O NEKATERIH VRSTAH ZLONAMERNEGA PROGRAMJA

Marjan Tomkiewicz
marjan.tomkiewicz@gov.si

Obvladovanje tveganj je ena temeljnih nalog poslovodnih delavcev - zanj so tudi odgovorni; ta članek želi prispevati njihovi boljši obveščenosti in s tem boljši kakovosti njihovih odločitev. Verjetno najširša splošna nevarnost, ki grozi vsem informacijskim sistemom, so računalniški virusi. To je posebna vrsta zlonamernih programov. Poleg orisa nastanka in delovanja virusov bo v prispevku tudi oris nekaterih doslej avtorju znanih ali predvidljivih vplivov na poslovne in druge organizacijske sisteme v celoti, tveganj v zvezi s tem in ukrepov, ki jih je v zvezi s tem mogoče storiti. Opozorilo: bralci, ki bodo v prispevku iskali napotke, kako virus napisati, se bodo trudili zaman.

0 O računalniških virusih in njihovem nastajanju

Od kod izraz 'virus' v računalništvu? V biologiji 'virus' pomeni - zelo poenostavljeno - biološki pojav, ki ga nekateri teoretiki umeščajo med živo in neživo; virus se more v celici razmnoževati (lastnost živega), a ga je mogoče kristalizirati (največkrat lastnost neživega)[1]. Pri tem celica praviloma propade. Če vzamemo, da je dednostna snov v jedru celice program, po katerem deluje celica, je virus program vrinjenec, ki skupaj z izvirnim programom celice uporabi celične mehanizme za svoje razmnoževanje. Ena vrsta zlonamernih programov je dovolj podobna živim virusom, da so jo poimenovali po njej. Računalniški virus v najširšem smislu je vsak *zlonamerni program* ali njegov del, ki z vednostjo in po načrtu avtorja dela reči, ki jih uporabnik ali kupec ne želi. Računalniški virus v ožjem smislu je izvedljiva koda, ki se vrine v računalniški program ali programe in jih uporabi kot okolje za razmnoževanje. Ob primerjavi s poenostavljenim orisom biološkega virusa ugotovimo podobnosti in razlike. Pri razmnoževanju računalniških virusov računalnik in informacijski sistem ne propadeta vedno, ampak je škoda odvisna od tipa virusa. V medijih in za laično bralstvo se izraz 'računalniški virus' večinoma uporablja nespecifično za vsak zlonamerni program, ki se je sposoben samodejno širiti na kakršen koli način, včasih pa tudi za vsak zlonameren program, tudi če se ne širi samodejno. V nadaljevanju bomo izraz virus uporabljali v pomenu vsakega zlonamernega programa, ki se je sposoben samodejno širiti.

1 Nekatere poti in možnosti širjenja računalniških virusov

1.1 Kje lahko pričakujemo računalniške viruse

Sprva so se virusi širili z izmenjavo programov na disketah in podobnih medijih in so bili dokumenti z besedilom nenevarni, kar je dolgo veljalo tudi za besedilo v elektronski pošti. Zdaj dokumenti z besedilom (na primer MS Word) omogočajo avtomatizacijo, ki se jo da zlorabiti. Vsak tip dokumenta, v katerem je mogoče izdelati kakršnekoli izvedljive postopke tako, da stečejo samodejno brez zavestne odločitve prejemnika (makro, skripti in podobno), je ranljiv za viruse.

Besedilo v elektronski pošti je pogosto iz navadnega besedila (*plain text*), ki je pri marsikaterih uporabnikih za elektronsko pošto privzeto - prešlo v obogateno besedilo (*rich text*), HTML ali podobno. Vsako od teh okolij je med tem časom dobilo možnosti, da ali vsebuje ali naslavlja dejavno vsebino, ki je lahko zlonamerna. Nekateri programi za ravnanje z elektronsko pošto taka sporočila odpirajo tudi samodejno. Verjetno tudi XML omogoča dejavno vsebino. Če jo, je tvegan medij.

1.2 Po katerih poteh nas lahko dosežejo računalniški virusi

Računalniški virusi nas torej lahko dosežejo po prav vsaki poti, po kateri nas lahko dosežejo podatki. Če upoštevamo psihologijo piscev računalniških virusov, lahko domnevamo, da skušajo biti učinkoviti. To pomeni, da bodo po eni plati merili na načine, s katerimi je mogoče doseči 'veliko tržišče', po drugi plati

1 *'Virus' -> 'sluz; strup' (iz lat.) (Slovar tujk, F. Verbinc, l. 1974, stan 758).*

pa na take, pred katerimi je obramba slaba. Trenutno je najpogostejši cilj elektronska izmenjava podatkov po omrežjih - po pošti, okuženih straneh, ki jih obiščete, po klepetalnicah in podobnem. Kaže, da je ranljiva tudi sedanja izvedba izmenjave sporočil (*direct messaging*), to pa velja tudi za posodobitve uporabnikove programske opreme in podobno. Dogajalo se je že, da je bil virus v izvirni programski opremi znanega velikega proizvajalca[2]. Tako je bilo na primer v gonilniku miške in v novi različici programa za dekomprimiranje - prav tedaj, ko je bila prav ta potrebna za namestitev nove različice protivirusnega programa enega znanih izdelovalcev. Več sodobnih virusov daje videz, da gre za Microsoftovo opozorilo o varnostni vrzeli in za njihov popravek zanjo. Premalo pozoren uporabnik ali celo administrator ga utegne sprožiti in to v administratorskem okolju, kjer podeduje administratorjeve pravice tudi virus! Enako pogosto uporabljajo sodobni virusi za širjenje dostop do omrežnih diskov v skupni uporabi in še nekatere druge možnosti, pri katerih za okuženje niti ni potrebno, da uporabnik vedoma sproži okuženi program na napadenem stroju. Vsi 'najuspešnejši' sodobni virusi načrtno uporabljajo več poti širjenja, nekateri tudi v optimiranem zaporedju. Blizu tega (in zato tako zelo 'uspešen') je W32/Nimda. Nikakor pa to ni izčrpen seznam možnih poti.

