Viktor Kanižai, master*
OTP banka Srbija a.d. Novi Sad, Novi Sad,
Novi Sad, Republika Srbija

UDK 004.491.22/.492
Stručni članak

ANTIVIRUSNA ZAŠTITA U KORPORATIVNOM OKRUŽENJU

SAŽETAK: Uslov neprekidne poslovne aktivnosti i dobar ugled neke kompanije zahteva pouzdane i uvek dostupne usluge. Danas, to nije moguće postići bez informacionih sistema, jer se upravo na informacionim tehnologijama (nadalje: IT) baziraju neophodne obrade podataka, pružanje usluga raznih vrsta. Međutim, rad tih sistema moguće je narušiti, kako onemogućiti redovan i nesmetan rad, tako i izazvati direktne materijalne štete na samim resursima. IT sistemi su osetljivi, nije lako upravljati njima, ali ih je lako napasti. Upravo iz tih razloga, potrebno je obratiti posebnu pažnju na prirodu poverljivosti, integriteta i dostupnosti podataka kojima taj sistem upravlja, baš kao i na opasnosti koje prete funkcionalnosti i bezbednosti samog sistema. Jedan od najčešćih metoda napada je napad ubacivanjem virusa. Neophodno je stoga posedovanje dobro projektovanog, centralizovanog sistema za antivirusnu zaštitu.

KLJUČNE REČI: virusi, antivirusna zaštita, IT bezbednost, zaštita podataka.

Uvod

Živimo u eri kompjuterizacije, trenutne i automatizovane obrade podataka. I pojedinci i korporacije u svojim svakodnevnim aktivnostima koriste računare i/ili računarske sisteme, kako bi povećali efikasnost, poboljšali produktivnost i smanjili troškove potrebne za izvršavanje datih aktivnosti. IT sistemi su postali deo nas samih.

Nove tehnologije, međutim, nose i nove metode napada. Primarni cilj više nije da se fizički ukrade računarski resurs, već podaci na njemu. Računari, serveri, laptopovi se danas već lako zamenjuju, ali podaci na njima su gotovo nezamenljivi. Najjednostavniji i najčešći oblik napada na bezbednost IT-a i podataka je uz pomoć eksploatacije računarskih virusa.

Računarski virus je zlonameran softver koji za cilj ima da uništi, ukrade, sakrije, modifikuje podatke pohranjene na računaru. Razlikuju za mnogi tipovi virusa, kao što su: crvi, tkzv. „malware“, tkzv. „spyware“, tkzv. „scareware“, trojanci, Botnet mreže, itd. Svaka vrsta nosi određene, posebne rizike po bezbednosti IT sistema i podataka pohranjenih u njemu, od nekih je odbrana laka, ali u nekim slučajevima zaštita sistema i podataka nije trivijalna. Zbog toga, neophodna je sveobuhvatna, dobro projektovana zaštita od virusa.

1. Virusi i zaštita od virusa

Svaki zlonameran program ima za cilj da „zarazi“ fajlove na računaru, računarskoj mreži, serveru, i zatim sam sebi pravi kopije. Neki narušavaju integritet podataka, nekima je krajnji cilj krađa istih, ili pak uništavanje. Postoje i virusi koji sakrivaju podatke na računaru i traže uplatu u određenom iznosu kako bi te podatke povratili korisniku.

Virusi obično prevare korisnika da on preduzme mere zahvaljujući kojima će se virus postaviti na računar – npr. klikom na priložen link, daunlodovanjem određenog fajla, posetom nekoj internet stranici, itd. Virus se može pojaviti na računaru i otvaranjem atačmenta u e-mailu nepouzdanog izvora, surfovanjem na internetu, priključivanjem prenosivog medija sa podacima,

* kanizsai.viktor@gmail.com

itd. Nakon što se virus postavio na računar, on se dalje širi bez dodatne interakcije sa korisnikom – bilo preko računarske mreže ili prenosivim medijima sa podacima.

