3 Zaščita pred spletnimi zlorabami

Kazalo

3.1 Vrste spletnih zlorab

Na svetovnem spletu se srečuje na stotine milijonov ljudi, ki med sabo komunicirajo, pregledujejo spletne strani in uporabljajo raznovrstne spletne storitve. Splet uporabljajo tudi osebe, ki niso dobronamerne, njihov cilj so materialne ali nematerialne koristi. Kot v resničnem svetu, se tudi v virtualnem svetu srečujemo z lažnimi identitetami, krajami, prevarami, goljufijami, dezinformacijami, žalitvami, nestrpnostjo idr.

Vendar stvari niso tako črnoglede, kot izgleda na prvi pogled. Z vsaj malo osnovnega znanja ter s pomočjo preudarnega ravnanja, se lahko obranimo marsikatere nevšečnosti.

Škodljiva programska koda so po domače programi, ki pri uporabniku povzročajo škodo. Škodljivi programi lahko brišejo datoteke, spreminjajo nastavitve računalnika, upočasnijo računalnik ali internetno povezavo. Internetno povezavo lahko tudi prekinejo, ukradejo gesla in druge pomembne podatke, tudi recimo digitalna potrdila, vzpostavijo t.i. »stranska vrata«, s pomočjo katerih lahko nepridiprav kadarkoli prevzame nadzor nad našim računalnikom in še mnogo več.

Če se na računalnik namesti škodljiv program je to tako, kot če bi nepridiprav dobesedno sedel za našim računalnikom in imel nad njim popolni nadzor.

Nujna je uporaba protivirusnega programa.

Nekaj vrst spletnih zlorab:

- Škodljiva programska oprema (virusi, trojanski konji, črvi, stranska vrata, beleženje vnosov)
- Škodljive vsebine, ki prizadanejo čustva (spletne strani o nasilju, umorih, spletna mesta za spodbujanje rasizma, anoreksije ali samomorov)
- Nezakonite spletne vsebine (otroška pornografija, rasistični govor, spodbujanje terorizma)
- Ustrahovanje preko spleta
- Kraja in komercializacija osebnih podatkov
- Poskusi vdorov ter vdori v računalniške sisteme
- Oviranje delovanja računalniških sistemov
- Kraja, brisanje in ponarejanje podatkov
- Kraja finančnih sredstev
- Kraja identitete

3.2 Preventivni ukrepi pred spletnimi zlorabami

Nekaj osnovnih nasvetov:

- Imejmo redno posodobljen operacijski sistem.
- Vključimo požarni zid operacijskega sistema.
- Namestimo in redno posodobljajmo protivirusni program.
- Namestimo in redno posodobljajmo »protivohunsko« programsko opremo.
- Obiskujmo le zaupanja vredne spletne strani.
- Izobibajmo se ponudbam, ki so neobičajno poceni ali celo brezplačne, običajno pa so zelo drage.
- Na spletu ne puščajmo po nepotrebnem svojih osebnih podatkov, še posebno ne številke kreditne kartice.
- Nakupujmo le pri zaupanja vrednih spletnih prodajalcih.
- Ne klikajmo na vsiljiva (reklamna) pojavna okna sumljivega izvora.
- Ne obiskujmo pornografskih spletnih strani.
- Ne obiskujmo spletnih strani s piratsko programsko opremo.
- Bodimo pozorni, če se je izgled spletne strani za e-bančništvo od zadnjega obiska kaj spremenila. Če se je, raje pokličimo center za podporo uporabnikom te banke in se informirajmo.

Več si lahko preberemo na naslovih

Safe.si: http://www.safe.si/

Varnostnaspletu.si: http://varnostnaspletu.si/o-projektu

Microsoft Slovenija: http://download.microsoft.com/download/0/9/9/0998d580-4e5c-41c7-ad69-11641dad6c8d/spletna%20varnost-3delni.pdf

3.3 Ukrepanje ob spletni zlorabi

V odvisnosti od ugotovljene spletne zlorabe se odločamo, kako ravnati.