Verjetno zaradi sodobnih učinkovitejših načinov snovanja in pisanja programov je postalo v zadnjih nekaj letih običajno, da se skuša skoraj vsak računalniški vsiljivec širiti na veliko načinov hkrati, mnogi na vse načine, ki so se v tistem času izkazali za učinkovite.

1.2.1 Priponke elektronske pošte

To je eden najpogostejših načinov širjenja. Vse več oblik (formatov) za izmenjavo podatkov, ki nedavno še niso bili izvedljivi, je v zadnjih nekaj letih postalo izvedljivih. Pred dobrimi desetimi leti je bil *Visual Basic for Applications* standardiziran in poenoten v zbirki MS Office. Kasneje so licenco za vgradnjo v svoja okolja kupili tudi drugi izdelovalci. Hitro je 'postal izvedljiv' HTML, podobno je z XML in z drugimi. V mnogih okoljih je postal izvedljiv *Rich Text Format* (RTF), ki smo ga še pred kratkim lahko priporočali kot sorazmerno varen standarden način izmenjave podatkov. Podobno kot MS imajo svoje rešitve za avtomatizacijo procesov, 'aktivno vsebino' in podobno tudi drugi. Večina takih rešitev ni manj ranljiva od prej navedenih primerov. Manj pogost cilj so večinoma zato, ker je zaradi manj pogoste uporabe manjša verjetnost, da bi bil pri naključnem uporabniku nameščen tisti izdelek in s tem dokument te vrste izvedljiv. Privzete nastavitve MS-izdelkov skrivajo končnice, kot so **.exe, *.vbs* in podobne, kar tudi poučenemu uporabniku oteži zaznavanje nevarnosti. Večina orodij za ravnanje s pošto ima tudi premajhna 'okenca' za prikazovanje imen, tako da se zadnji deli dolgega imena običajno ne prikažejo. To uporabljajo pisci virusov z izbiro imen z več pikami in dolgim zaporedjem presledkov, kot so *'Ljubi moji.txt.vbs'*. V majhnem okencu bi bilo vidno in na videz nenevarno *'Ljubi moji.txt'*. Poleg tega 'dovolj poučenih uporabnikov' ni mnogo. Ob našem zadnjem pregledu nekje na internetu je bilo število splošno znanih končnic nekje okoli 5000, med katerimi je bilo precej tudi večpomenskih.

Priporočali bi uporabo takega orodja za ravnanje s pošto in nastavitev, ki prikaže vse končnice, ki ne odpira samodejno nobene priponke in ki vsebuje 'špartanske' programe za ogled, tako da se pri ogledu ne sproži nič aktivnega. Vendar take rešitve niso atraktivne in večina izdelovalcev verjetno meni, da niso tržno zanimive, tako da jih ni lahko najti ali pa takega delovanja privzete nastavitve ne omogočajo. Trenutno je videti, da bi bilo uporabnikom še najbolje predpisati, kaj smejo sprejemati, vse drugo pa bi morali posredovati pooblaščenim v pregled. Vendar ima lahko tudi tak pristop nezaželene stranske učinke.

1.2.2 Elektronska sporočila, katerih osnovno besedilo ni navadno besedilo

Precej orodij za ravnanje z elektronsko pošto nudi možnost, da se osnovno besedilo pošlje v obliki, ki omogoča poudarjanje besedila z različnimi velikostmi znakov, nacionalnimi znaki kot so pri nas šumniki, s podčrtavanjem in v barvah. Mnoga pogosto uporabljana imajo to tudi za privzeto vrednost ob namestitvi. Taka orodja odpirajo razno dejavno vsebino pogosto neposredno, ne da bi kdo kliknil nanje. MS program Outlook 98 nudi *'Rich Tekst Format* (HTML)', tako kot piše v meniju. Vsaka od obeh oblik je izvedljiva, tako da vsebuje in praviloma sama izvede izvedljive dele. Po privzetih vrednostih se v mnogih okoljih tudi izvedejo v ogledu (*'Preview'*). Ena od možnih izbir te različice programa je, da se kot privzeti program za ravnanje z besedilom v e-pošti uporablja MS Word, ki vsebuje *Visual Basic for Applications* in je s tem izredno ranljiv na viruse. Nobeno običajnih orodij za obravnavanje e-pošte ne prikazuje tipa sporočila ali končnice zlahka.

1.2.3 Pristop na internet

Strani na internetu vsebujejo dejavno vsebino bodisi na istem strežniku bodisi kot kažipot na drug strežnik.

2 *Če (spet) preberete 'licence agreement', boste ugotovili, da se za namestitev programske opreme morate strinjati, da proizvajalec ni odgovoren za nikakršne posledice, povezane z namestitvijo in/ali uporabo take opreme - teoretično morda tudi, če bi vedel, da distribuira okuženo programje.*

Pogoste reference na druge strežnike so bili na primer števci obiskov za merjenje vidnosti reklam, dokler se ta tehnologija ni posodobila. Strežniki, ki ponujajo vsebino na internetu, so hudo ranljive tarče in sodobni virusi in podobni vsiljivci to izrabljajo. Že odpiranje strani, na katero so podtaknjene okužene reči (objekti), z brskalnikom, ki ima običajne nastavitve, lahko zadošča za okuženje uporabnikovega računalnika, če ni zavarovan s programom, ki prepoznava znane virusne vzorce ali že, če so njihovi opisi prestari.

Trenutno najhitrejši znani način okuženja je tisti, pri katerem vsiljivec ne potrebuje človeškega posrednika, ki bi sprožil okuženi program na računalniku - cilju, ampak je zasnovan tako, da sam odkriva ranljive strežnike in se nameša na njih. Ocenjeni potrebni čas za popolno okužbo vseh ranljivih strojev na svetu z vsiljivcem, ki med drugimi uporablja tudi ta način širjenja, je 15 (petnajst) minut. Ta čas je prekratek za večino do sedaj uspešnih vrst obrambnih ukrepov - saj ni časa niti za analizo niti za distribucijo rešitve. Zelo dober prispevek o tem je bil (v času pisanja) na *http://www.cs.berkeley.edu/~nweaver/warhol.html*.