1.1. Pretnje prema tipovima virusa

„Malware“, tj. malver, predstavlja skraćenicu od termina „zlonamerni softver“ (en. Malicious software), i on je softver koji se koristi ili je stvoren da ometa rad računara, prikupi osetljive podatke, ili dobije pristup računarskim sistemima. On se može pojaviti u obliku koda, skripti, aktivnog sadržaja i drugog softvera, programa. Malver je opšti termin koji se koristi, a koji se odnosi na različite oblike neželjenog, neprijateljskog ili nametljivog softvera. Malver obuhvata računarske viruse, crve, trojance, advere i druge zlonamerne programe.

Računarski crv je samostalan zlonamerni računarski program koji se replicira, kako bi se proširio na druge računare. Za širenje često koristi računarsku mrežu, oslanjajući se na bezbednosne propuste na datim računarima. Za razliku od računarskih virusa, crvi ne moraju da se inkorporijaju u neki postojeći, legalan program. Crvi skoro uvek izazivaju barem neku minimalnu štetu na mreži, čak i ako je to samo konzumiranje propusnog opsega, dok virusi gotovo uvek pokvare ili modifikuju fajlove na datim računarima.

„Spyware“, tj. spajver je tip malvera koji je instaliran na računarima da bi prikupljao informacije o korisnicima bez njihovog znanja. Prisustvo spajvera je obično sakriveno od korisnika, i teško se otkriva. Spajver prati računarske aktivnosti korisnika, a neke funkcije spajvera mogu se proširiti i izvan opsega jednostavnog praćenja. Spajver može da prikuplja skoro svaku vrstu podataka, uključujući i lične podatke, kao i navike surfovanja po internetu, logovanja korisnika po raznim korisničkim nalozima, i informacije o bankarskim računima, kreditnim karticama.

„Scareware“, tj. skerver obuhvata nekoliko klasa prevara softvera sa zlonamernim kodom, koje su prodate potrošačima preko određenih neetičkih marketinških praksi. Pristup za prevaru koristi socijalni inženjering da bi izazvao šok, anksioznost, ili percepciju pretnje, uglavnom usmeren prema bezazlenom korisniku. Neki oblici spajvera i spemova takođe koriste skerver taktiku. Taktika koju kriminalci često koriste podrazumeva ubeđivanje korisnika da im je virus zarazio računar, a zatim ukazuje se na to da treba da preuzmu (i plate „licencu“) lažni antivirus da bi navodne zaraze računarskim virusima uklonili. Obično su navodni virusi u potpunosti izmišljeni, a softver koji se preuzima i plaća je nefunkcionalan i sam je malver. Drugim rečima, korisnika prvo uplaše da mu je računar zaražen virusima i odmah mu nude i rešenje. Međutim, to rešenje je zapravo stvarni virus i korisnik misleći da instalira antivirusni softver instalira virus.

Trojanski konj, ili trojanac, jeste vrsta malvera koji se maskira kao da je legitimna datoteka ili koristan program, ali čija je istinska svrha, na primer, da omogući hakeru neovlašćen pristup računaru. Trojanci se ne inkorporiraju u druge fajlove kao što to čine računarski virusi. Trojanci mogu da kradu podatke ili nanesu štete računarskim sistemima. Trojanci koriste razne opcije daunlodovanja preko interneta, onlajn igrice ili internet aplikacije da bi postigli cilj zaraze nekog od računara. Termin trojanac nastao je iz priče o Trojanskom konju u grčkoj mitologiji, jer trojanci koriste formu „socijalnog inženjeringa“, predstavljajući sebe kao bezopasne, korisne poklone, kako bi ubedili žrtve da ih instaliraju na svojim računarima.

