega strežnika, nastavitve nivoja varnosti pa na najvišji možni nastavitvi, ki še omogoča nemoteno redno delo uporabnikov. Nastavitve se vodijo centralno z uporabo domenske politike.

Namestitev programske opreme s strani uporabnikov mora biti onemogočena in je prepovedana. Pravice do nameščanja programske opreme izjemoma podeljuje zaposleni SIIT-a samo osebam na podlagi potrditve OSUVI-ja.

3.5 Povezovanje v internet preko drugih omrežij

Osebni računalniki lahko z uporabo mobilnih in drugih komunikacijskih naprav ali z uporabo klicnih modemov dostopajo do interneta, s čemer lahko zaobidejo tehnična sredstva za filtriranje prometa, nadzor nad uporabo interneta in za zaščito pred zlonamerno programsko opremo. Če uporabniki za dostop do interneta uporabljajo takšne vrste povezav, so dolžni zagotoviti, da je takšen osebni računalnik ali komunikacijska naprava fizično izolirana od komunikacijskega omrežja Urada. Hkrati morajo zaposleni SIIT, ki so zadolženi za omrežje in domensko politiko, z ustreznimi sistemskimi nastavitvami onemogočiti povezovanje z več vzporednimi omrežji.

3.6 Razvoj novih programskih rešitev

Pri razvoju novih programskih rešitev je pri načrtovanju potrebno upoštevati tudi tehnične zahteve za zaščito programskih rešitev pred zlonamerno programsko opremo. Prav tako je v okviru testov nove programske rešitve v nekaterih primerih potrebno izvesti tudi teste napadov z zlonamerno programsko opremo ter se tako prepričati o tem, da ima čim manj programskih ranljivosti.

4 UPORABNIŠKE AKTIVNOSTI

Tehnična sredstva ne morejo nikoli v celoti zagotoviti popolnega varovanja računalniških sredstev in uporabnika pred zlonamerno programsko opremo. Uporabnik mora zato pri zaščiti pred zlonamerno programsko opremo aktivno sodelovati z izvajanjem ustreznih aktivnosti. V veliki meri so konkretne želene in neželene aktivnosti, ki prispevajo k povečani varnosti pred zlonamerno programsko opremo, opisane v Pravilniku uporabe elektronske pošte in Pravilniku uporabe interneta. Poleg aktivnosti, opisanih v obeh pravilnikih, pa morajo uporabniki upoštevati predvsem načelo previdnosti, in sicer:

- ✎ morajo, če sumijo, da na informacijskem sistemu deluje ali je prisotna zlonamerna programska oprema takoj nehati delati z njim, obvestiti sistemsko tehnično podporo (surs.podpora) in upoštevati njena navodila;
- ✎ ne smejo zaganjati izvršljive programske opreme, ki ni del njihovega informacijskega sistema (izvirajo npr. s svetovnega spleta, elektronske pošte, pomnilniških medijev);
- ✎ ne smejo zaganjati dokumentov, npr. s svetovnega spleta, elektronske pošte, pomnilniških medijev, če so sumljivi, če ne vedo, čemu so ti dokumenti namenjeni ali če ne poznajo njihovega izvora;
- ✎ morajo, če sumijo ali ugotovijo, da sistem za protivirusno zaščito ne deluje ali ni ustrezno posodobljen, takoj nehati uporabljati informacijski sistem, obvestiti sistemsko tehnično podporo (surs.podpora) in upoštevati njena navodila.

5 ODZIV NA OKUŽBO Z ZLONAMERNO PROGRAMSKO OPREMO

Uporabnik, ki sumi, da bi se na njegovi delovni postaji lahko nahajala zlonamerna programska oprema, mora o tem takoj obvestiti sistemsko tehnično podporo (surs.podpora).

Sektor Informacijske infrastrukture in tehnologije pripravi odzive na sum okužbe z zlonamerno programsko opremo v okviru postopkov za upravljanje incidentov ter kriznih načrtov v okviru politike neprekinjenega delovanja.

6 KONČNE DOLOČBE

Odbor za sistem upravljanja varstva informacij (OSUVI) izvaja redne letne pregleda tega pravilnika in ga po potrebi uskladi z drugimi pravilniki in politikami Urada ali prilagodi potrebam Urada.

Ta pravilnik začne veljati trideseti dan po objavi na internem portalu Urada.

Številka: 007-47/2011/9

Datum: 21. 9. 2011



Križman
Mag. Irena Križman,
generalna direktorica