1.2.4 Stari tipi virusov tudi niso nenevarni: zagonski virusi

Privzete vrednosti nastavitev večine sodobnih osebnih računalnikov so še vedno take, da se najprej poskuša zagon z diskete, nato šele z diska. V okolju s takimi nastavitvami je dovolj stara okužena disketa v disketni enoti in izpad električne napetosti, da računalnik le enkrat steče z okužene diskete, pa ga naslednjič na običajni način ni več mogoče pognati. Reševanje vsebine diska pa ni storitev, ki bi jo poceni ponujali v okolici in se pogosto ne splača, še posebej pa ne v primeru, če je bila vsebina diska prej zakodirana. Torej tudi starih vrst virusov pri obrambi ne smemo popolnoma pozabiti.

2 Nekateri neposredni učinki računalniških virusov

2.1 Zamašitev prenosnih poti

Precej virusov, ki se dejavno[3] širijo po omrežjih, lahko povzroči zelo resno poslovno škodo tudi, če ne vsebujejo posebnih mehanizmov za namerno povzročanje škode. Take vrste virus povzroči tolikšno povečanje prometa, da že samo s tem prepreči redno uporabo vira, ki ga uporablja za širjenje. '*Love letter*' in podobni virusi so zamašili poštne strežnike, kar je onemogočilo normalno poslovanje. Zelo verjetno je bilo, da so se v plazu pošte med deset tisoči virusnih sporočil izgubila prava sporočila, kar je tudi povzročilo resne poslovne težave in precejšno poslovno škodo. Če na primer prejemnik ni zaznal naročila in zato ni poslal naročenega, če ni izdal računa, ali prejel sporočila o plačilu in zato neupravičeno na napačen način terjal stranko zaradi neplačila, če zaradi zasutega poštnega strežnika kupci niso mogli izdajati naročil (in ta izpad je šel v deset tisoče in več), potem imamo to lahko za zelo resno poslovno motnjo, ki bi mogla biti za podjetje, ki je od elektronskega poslovanja bistveno odvisno, celo usodna.

'*Code Red*' in podobni pa z iskanjem neokuženih računalnikov v okolju zasitijo promet v dosegljivem okolju mreže in s tem preprečijo, da bi se na tistem območju omrežja računalniki mogli sporazumevati med seboj. V takem primeru so onesposobljene vse aplikacije vrste uporabnik-strežnik, aplikacije z namestitvijo na centralnem strežniku ali vrste *Application Service Provider* (ASP), saj uporabnikov računalnik npr. ne more doseči poštnega strežnika, strežnika s skupno bazo podatkov, strežnika, kjer je nameščena aplikacija. Če bi prodajno mesto ('*point of sale*') za svoje delovanje uporabljalo tako arhitekturo, bi ga to v celoti onesposobilo, kar bi prizadelo tako redno poslovanje kot ugled firme, ki bi se ji to zgodilo (onesposobitev blagajn, bančnih okenc in bankomatov ipd.). Tako škodo povzročijo virusi, ki nimajo nobenega neposrednega uničevalnega mehanizma.

2.2 Sprožilci in izrecno programirane motnje

Mnogi izmed virusov imajo vgrajene raznovrstne sprožilce, ki skušajo ob različnih priložnostih (pogosto naključno, v različnih okoliščinah z različno verjetnostjo) povzročiti motnje ali škodo. Pogosto ima isti virus več sprožilcev, ki so lahko različnih vrst.

Tako eden od v zadnjem času najpogosteje zaznanih virusov *W32/Sircam-A* z verjetnostjo 1/50 sproži postopek, ki skuša zasititi disk 'C:' z datoteko, ki jo spravi v 'koš', ter na 16. oktober z verjetnostjo 1/20 takega, ki skuša izbrisati vse podatke na trdem disku, pri čemer se lahko ta postopek v nekaterih primerih sproži kadarkoli. To ni vse: mehanizem za širjenje virusa po e-pošti uporabi za masko dokumente iz okuženega okolja in more pošiljati zaupne dokumente neupravičenim prejemnikom, kar je v mnogih primerih izredno resna nevarnost. Opis na *http://www.symantec.com/avcenter/venc/data/w32.sircam.worm@mm.html* je eden od podrobnejših opisov na straneh različnih izdelovalcev protivirusnih programov. Drugi, tudi zelo pogost, le malce starejši virus *32/Magistr-A* skuša v uničevalnem postopku izbrisati vse dostopne datoteke na vseh dostopnih diskih,

3 *Pasivno ali trpno širjenje imenujmo, če je za sproženje širjenja potreben uporabnikov poseg, na primer odpiranje pošte ali priponke. Aktivno ali dejavno širjenje je, če program z okuženega računalnika sam išče druge ranljive računalnike.*

lokalnih in omrežnih, ter nastavitve in zagonske postopke v pomnilnikih matične plošče, kar v večini primerov pomeni, da je matično ploščo najceneje nadomestiti z novo, pa tudi pomnilnik, procesor in še kaj, če je stroj le malo starejši.

2.3 Namerno trenutno in namerno postopno uničenje podatkov

V prejšnjem razdelku smo navedli dva primera uničenja podatkov v trenutku in popolnoma. Takemu dogodku smo lahko kos le z obnovo podatkov z varnostne kopije, pri čemer je množica sprememb od časa zadnjega snemanja varnostne kopije praviloma izgubljena (običajno en dan), kar lahko pomeni en dan poslovnih transakcij in zelo resno poslovno škodo (recimo v banki). Še težje pa so posledice postopnega uničevanja podatkov. Pri tem se motnja največkrat ne opazi takoj, tako da je lahko okvarjenih tudi več zaporednih varnostnih kopij. Precej verjetno je, da zlasti v okolju, kjer zaradi zniževanja stroškov ne uporabljajo dovolj kakovostnih naprav, za motnje osumijo nakljućne napake. Tako je obnova podatkov možna le na zelo staro stanje in je izguba vmesnih sprememb še bistveno večja. V mnogo primerih je to verjetno ena najtežjih vrst škode.