Botnet mreža je kolekcija povezanih računara preko interneta čije zaštite su narušene i njihova kontrola je ustupljena zlonamernim trećim licima. Svaki takav kompromitovani računar, poznat kao „bot“, nastaje kada se računar zarazi sa određenim malverom. Onaj ko upravlja botnet mrežom u stanju je da usmeri aktivnosti ovih kompromitovanih računara preko komunikacionih kanala mrežnih protokola, kao što su npr. IRC (Internet Relay Chat) i HTTP (Hypertext Transfer Protocol). Najčešće se botnet mreže koriste za napade tipa DDOS (Distributed Denial of Service), koji za cilj imaju preopterećenje napadnutog računara, koji upravo zbog tog preopterećenja odbija da izvrši usluge koje su predviđene njegovim radom. Namera ovakvih napada je, s jedne strane pokazivanje moći, a sa druge iznuda novca – „Plati ako želiš da prekinemo napad i vratimo ti mogućnost nesmetanog rada“. Danas se botnet mreže mogu već i iznajmiti, što znači da ne treba biti nikakav ekspert za računare, samo se uplati određeni iznos za koji se za uzvrat dobija pristup konzoli koja upravlja zaraženim računarima.

Na slici koja sledi prikazan je trenutak detektovanih aktivnih virusnih napada na mapi, koja se može pratiti preko tkzv. projekta „Honeynet“. Tačkice obeležavaju napade. Lako se može uočiti da je trenutno žarište u Centralnoj Evropi.

Slika 1. Geografska raspodela napada

Slika 2. prikazuje region okoline Republike Srbije. Vidi se da u datom trenutku posmatranja mape nisu zabeleženi napadi u Srbiji, ali to ne znači da je Srbija neaktivna po ovom pitanju, već da je to takav slučaj za posmatrani trenutak.

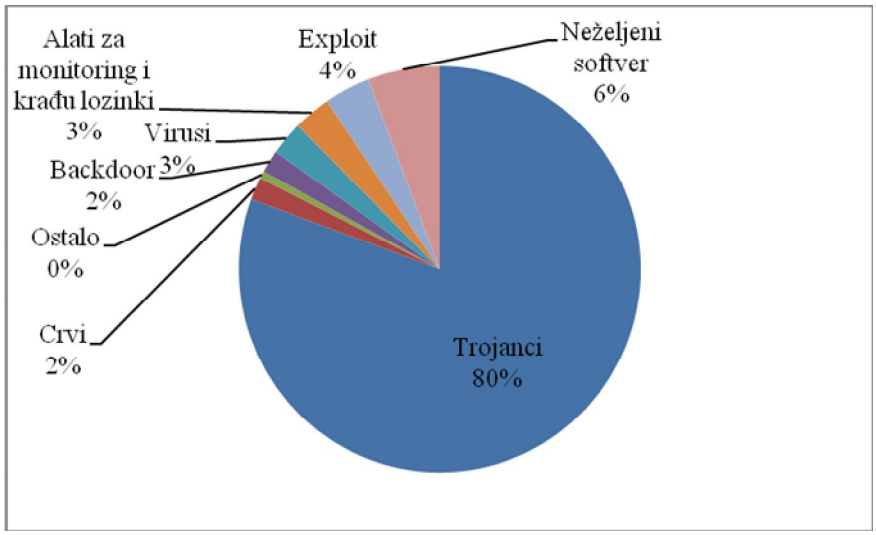
Slika 2. Mapa napada u okruženju

Tabela koja sledi prikazuje kvartalne trendove za prvih 10 malvera otkrivenih antivirusnom zaštitom Majkrosofta.

Tabela 1. 10 najčešćih malvera po kvartalima

R.br.	Tip	Kategorija	3Q11	4Q11	1Q12	2Q12
1	Win32/Keygen	Neželjen softver	3,424,213	4,187,586	4,775,464	4,775,243
2	Win32/Autorun	Crvi	3,292,378	3,438,745	3,316,107	3,510,816
3	JS/Pornpop	Adver	3,944,489	3,906,625	3,994,634	2,838,713
4	JS/IframeRef	Trojanci	1,612,828	1,191,929	952,111	2,493,830
5	Win32/Sality	Virusi	1,728,966	1,951,118	2,101,968	2,097,663
6	Win32/Hotbar	Adver	2,870,465	2,226,173	3,008,677	2,073,789
7	Win32/Dorkbot	Crvi	1,107,300	1,713,962	1,883,642	2,055,244
8	ASX/Wimad	Trojanci	748,716	1,825,291	1,487,334	1,890,806
9	Win2/Obfuscator	Neželjen softver	1,521,959	1,623,137	1,393,148	1,851,304
10	Win32/FakePAV	Trojanci	128,045	28,694	59,166	1,833,434

Slika 3 pokazuje kategorije zlonamernih softvera pronađenih i blokiranih na internet sajtovima od strane SmartScreen Filter u prvoj polovini 2012. godine.