3.3.1 Okužba s škodljivo programsko opremo

Pazlijo preberemo sporočilo protivirusnega programa. Ponavadi nam svetuje čiščenje oz. odpravo škodljive programske opreme. Če tega ne zmore, bo premaknil okuženo datoteko v t.i. **karanteno**. To je poseben zaščiten prostor na trdem disku, katerega varuje protivirusni program.

Bodimo pazljivi, če nam program ponuja brisanje okužene datoteke, vemo pa, da je v njej pomembna vsebina, katere nismo varnostno kopirali. To pomeni, da imamo le to datoteko in z izbrisom bi sami sebi povzročili veliko škodo. V takem primeru raje pokličimo nekoga, ki ima dovolj znanja in izkušenj pri odpravi škodljive programske opreme. Ta oseba bo ocenila, kakšne so možnosti za ohranitev datoteke.

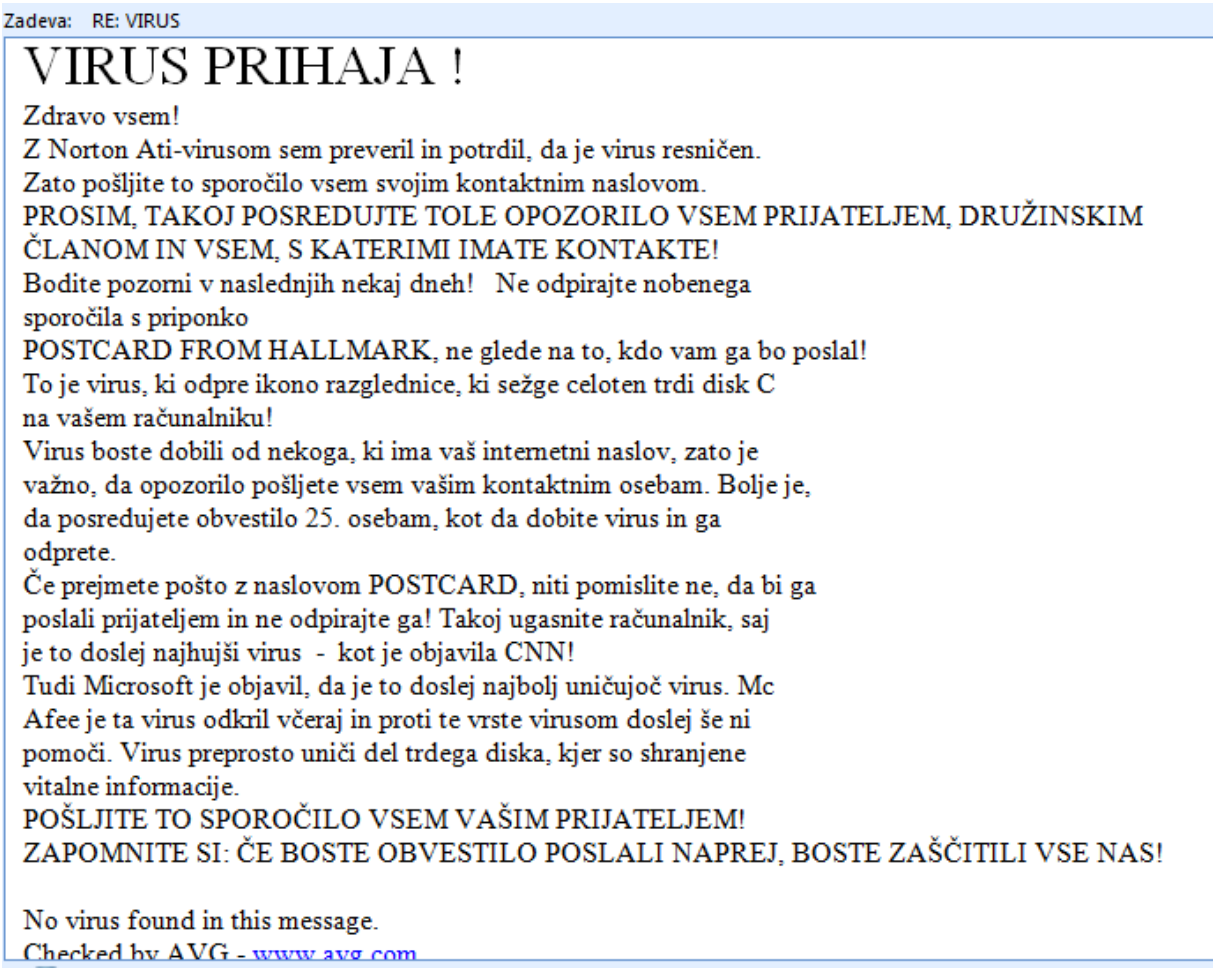
Možni ukrep:

1. Če nismo še nikoli odpravljali okužbe, potem raje pustimo računalnik pri miru in pokličemo strokovnjaka (preskočimo ostale korake)
2. Preglejmo sporočilo protivirusnega programa
3. Če ni bilo možno odstraniti škodljive programske opreme, bo program vprašal za ukrep
4. Če ponudi brisanje le škodljivega programa, potrdimo
5. Če ponudi brisanje datoteke (besedilne), ki je okužena, odklonimo
6. Datoteko (besedilno) raje premaknemo v »karanteno«.
7. Pokličemo strokovnjaka in on bo presodil, kako očistiti datoteko.

3.3.2 Prejem e-pošte s sporočilo o novem virusu

To je neškodljivo sporočilo, osnovni namen je le ustvarjanje nelagodja in branje ter obveščanje drugih. Jemlje čas in po nepotrebnem zaseda prenosne poti ter poštne predale.

Primer je spodaj.



Zadeva: RE: VIRUS

VIRUS PRIHAJA !

Zdravo vsem!
Z Norton Ati-virusom sem preveril in potrdil, da je virus resničen.
Zato pošljite to sporočilo vsem svojim kontaktnim naslovom.
PROSIM, TAKOJ POSREDUJTE TOLE OPOZORILO VSEM PRIJATELJEM, DRUŽINSKIM ČLANOM IN VSEM, S KATERIMI IMATE KONTAKTE!
Bodite pozorni v naslednjih nekaj dneh! Ne odpirajte nobenega sporočila s priponko
POSTCARD FROM HALLMARK, ne glede na to, kdo vam ga bo poslal!
To je virus, ki odpre ikono razglednice, ki sežge celoten trdi disk C na vašem računalniku!
Virus boste dobili od nekoga, ki ima vaš internetni naslov, zato je važno, da opozorilo pošljete vsem vašim kontaktnim osebam. Bolje je, da posredujete obvestilo 25. osebam, kot da dobite virus in ga odprete.
Če prejmete pošto z naslovom POSTCARD, niti pomislite ne, da bi ga poslali prijateljem in ne odpirajte ga! Takoj ugasnite računalnik, saj je to doslej najhujši virus - kot je objavila CNN!
Tudi Microsoft je objavil, da je to doslej najbolj uničujoč virus. Mc Afee je ta virus odkril včeraj in proti te vrste virusom doslej še ni pomoči. Virus preprosto uniči del trdega diska, kjer so shranjene vitalne informacije.
POŠLJITE TO SPOROČILO VSEM VAŠIM PRIJATELJEM!
ZAPOMNITE SI: ČE BOSTE OBVESTILO POSLALI NAPREJ, BOSTE ZAŠČITILI VSE NAS!

No virus found in this message.
Checked by AVG - www.avg.com

Ukrep:

Sporočilo enostavno pobrišemo in ga ne razpošiljamo naokoli. Obvestimo zgolj znanega pošiljatelja, da je tovrstno sporočilo potrebno le ignorirati, ga ne razpošiljati naprej in v bodoče že takoj pobrisati.