2.4 Kvarjenje varnostnih sistemov in njihovih nastavitev

Pogost učinek virusov je načrtno in sistematično odpiranje novih varnostnih vrzeli, najprej tistih, ki jih ima tržna programska oprema skupaj sama (upoštevaje psihologijo uporabnikov), nadaljnji vsiljivci pa izrabljajo tudi tiste, ki so jih pustili njihovi predhodniki. Tako uporablja virus *W32/Nimda* med drugim varnostne vrzeli, ki jih je zapustil predvsem strežniški vsiljivec '*Code Red*' in ki jih prepogosta praksa administratorjev, da uporabljajo isti računalnik in isto prijavo tako za snemanje popravkov z interneta kot za administracijo lokalnega omrežja, še širi.

To je lahko tudi posledica napačnega načina varčevanja uprave: če so administratorji preobremenjeni in nimajo po dveh strojev, bodo tako oni kot njihovi predstojniki hitro ugotovili, da stalno prijavljanje med administrativno, privilegirano in popolnoma običajno registracijo jemlje nepotrebno veliko časa. Zato pričnejo mnogi opravljati vse svoje naloge, tudi nevarne, v istem, pooblaščenem administrativnem okolju. Mehanizem širjenja virusa *W32/Nimda* je zmožen izrabiti tak položaj izjemno dobro, kar pove tudi njegovo ime - '*Nimda*' je obrnjeno '*Admin*', pogosta kratica za administratorja. Dodatna nevarnost te vrste virusov pa je, da njihovi učinki malo premalo pozornemu (ali preslabo opremljenemu ali izurjenemu) opazovalcu sploh niso opazni in so te varnostne vrzeli lahko neopaženo odprte daljši čas.

2.5 Kraja in ponarejanje podatkov

Večina organizacijskih sistemov ima tudi podatke, ki so zaupne narave. Motnja ali onesposobljenje varnostnih sistemov lahko take podatke napravi dostopne. Druga, enako verjetna možnost je, da je že načrtovani cilj motnje varnostnih sistemov sprememba podatkov, ki bo v informacijskih sistemih žrtev ostala neopažena dovolj dolgo, da bo imel vdiralec od tega korist. Ta korist so lahko varnostne vrzeli, ki omogočajo ali olajšujejo naslednje vdore, uporaba žrtvinega računalnika za nadaljnje napade in s tem prikrivanje sledi do povzročitelja, kompromitiranje posameznika ali organizacijskega sistema, ki je lastnik napadenega računalnika. Ni nujno, je pa možno in pogosto, da gre tudi za premoženjske koristi.

2.6 '*Nagajivosti*' ('jokes')

Obstajajo programi, ki na videz ne povzročajo škode. Zatresejo sliko na ekranu, prikažejo ognjemet, prikažejo ali simulirajo '*BSOD*' ('*Blue Screen of the Death*', to je modri ekran, ki se pojavi ob resnih napakah delovanja Windows NT) in podobno. Tudi ti niso čisto neškodljivi. Nekateri med njimi so bili nekaj časa le šale, nato pa naknadno uporabljeni kot krinka, za katero je v ozadju tekel kateri od bolj uničevalnih virusov. Ker *BSOD* običajno pomeni, da je računalnik med ostalim 'zmrznil', ga utegne uporabnik sam pri tovrstni nagajivosti nastavitve resetirati in tako izgubiti vse neshranjene podatke. Zato tudi nagajivosti ne gre jemati preveč zlahka.

2.7 Programerske in druge napake v virusih

Vsak malo večji program ima najmanj eno neodkrito napako. Ko jo odkriješ in odpraviš, še vedno velja isto pravilo. Tako je nekoč učil ing. Nace Nadrah pri pouku programskega jezika COBOL. Seveda obstajajo načini zasnove programov, nadzora in preverjanja izdelkov ipd., ki pomembno zmanjšujejo pogostnost napak. Verjetnost napak je tem večja, če ni niti dovolj znanja niti truda, da jih ne bi bilo. Pri piscih zlonamernih programov v splošnem najbrž ni pričakovati posebne skrbi za kakovost zasnove in programiranja.

Omenili bomo še eno ali dve veliki skupini vzrokov napak. Zlonamerni program je praviloma narejen za določeno okolje. Lahko pa se zgodi, da se izvede v drugem okolju (npr. prejšnja ali naslednja različica okolja, sorodni izdelki - od operacijskega sistema do npr. poslovne zbirke podatkov itd.). V drugačnem okolju zelo pogosto, celo praviloma, ne deluje tako, kot je pisec načrtoval. Podobno je s posledicami napak pri prenosih ali zaradi strojnih napak nasploh.

2.8 Potegavščine

Obstaja mnogo lažnih svaril pred raznovrstnimi grožnjami in niti ta niso neškodljiva. Vrste škode lahko razporedimo na:

- izgubo časa zaradi njih
- nepotreben poštni ipd. promet (učinek kot pri poštnih verigah)
- uporaba potegavščine za njej podoben virus, ki pa ga uporabniki niso jemali resno, dokler ni bilo prepozno
- iz strahu pred 'virusom' uporabnik sam izbriše katerega od programov, ki jih potrebuje na svojem računalniku (primer http:www.virusbtn.com/Hoax/details.html#sulfnbk)

Kako širjenje potegavščin preprečiti? Najenostavneje je, če prejeta svarila vsi posredujejo usposobljeni in pooblaščeni osebi, praviloma administratorju, ta pa

- ukrepa, če je svarilo utemeljeno in je ukrep potreben (lahko, da je grožnja že znana)
- pojasni naravo potegavščine in to posreduje tako tistemu, ki mu je poslal sporočilo v informacijo kot tistim, ki so jo razširjali.

Kako lahko uporabnik sam prepozna potegavščine, če take osebe ni? Večina potegavščin ima nekaj podobnih lastnosti:

- Če govori o groznem virusu, pred katerim ni obrambe, praviloma omenja čase v relativni obliki (včeraj ali podobno). Doslej sem zaznal le eno potegavščino, opisano na primer na *http://www.icsalabs.com/html/communities/antivirus/hoaxes/budfrogs.shtml*, kjer je bil datum 05/13/97 izrecno naveden. V zadnji različici, zaznani 18. 9. 2001, je 'dobronamerni pošiljatelj' ta del seveda izbrisal. Kdo bo verjel v nov, skrajno nevaren virus, za katerega ve malokdo, in za katerega še ni obrambe, čeprav naj bi vsi pošiljali svarilo o njem vsem, ki jih poznajo že od leta 1997?
- Pisci potegavščin se radi sklicujejo na avtoriteto - a tako, da bralec brezuspešno izgublja čas, ko skuša navedbe preveriti.