Slika 3. Kategorije malvera na sajtovima u ½ 2012.

Iz navednih činjenica jasno se može zaključiti da virusi korisnicima, kompanijama mogu naneti ozbiljne direktne i indirektne materijalne, a takođe i reputacione štete. Upravo zbog toga neophodna je implementacija dobro projektovanog i redovno održavanog antivirusnog sistema.

1.2. Antivirusna zaštita

Neminovno se postavlja pitanje: Kako se zaštititi? Ukratko rečeno, antivirusna zaštita treba da je višeslojna. Ona mora biti tehnički realizovana – sistem antivirusne zaštite, redovno ažuriranje softvera i operativnog sistema na računarima, itd., ali su potrebni i dobro obučeni ljudi

– pažljiva upotreba interneta i sistema elektronske pošte, kao i prenosivih medija sa podacima. Jedno bez drugog samo delimično rešava problem.

1.2.1. Sistem antivirusne zaštite

Sistem antivirusne zaštite treba da bude jedinstven u kompaniji. Ne sme se dozvoliti da paralelno bude prisutno više sistema za zaštitu od virusa, jer je tada upravljanje istim vrlo složen posao. Takođe, u takvom slučaju se mogu pojaviti i neprevidivi zastoji u nesmetanom radu računara i celokupnog IT sistema – konflikti raznih tipova.

Antivirusna zaštita treba da je centralizovana. Ona mora obuhvatiti sve računare date kompanije, a sistemom treba da se upravlja „sa jednog mesta“. Centralizovano se upravlja instalacijom antivirusnog softvera na sve radne stanice, tj. instalacija se ne odvija „ručno“. To s jedne strane znači uštedu vremena, a sa druge osigurava da će zaista svi računari biti uključeni u sistem antivirusne zaštite – isključuje se ljudski faktor rizika usled kojeg bi neki računari mogli biti „zaboravljeni“. Pored instalacije, centralno se vrši i monitoring rada samog sistema, kao i događaja vezanih za računarske viruse.

U datoj kompaniji mora da bude određeno lice ili organizaciona jedinica koja je odgovorna za planiranje, implementaciju i upravljanje antivirusnom zaštitom. Nije dobro ako se ova zaštita prepusti onima koji u svom svakodnevnom radu imaju i sasvim drugačija zaduženja koja nisu striktno vezana za bezbednost IT i zaštitu podataka.

Neophodna je izrada i usvajanje interne normativne regulative koja propisuje zadatke i zaduženja vezanih za antivirusnu zaštitu, a koja se odnosi na sve zaposlene. U toj regulativi potrebno je jasno naznačiti sva načela zaštite u datoj kompaniji, i to tako da svim zaposlenima bude jasna srvha i primena zaštite, kao i zaduženja koja iz nje proizilaze. Treba da im je naglašeno da je strogo zabranjeno samovoljno deaktiviranje sistema zaštite instaliranog na svom računaru, a ukoliko je moguće to treba i tehnički onemogućiti.

Nakon instalacije centralizovanog sistema za antivirusnu zaštitu, istu je potrebno ispravno konfigurisati. Posebno se podešava rad centralnog servera zaštite, a posebno se kreiraju konfiguracije vezane za klijentske računare (klijentske u smislu antivirusne zaštite). Mora da se osigura redovno ažuriranje baze pomoću kojeg se pronalaze virusi. Ako ova baza nije ažurna sistem neće blagovremeno reagovati na nove viruse. Najbolja je praksa da se centralni server ažurira preko interneta minimum jednom dnevno, a klijentski računari antivirusne zaštite preko interne mreže date kompanije preuzimajući ažurne definicije od centralnog servera. Na taj način smanjuje se opterećenje saobraćaja prema internetu, a ujedno se osigurava i da svi računari imaju jedinstvenu definiciju virusa, tj. bazu. Homogenost kod antivirusne zaštite je ključna, jer smanjuje mogućnosti neprevidivog rada IT sistema usled raznih mogućih konflikata zbog neuskladivosti softverskih rešenja i baza podataka – bilo virusne ili korisničke.