Če bi jaz napisal sklic na Microsoftovo domačo stran na http://www.microsoft.com, namesto polnega naslova (URL) nekega članka o virusih[4]

http://www.microsoft.com/windowsME/using/computer-health/articles/virusinfo.asp,

bi običajni uporabnik zelo verjetno obupal, preden bi ga našel, četudi dejansko obstaja.[5]

Pri potegavščinah takega članka praviloma ni, uporabnik pa domneva, da ga le ne zna najti.

- Večina potegavščin skuša z različnimi poudarki doseči, da bi jo prejemnik posredoval vsem, ki jih pozna.

3 Nekatere običajne možnosti preventive pred virusi

Žal za zdaj kaže, da je varno računalništvo bodisi neizvedljivo, bodisi v praksi v sedanjih okoliščinah predrago. Poenostavljeno rečeno, če je nekdo pripravljen uporabiti dovolj velika sredstva za napad in če branilec ne razpolaga s potrebnimi sredstvi ali če jih za obrambo ni pripravljen nameniti, je uspešen prodor ne le mogoč, ampak tudi zelo verjeten. Za obrambo pred virusi in drugimi vsiljivci je mogočih več strategij in arhitektur in vsaka med njimi ima svoje močne in šibke plati. Nekatere od njih bomo opisali.

3.1 Nekatere splošne možnosti prepoznavanja

Pri prepoznavanju izhajamo iz tega, kako prepoznavamo človeškega vsiljivca. Med osnovnimi možnostmi je prepoznavanje po videzu ali drugih lastnostih in prepoznavanje po ravnanju. Pri zlonamernih programih je pojav dovolj soroden. Kadar poznamo identiteto človeškega vsiljivca, ga moremo prepoznavati z različnimi biometričnimi postopki, s potrdili (certifikati) ali kombinacijo obojega.

Kadar poznamo neželene postopke, imamo lahko težavo v formaliziranju tega, kaj je nezaželeno in v kakšnem okolju je to nezaželeno, kar je tudi eden bistvenih problemov sodobne zakonodaje. Pojav je še bolj poudarjen v računalniškem okolju in bo tak vse dotlej, dokler bo prevladovala uporaba 'trde logike'. Jasno je še nekaj: če ima nekdo opravka z nekim tipom vsiljivca ali pa z nekim tipom neželene dejavnosti v njegovem informacijskem sistemu prvič (neznan virus, neznana vrsta neželene dejavnosti), ga mora nekako zaznati. Možnosti sta v glavnem prepoznavanje po posledicah ali pa previdnost, tako da uporabnik sumljivo zadevo brez proženja pošlje v analizo. Nedvomno je v večini primerov druga možnost bistveno cenejša. Šele na osnovi analize nastanejo posodobitve programske opreme za varovanje pred zlonamernimi programi, popravki za zapiranje varnostnih lukenj in podobno. Pri tem je bistvena obveščenost in motiviranost ne le administratorjev, ampak še posebej uporabnikov. Tudi za to je potrebno stalno namenjati potrebna sredstva.

3.2 Odkrivanje znanih programskih vsiljivcev na uporabnikovem računalniku

Dobri programi za preprečevanje proženja zlonamernih programov, torej tudi računalniških virusov,

4 *Microsoft je nekoč objavil, da o virusu nikoli ne bo objavil nobenega članka, in da so tako vse reference o virusih na njegove strani potegavščine. Ampak 'nikoli' je dolga doba, v kateri se marsikaj zgodi.*

5 *Ta naslov in prispevek sta obstajala v času pisanja prispevka, ni nujno, da še obstajata v času branja prispevka.*

po nalaganju in pred začetkom teka vsake izvedljive reči na uporabnikovem računalniku pregledajo, ali je na seznamu nezaželenih. Seznam vsiljivcev znanega proizvajalca obsega blizu 70.000 enot. Taka naloga je zahtevna in tudi pri optimalni rešitvi uporabi dovolj virov, da lahko ovira osnovno uporabnost manj zmogljive naprave. Zato je treba pri načrtovanju potrebnih zmogljivosti ta dejavnik upoštevati.

Zelo jasno je tudi, da je treba seznam vsiljivcev stalno dopolnjevati, sicer rešitev zelo hitro postane neuporabna. Posodabljanje programa v celoti, zlasti pa seznama opisov, je proces, ki ga je treba prožiti po potrebi. Pri dobrih izdelkih je to mogoče početi z enega mesta, pogosto tudi na več načinov, mogoč pa je tudi centraliziran nadzor nad varovanjem računalnikov uporabnikov. Možno je urediti tudi popolnoma samodejno proženje posodabljanja za vsak nov opis, a taka rešitev zahteva in zasede zelo velike zmogljivosti. Med drugim povzroči pogost in velik promet na omrežju, starejši računalniki lahko postanejo zato preobremenjeni. Za presojo, kdaj je posodobitev potrebna, je za zdaj še vedno potreben človek - recimo mu administrator protivirusne zaščite.

Enako je mogoče, da postopek iz kakršnega koli vzroka na posameznem stroju ali skupini ne uspe in spet je potreben človek, da odpravi težave, katerih narave praviloma vnaprej ni mogoče predvideti. Od pogostnosti težav in zaupnosti informacijskega okolja pa je odvisno, ali je smotrneje usposobiti lastno osebje, uporabljati storitve zunanjih ponudnikov ali pa s kako kombinacijo navedenega.

3.3 Centralizirano odkrivanje vsiljivcev na poštnem ali podobnem infrastrukturnem strežniku (požarni zid ipd.)

Prednost te rešitve je, da poteka pregled na enem mestu. Pomanjkljivost je, da nihče ne nudi rešitve, ki bi mogla odkrivati nezaželene vzorce v kodiranem prometu. Dobre rešitve na uporabnikovem računalniku pa lahko posežejo vmes potem, ko so podatki že dekodirani.

Smotrno je torej uporabljati tako centralizirano zaščito kot dodatno za očiščenje večine prometa, ni pa sprejemljivo, da bi bila to edina zaščita proti znanim vrstam vsiljivcev.

Razen tega precej takih zaščit nima urejenega dobrega obveščanja pošiljatelja in prejemnika, tako da okužena e-pošta včasih izgine, pa pošiljatelj ne izve, da ni bila vročena, prejemnik pa ne, da mu je bila namenjena.

3.4 Odkrivanje sumljivih načinov obnašanja

Sklepamo torej lahko, da ni nič bolj mogoče vnaprej predvideti vseh možnih načinov nezaželenega ravnanja, kot je možno vnaprej predvideti posamezne vrste vsiljivcev in njihove značilnosti. Zato je tudi tu potrebno posodabljanje, kar pa je manj enostavno kot le dopolnjevanje opisov znanih vsiljivcev. Že prepoznavanje istih dejavnosti je pogosto odvisno od vrste operacijskega sistema, njegove različice, nameščenih paketov popravkov in drugih spremenljivk.

3.5 Zanesljivejša računalniška okolja

Če preberemo licenčno pogodbo običajnih tržnih izdelkov računalniške opreme, bomo lahko tudi presodili, kakšno zanesljivost so izdelovalci pripravljeni jamčiti. Načrtovalci programskih izdelkov ocenjujejo, kaj je trg pripravljen kupiti in videti je, kot da trg za zdaj ni pripravljen plačati zanesljivejših izdelkov. Tako kaže, da je ranljivost sodobnih izdelkov stalnica, kakor je stalnica tudi spremenljivost vsega v življenju. Lahko se zgodi tudi, da bomo mogli izbirati med zanesljivejšimi, na računalniške viruse manj ranljivimi okolji. Vendar če se ne bo zgodilo kaj bistveno novega, ne moremo pričakovati res odpornega okolja.

3.6 Obveščanje uporabnikov - praksa varnega računalništva

Če previden uporabnik pošlje v analizo sumljivo zadevo ne da bi jo sprožil in je resnično nevarna, tako da bi povzročila veliko škodo, je to bistveno cenejše od zaznavanja po posledicah. Po drugi plati pa bi pošiljanje večine prejetih podatkov v analizo ohromilo vsak informacijski sistem, katerega del je izmenjava podatkov. Zato je pomembno, da uporabniki dovolj dobro poznajo znake, ki so osnova za sprejemljivo odločitev med običajnim obravnavanjem prejetega in pošiljanja v analizo. Tukaj ne bom opisoval podrobnosti, ker se stanje na tem področju tako hitro spreminja, da do objave že zastarijo.

Eden od primerov pravil, ki naj bi se jih držali uporabniki, se nahaja na primer na naslovu *http://www.sigov.si/cvi/slo/virus/safehex.htm*. Zelo verjetno pa je bistveno boljša rešitev, če uporabnikov ne učimo prepoznavati nevarnosti, ampak predvsem obvladovati tisto, kar je za njihovo delo običajno. Vse drugo naj gre v analizo in povratna informacija uporabnikom lahko dopolnjuje njihovo poznavanje tega, kar je za njihovo delo običajno. Informacija o dejansko nevarnem pa naj dopolnjuje bazo podatkov z opisi vsiljivcev ponudnika programske opreme za varovanje pred virusi. Podobno lahko ravnamo s podatki, ki si jih samodejno izmenjujejo programi. Zasnujemo jih tako, da samodejno obravnavajo formalno pravilne podatke, torej take, ki ustrezajo formalnemu pravilu. Vse drugo naj nekdo analizira in en tok povratnih informacij iz analize naj izpopolnjuje opis formalno pravilnih podatkov, drugi pa opise neželenih, nevarnih pojavov ter nabor ukrepov v posameznih primerih.

3.7 Šibke točke naštetih vrst zaščite

Okužba z virusi je lahko nepredstavljivo hitra: zadošča le 15 minut za razširitev virusa po vsem svetu. Klasični postopek obrambe po scenariju zaznanje, analiza, načrtovanje odziva, distribucija obrambe, uveljavitev obrambe je torej očitno prepočasen in nezadosten.

Kaže, da potrebni način vsebuje tudi

- uporabo v osnovi zanesljivejših in manj ranljivih izdelkov in
- stalno dejavnost odkrivanja in odpravljanja varnostnih vrzeli, ki bi jih bilo mogoče uporabiti za vdor, tako da v času napada ne bi bilo šibke točke, na katero napadalec meri.

Ni mogoče oceniti, ali je mogoče pričakovati varnejše in zanesljivejše tržne programske izdelke, preveč je možnosti za metuljni efekt. Za aktivno iskanje in odpravljanje lastnih šibkih točk pa so poleg informiranosti odločevalcev potrebna sredstva, za katera je mogoče in verjetno, da jih veliko ciljev preprosto nima.

4 Kaj, če se vseeno zgodi

Praviloma je bolje, če je organizacija na tak dogodek pripravljena. V bistvu je potrebno, da imajo vpleteni predstavo, do česa lahko pride, kako dogodek prepoznati in kako ukrepati ob njem in po njem. Seveda morajo imeti potrebno orodje, znanje in opremo. To pomeni, da mora biti nekomu naloženo, naj grožnje oceni, razmisli o možnih izidih in ukrepih v odgovor nanje. To je lahko notranji ali zunanji izvajalec (posameznik, oddelek ali organizacija). Prednost notranjega izvajalca je običajno boljše poznavanje stanja ter lažja skrb za zaupnost, slabost pa to, da njegovih ugotovitev v organizaciji pogosto ne upoštevajo in v takem položaju pogosto izgubi motivacijo za dobro delo, tudi če jo je imel. Med pomanjkljivostmi zunanjega izvajalca sta slabše poznavanje stanja in problem doseganja zaupnosti, kadar je ta bistven dejavnik za organizacijo, a se priporočila pogosteje uresničijo in konkurenca praviloma izloči preslabe in nemotivirane izvajalce. Naloge s tega področja je torej potrebno nekomu zastaviti in skrbeti, da se izvršujejo in izvršijo.