Pored ažurnosti baza virusnih definicija, od ključnog je značaja i redovno skeniranje na viruse. Skeniranje podrazumeva pretragu koju vrši antivirusni softver na računaru da bi uporednom proverom preko svoje baze definicije virusa utvrdio postojanje/nepostojanje virusa na datom računaru. Skeniranje mora biti redovno, najmanje nedeljno jednom, i da takođe pokriva sve računare. Poželjno je takođe, da se pri svakom uključivanju računara izvrši „brzo“ skeniranje (ne skenira se ceo hard disk, već samo kritična „mesta“), jer se na taj način otkrivaju virusi koji

se pokreću pokretanjem samog računara. Pored tkzv. „startap“ skeniranja, preporučuje se brzo skeniranje i nakon izvršenog ažuriranja virusnih definicija. Razlog ovome jeste da se nakon ažuriranja pojavljuju nove definicije virusa, tj. sistem će biti u mogućnosti da prepoznaje najnovije viruse koje do tada nije mogao da detektuje. Računar je mogao biti zaražen virusom za koji antivirusni softver tek kasnije „sazna“, i stoga je vrlo preporučljivo da se nakon ažuriranja virusnih definicija izvrši jedno brzo skeniranje. Skeniranje treba da je obavezno i pri umetanju prenosivog medija sa podacima u dati računar. Najveći izvori zaraza jesu internet i prenosive memorije, pa je upravo zbog toga neophodno da se na ove aktivnosti obrati posebna pažnja.

Pored napred navedenih podešavanja potreban je i konstantan monitoring ispravnog rada samog sistema. Neretko se u praksi dešava da npr. iako je ažuriranje adekvatno podešeno, ono se ipak ne izvrši na predviđen način. Ili, još jedan primer iz prakse, instalacija na klijentski računar se ne izvrši na planiran i željen način. U svim slučajevima kada se uoči odstupanje od podešenog rada, neophodna je „ručna“ intervencija, što često i nije lak zadatak. Analiziraju se logovi, interakcije sa drugim sistemima, mrežni saobraćaj, itd. i na osnovu toga preduzimaju se mere za oktlanjanje propusta, kao i osmišljavanja rešenja kako se ubuduće takvi događaji ne bi dešavali.

1.2.2. Dopunska tehnička rešenja

1.2.3.

Pored implementacije i ispravnog rada dobro projektovanog, centralizovanog sistema antivirusne zaštite, postoje i druga tehnička rešenja koja dodatno osiguravaju bezbednost IT i zaštitu podataka sa aspekta zaštite od virusa.

Uvek je potrebno poći od toga na koji se način virusi postavljaju i šire. Prvo, poznato je da virusi često koriste slabosti, ranjivosti operativnog sistema ili drugih, legalnih programa instaliranih na računaru. Zbog toga, neophodno je da se osigura redovno ažuriranje tih programa i samog operativnog sistema, jer se kroz ta ažuriranja otklanjaju moguća mesta napada. Virusi najčešće „dolaze“ preko interneta (surfovanjem ili preko sistema elektronske pošte), ili preko prenosivog medija sa podacima (USB memorije). Iz tih razloga, neophodno je uspostavljanje antivirusne zaštite i na mrežni saobraćaj kompanije prema internetu, koji će da filtrira mrežnu komunikaciju i odbija pakete podataka za koji utvrdi da predstavljaju virus, ili deo virusa. Sa aspekta bezbednosti, najbolje rešenje je ono gde su interna mreža kompanije i internet potpuno odvojene mreže, tj. računar koji je priključen na internu mrežu nema uopšte pristup internetu.