4.1 Načrti

Potrebni so načrti za stalno preventivno dejavnost, npr. redno izdelavo varnostnih kopij ali podobnega, spremljanje morebitnih svaril za odpovedi strojne opreme, redno spremljanje novih groženj, spremljanje znakov o morebitnih vdorih in podobnih aktivnosti. Potrebni so načrti za primer, ko do katastrofe le pride: kaj storiti, da se škoda ne povečuje? Kaj storiti, da je odpravljena z najmanjšo izgubo zaradi ustavljenega poslovnega procesa? Ali je treba prej vzpostaviti sprejem naročil ali izdajanje računov, če sistemi niso integrirani - kaj je za poslovni sistem v danem trenutku pomembnejše? To pomeni tudi načrte za primere izgube ali nevarnosti izgube podatkov in v primeru nepooblaščenega pristopa do podatkov.

4.2 Preverjanje odločilnih dejavnikov

Ni potrebno, da so vsi načrti formalizirani vedno ali takoj. Pomembno je, da se tekoči del redno izvaja in se pomanjkljivosti zaznavajo. Preizkušeni morajo biti bistveni dejavniki načrta za obnovo po katastrofi, celo več, v nekaterih primerih je nujno, da se določeni dejavniki redno preizkušajo. Taki primeri so lahko spremljanje čitljivosti medija varnostnih kopij ter merjenje in ocena potrebnega časa ponovne vzpostavitve informacijskega sistema iz varnostnih kopij. S tem, ko narašča obseg obravnavanih podatkov, lahko preseže čas shranjevanja ali čas obnovitve vse sprejemljive meje, pa brez preizkusa morda tega nihče ne opazi. Podobno so lahko neopaženo presežene zmogljivosti rezervnih računalniških naprav.

5 Nekateri posredni učinki računalniških virusov

Posredni učinki so med drugim:

- izguba podatkov
- stroški ponovne usposobitve za delo
- zastoj pri delu – čas do odprave neposredne škode
- oslabitev ali onesposobitev varnostnih sistemov
- kaznivost širjenja – vedoma ali iz hude malomarnosti.

Vsakega od teh in drugih podobnih učinkov je potrebno upoštevati. Smotrno ga je ovrednotiti tudi denarno in dobljene vrednosti primerjati s stroški protivirusne zaščite.

6 Postopki in stroški varovanja pred virusi

6.1 Osebje

Za varovanje pred virusi in drugimi vsiljivci je nepoučen, premalo ali pa narobe poučen izvajalec dobesedno nevaren. Podobno je nevaren tudi izvajalec z neprimernimi osebnostnimi lastnostmi:

- nekomunikativen izvajalec: le-ta sčasoma ne bo prejel nobenih sporočil več o nenavadnih dogodkih od uporabnikov;
- lahkomiseln ali v svojo zanesljivost zaverovan izvajalec: je primarni cilj virusov, kakršen je *W32/Nimda*.

Preslaba poučenost je le malce boljša od nepoučenosti. Izvajalec mora imeti pogoste stike s sodobnimi

tehnologijami ter z njimi povezanimi morebitnimi novimi nevarnostmi. Mora jih poznati tudi zato, da ima predstavo, kje so možnosti in mesto za umestitev varnostnih mehanizmov in da lahko na osnovi tega načrtuje in upravlja, na primer mehanizme za posodabljanje opisov in programov programske opreme za prepoznavanje znanih vrst vsiljivcev. Poznati jih mora zato, da ve za možnosti okvar, ki jih povzročajo vsiljivci in za možnosti popravil in drugih načinov odpravljanja posledic. V nasprotnem primeru je v primerjavi s tistimi, ki poskušajo vdore, neizogibno v podrejenem položaju. To pomeni, da je potrebno stalno zagotavljati sredstva za strokovno literaturo, za usposabljanje in druge načine pridobivanja znanja, pa tudi sredstva za testno okolje, v katerem je mogoče preizkusiti postopke, ne da bi ogrozili osnovne poslovne procese. Varčevanje na tem področju je tvegano in se utegne izkazati za drago, za organizacijo lahko tudi usodno drago rešitev. Mogoče je najeti zunanje izvajalce, kar pa ni nujno ceneje. Med drugim jim je treba dati dovoljenja za dostop in pooblastila, ki lahko omogočajo dostop do zaupnih podatkov. Morebitno zlorabo takih dovoljenj je težko nadzirati. Zunanji izvajalci, na katerih izbiro k njim napotenega osebja organizacija, ki uporablja njihovo storitev, praviloma nima vpliva, najbrž niso vedno najboljša rešitev, tudi kadar so morda na prvi pogled najcenejša.

6.2 Nekaj nalog osebja za izvajanje protivirusne zaščite

Delovanje je usmerjeno predvsem v preventivno ukrepanje:

- odkrivati in zapirati varnostne vrzeli,
- ko je čas za to, prožiti posodabljanja programov in opisov protivirusne zaščite,
- spremljati, ali so posodabljanja uspela, in ukrepati, kadar niso,
- prepoznavati neuresničene grožnje, ki so jih posredovali uporabniki v analizo, in dotlej neznane posredovati izdelovalcu (ali izdelovalcem) programov, ki jih organizacija uporablja
- prepoznavati potegavščine in skrbeti, da se nepotrebno ne širijo,
- prepoznavati in spremljati nove in potencialne grožnje,
- preverjati ogroženost zaradi uvajanja novih tehnologij,
- spremljanje in preverjanje ravni kakovosti protivirusne (itd.) programske opreme, ki jo organizacija uporablja, in ocenjevati razloge za morebitno menjavo,
- preverjati primernost uporabljane ali dostopne protivirusne zaščite za novo uvajana okolja (nove različice operacijskih sistemov itn.).

Zgornji seznam obsega glavne priporočljive postopke, nikakor pa ni zaključen, ker se potrebni ukrepi dopolnjujejo in uvajajo glede na stanje tehnologije, nevarnosti, možnosti in potrebe.

V primeru vdora in nastanka škode je treba:

- preprečiti nadaljnjo škodo
- sodelovati pri vzpostavitvi pogojev za nadaljevanje poslovnega procesa
- skrbeti, da pri tem (npr. iz varnostnih kopij) ne pride do ponovnega vdora.