Takođe, potrebno je implementirati sistem zaštite i na e-mail server kompanije, pomoću kojeg će se vršiti skeniranje svih e-mailova i onemogućiti da korisnik dobije e-mail koji u sebi sadrži virus.

Jedan od vrlo efikasnih metoda za suzbijanje širenja virusa u kompaniji jeste ograničavanje upotrebe USB memorije. Retko ko vodi računa o tome u koji i kakav računar umeće svoju USB memoriju i zbog toga se često dešava da korisnik iz nepažnje „pokupi“ mnoštvo virusa na svoj USB. Takav USB kada umetne u svoj računar, zaraza virusima je gotovo neminovna, zavisno od kvaliteta antivirusne zaštite. Zbog ovih razloga, najbolja praksa pokazuje da se broj virusa u datoj kompaniji može drastično smanjiti onemogućavanjem, tj. ograničavanjem upotrebe USB memorije.

1.2.4. Obuka korisnika

Tehnička rešenja sama po sebi nisu dovoljna u borbi protiv virusa. Sistem može biti osmišljen kao neprobojan, ali rizik od ljudskog faktora je najveći. Antivirusni sistem može biti ispravno implementiran i konfigurisan, ali je krajnji korisnik taj koji svojim aktivnostima može da izazove nepredvidive događaje.

Svi zaposleni moraju biti upoznati sa načinom funkcionisanja antivirusne zaštite. Neophodno je da budu svesni da su i oni činioci celokupnog sistema zaštite. Treba da znaju kako da upravljaju antivirusnim softverom na svom računaru – kako izgleda ikonica kada je sve u redu, a kako kada postoji problem, kako se vrši ručno skeniranje, itd.

Takođe, treba da znaju i „pravila ponašanja“, tj. da moraju biti pažljivi pri upotrebi samog računara, surfovanja internetom, upotrebi sistema elektronske pošte, upotrebi prenosivog medija sa podacima, itd. Treba da su svesni rizika koji prete napadima virusa, i kako ih smanjiti ili eliminisati u potpunosti.

1.2.5. Pravna regulativa

Krivični zakonik Republike Srbije (nadalje: KZRS) u članu 300. reguliše slučajeve pravljenja i unošenja računarskih virusa, što predstavlja još jedan vid – zakonski – zaštite od virusa. Po KZRS, ko napravi računarski virus u nameri njegovog unošenja u tuđ računar ili računarsku mrežu, kazniće se novčanom kaznom ili zatvorom do šest meseci, a ko unese računarski virus u tuđ računar ili računarsku mrežu i time prouzrokuje štetu, kazniće se novčanom kaznom ili zatvorom do dve godine. Uređaj i sredstva kojima je učinjeno krivično delo oduzeće se.

2. Represivne mere zaštite

U sklopu celokupnog sistema za zaštitu od virusa, potrebno je dobro definisati mere koje je potrebno preduzeti u slučaju otkrivanja virusa u IT sistemu. Pre toga, naravno, neophodno je konstantno praćenje svih logova i događaja koji su vezani za otkrivanje virusa, centralno i centralizovano. Sistem treba podesiti tako da u slučaju otkrivanja virusa na bilo kom računaru ili u komunikaciji između dva ili više računara, odmah pošalje upozorenje nadležnim licima u kompaniji, a pored toga i da signalizira postojanje virusa i na zaraženom klijentskom računaru.

Treba jasno definisati ko i šta preduzima u ovakvim slučajevima kako bi se najpre zaustavilo širenje zaraze, a potom ona i otklonila sa datog računara ili više njih. Potrebno je da i korisnik bude svestan da mu je računar zaražen, da on sam preduzme sve mere u njegovoj nadležnosti (ako je npr. zaraza putem USB memorije, tada je mora odmah izvaditi) i da neodložno obavesti nadležna lica o postojanju zaraze i preduzetim merama, kako bi stručna lica mogla što hitnije da reše problem.