Pri tem štejemo, da so postopki za zanesljivo delovanje informacijskega sistema (z varnostnimi kopijami in podobnim) s to povezana, a ne identična naloga in zato tovrstnih nalog tu ne naštevamo.

6.3 Posebna oprema za protivirusno zaščito

Na razpolago morajo biti računalniki in programi za hitro posodabljanje protivirusnih orodij ter za nadzor nad pravilnostjo in pravočasnostjo izvajanja postopkov. Poleg tega je mora biti na voljo tudi opremo za obči nadzor varnosti. '*Code Red*' se je izdajal s plazom dodatnega prometa po omrežju, ko je iskal nove 'žrtve', kar pa je moral nekdo opazovati z ustrezno opremo, sicer bi ostajal povečani promet neodkrit.

6.4 Licenčnine in stroški posodabljanja protivirusnih programov

Načrtovanje, preverjanje, posodabljanje za trg namenjenih protivirusnih programov, vzdrževanje infrastrukture za distribucijo in vzdrževanje sposobnosti za hiter odziv na kritične položaje niso prav poceni, tudi če ne upoštevamo donosnosti, ki jo od tržno usmerjenih podjetij zahtevajo vlagatelji. Preveč ceneni programi običajno pomenijo, da izdelovalec ne bo mogel doseči kakovosti in primernega odziva pri podpori. Podobno je mogoče, da se cena nekoliko dražjega programa izravna s prihranki zaradi manjše obremenitve administratorjev in s tem njihovega manjšega potrebnega števila. Zavedati se je treba, da obsega menjava orodja za protivirusno zaščito resno testiranje kandidatov, lahko tudi na vsaki od značilnih konfiguracij, kar pomeni precejšnje breme in je to smotrno napraviti le, kadar je nujno.

6.5 Potrebne večje zmogljivosti računalnikov za redno delo

Samodejni pregledi prejetih in oddanih informacij na znane vrste vsiljivcev so obsežna in - kar zadeva računalniško moč - kar precej zahtevna naloga. Če ob načrtovanju zmogljivosti ta dejavnost ni bila upoštevana, zmogljivosti pogosto ne zadoščajo. V takem primeru se včasih sprejme odločitev, da je bolje začasno poslovati z izklopljenimi varnostnimi mehanizmi kot

sploh ne poslovati, nato pa tisti 'začasno' postane dolgo-časno.

V drugih okoljih presodijo povečanje sredstev, potrebnih za nabavo opreme, ki bo kos zaradi varnosti povečanim zahtevam, in se odločijo, da takih sredstev bodisi nimajo, bodisi bodo donosnejša, če jih namenijo za kaj drugega.

Rekli bi lahko, da odločevalci v takih okoliščinah nimajo dobre predstave o tveganjih, ki jih s tem sprejemajo.

6.6 Obveščanje in usposabljanje običajnih uporabnikov

Mnogi uporabniki in njihovi predstojniki so mnenja, da jim o tehnologiji, ki jo uporabljajo, ni treba nič vedeti. Mnenja so, da naj bi bila njihova naloga ukvarjati se predvsem s tem, za kar so plačani in bistveno manj s tem, kako to počno, zlasti kar zadeva računalniško podprto poslovanje. Tak pogled je enako nespameten kakor če bi bančne (ali druge) delavce, ki opravljajo prevoze denarja, usposobili le za prenašanje škatel, vožnjo vozila ter izpolnitev in podpisovanje dokumentov ob prevzemu in oddaji denarja, ne pa tudi za ravnanje v primeru napada. Vzpostaviti in redno vzdrževati je treba pripravljenost vseh uporabnikov (in pri tem so tisti na vrhu piramide pogosto posebno slab zgled) za sodelovanje in komuniciranje z varnostno službo.

7 Sklep

Nevarnost zaradi zlonamernih programov obstaja. S primernimi ukrepi jo je možno bistveno zmanjšati, ne pa vsaj zaenkrat tudi preprečiti. Da bi bili pri preventivi uspešni, morajo sodelovati tako strokovnjaki za področje računalniške varnosti, posebej za protivirusno zaščito, vodilni in vodstveni delavci v informatiki kot tudi drugi upravljavci v organizaciji začenši z generalnimi direktorji. Tovrstna komunikacija je bistveni del sistema varovanja proti opisanim vrstam groženj. Eden od osnovnih namenov tega prispevka je prav omogočiti, da bi se upravljavci lažje sporazumevali z izvajalci varovanja.

8 Viri in reference za nadaljnje branje

1. Varna izmenjava podatkov v slovenski državni upravi - http://www.sigov.si/cvi/slo/virus/safehex.htm
2. Povzetek slovenske zakonodaje, ki zadeva računalništvo in računalniško varnost - http://www.arnes.si/si-cert/kz.htm)
3. http://www.sophos.com/pressoffice/resources/en/
   Computer virus prevention: a primer
   Is virus writing really that bad?
   Active content: friend or foe?
   An introduction to computer viruses
4. Sophos Reference Guide1900/2000, ISBN 0 9513420 8 8
5. Warhol Worms: The Potential for Very Fast Internet Plagues,
   Nicholas C Weaver - http://www.cs.berkeley.edu/~nweaver/warhol.html
6. Symantec Security Response, http://securityresponse.symantec.com/, na dnu strani
   Security Articles
   White Papers
   Virus Encyclopedia
7. F-Secure Press Kit - http://www.datafellows.com/news/press_kit/
   Case studies
   White Papers
8. Virus Bulletin - http://www.virusbtn.com/index.html
   Seznami virusov, ki trenutno krožijo - http://www.virusbtn.com/WildLists/
   Strani ponudnikov protivirusne zaščite - http://www.virusbtn.com/AVLinks/
9. Informacije in rezultati primerjalnih testiranj izdelkov (certification) -http://www.icsalabs.com/

◆

Marjan Tomkiewicz je zaposlen na Statističnem uradu RS, kjer je delal kot programer, sistemski inženir, pri pomoči uporabnikom osebnih računalnikov. V zadnjih letih je njegova prioritetna naloga protivirusna zaščita sistema SURS, poleg posodabljanja omrežne, računalniške in vseh plasti programske opreme.

◆