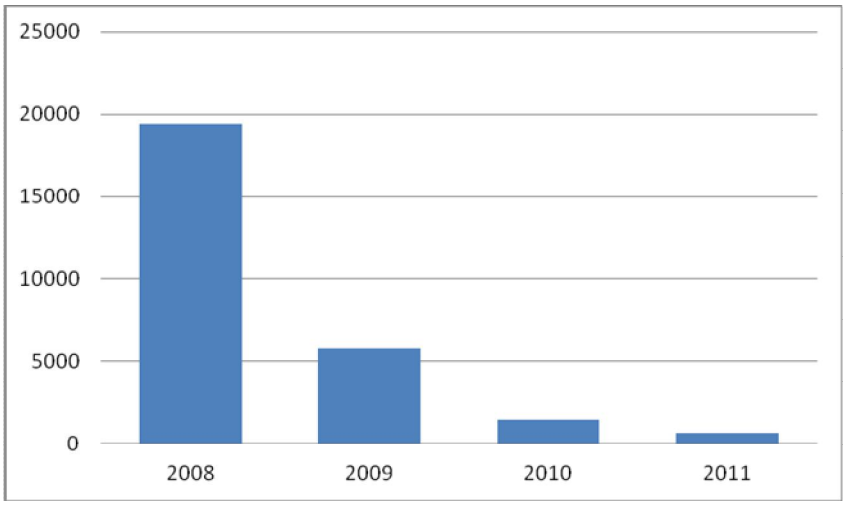
Antivirusni sistem u većini slučajeva – ako je samo tehničko rešenje dobro osmišljeno i izabrano – sam odbije virusne napade, ali se neretko dešava da je neophodna ručna intervencija. Ovakve intervencije, zavisno od dubine zaraze i stručnosti nadležnih lica u kompaniji, mogu da

potraju od nekoliko minuta do nekoliko dana (reinstalacija i rekonfiguracija većeg broja računara).

Nakon otklanjanja virusa, potrebno je izvršiti analize o događaju i utvrditi potrebne mere kako se slični događaji u budućnosti ne bi dešavali, ili da bi se njihov broj barem smanjio na minimalne vrednosti.

3. Odabir tehničkog rešenja

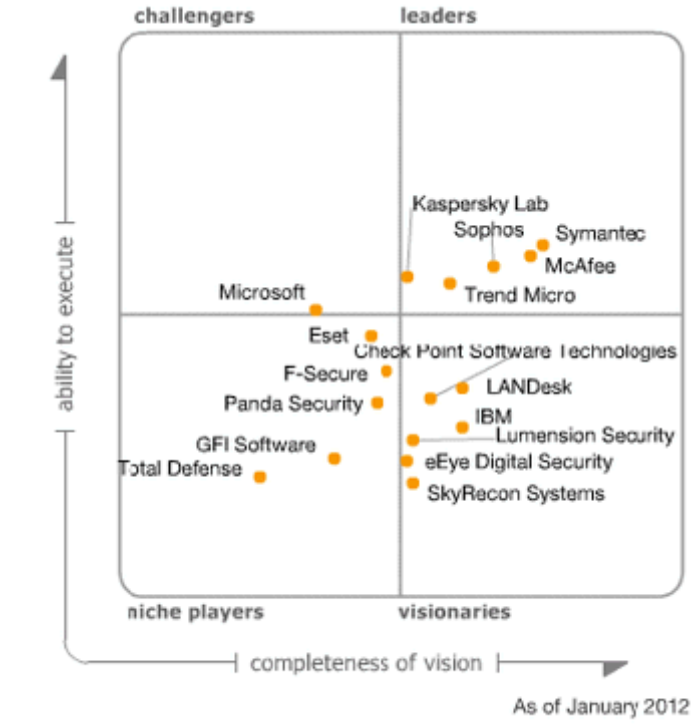
Pri razmatranju sistema antivirusne zaštite neminovno se postavlja pitanje: Kako izabrati pravi? Pravog recepta nema, svaki sistem – korisnički i antivirusni –specifičan je, sam za sebe. Pri razmatranju treba uzeti u obzir sve navedeno u ovom radu, kao i ranija iskustva. Takođe, vrlo je bitno da se izabere takvo rešenje koje neće ugroziti nesmetan rad kompanije – antivirus koji preopterećuje računare i servere, jeste da će možda pružiti dobru zaštitu, ali će i onemogućiti obradu podataka i pružanje usluga date kompanije. Drugim rečima, potrebno je naći rešenje koje je „izbalansirano“ između zaštite i nesmetanog rada. Slika 4. pokazuje broj oktrivenih virusa u jednoj banci u Republici Srbiji, u periodu od 2008-2011. godine.



Slika 4. Broj virusa opada

U toj banci su 2008. godine implementirali novi antivirusni sistem, što je za rezultat imalo da je novi sistem pronašao sve viruse na računarima, i one koje staro rešenje nije pronašlo. Virusi su obrisani i zato je od te godine njihov broj sve manji. Takođe, sledeće godine je započeta intenzivna obuka zaposlenih iz oblasti zaštite podataka, a pored toga implementirane su i dodatne tehničke mere zaštite, što za celokupan rezultat ima drastično smanjenje broja virusa u IT sistemu banke.

Na kraju, sledi slika, tkzv. magični kvadrant Gartnera (svetsko priznata kompanija za istraživanje i konsalting u polju IT-a) za januar 2012. godine, vezan za zaštitu računara, pri čemu su uzete u obzir sledeće usluge rešenja: antivirus, fajervol, sprečavanja upada, kontrola portova i uređaja, enkripcija fajlova i diskova, sprečavanje odliva podataka i kontrola aplikacija.



Source: Gartner (January 2012)

Slika 5. Najbolja tehnička rešenja zaštite računara po Gartneru

Zaključak

Antivirusna zaštita mora biti višeslojna, dobro projektovana, ažurna, jedinstvena i centralizovana. Za njenim upravljanje neophodna su stručno obučena lica. Pored samog sistema antivirusne zaštite postoje i druga, dodatna tehnička rešenja koja osiguravaju veći stepen zaštite. Iz celokupnog sistema zaštite ne treba izuzeti zaposlene u kompaniji, tj. korisnike, koji se redovno moraju obučavati o osnovnim principima antivirusne zaštite, kao i o potrebnim merama za preduzimanje u slučaju oktrivanja virusa na njihovom računaru. Ne postoji 100 % bezbedan sistem, ali se ovom rezultatu može vrlo usko približiti. Ne treba zaboraviti, sistem antivirusne zaštite mora uvek da pobedi, dok je virusu dovoljno samo jednom dapobedi.

LITERATURA

[1] Krivični zakonik Republike Srbije, Sl. glasnik RS, br. 85/2005, 88/2005 − ispr., 107/2005 − ispr., 72/2009 i 111/2009.

[2] Magic Quadrant for Endpoint Protection Platforms, Gartner, http://www.gartner.com/technology/reprints.do?id=1-18TSH6H&ct=120117&st=sb, poslednji put pristupano 11. 11. 2012.

[3] Microsoft Security Intelligence Report Volume 13, http://www.microsoft.com/.

[4] The Honeynet Project, www.honeynet.org, poslednji put pristupano 11. 11. 2012.

[5] Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Main_Page.

Viktor Kanižai, M. A.

ANTIVIRUS PROTECTION IN CORPORATE ENVIRONMENTS

Summary

The condition of continuous business activities and good reputation of a company requires reliable and always available services. Today, this is not possible without information systems, because the required data processing and providing services of various kinds is based on the information technology (hereafter IT). However, it is possible to disrupt the operation of these systems, disable both the regular and smooth operation, and cause direct damage to the resource itself. IT systems are vulnerable, they are not easy to manage, but they are easy to attack. For these reasons, it is necessary to pay particular attention to the nature of data confidentiality, integrity and availability for systems that manage these data, as well as the dangers that threaten the security and functionality of the system. One common method of attack is an attack by inserting a virus. It is necessary, therefore, the possession of well-designed, centralized system for antivirus protection.

Key words: viruses, antivirus protection, IT security, data protection.