I. Mrđen*

SIGURNOST UMREŽENIH RAČUNALA POD OPERATIVNIM SUSTAVOM WINDOWS

UDK 004.451:004.7]:343.533
PRIMLJENO: 1.2.2006.
PRIHVAĆENO: 17.3.2006.

SAŽETAK: U vrijeme kada je internet nastajao kao eksperimentalna mreža njegovi programeri sigurnosti umreženih računala nisu predvidjeli mogućnost zlouporabe računalnih sustava. Stoga nisu dovoljno pozornosti posvetili definiranju i uvođenju računalne sigurnosti, kako za pojedince, tako i za institucije koje se koriste umreženim računalnim programima, te za cijelo društvo kojemu ta umrežena računala mogu predstavljati opasnost. Uvažavajući elemente rizika u tehnološkom smislu, te razvoj osobnih računalnih programa Microsofta, proizvođača programa sigurnosti umreženih računala pojavila se potreba da se ti isti računalni programi i adekvatno zaštite od nepoželjnih osoba i skupina koji bi željeli zloupotrijebiti njihove informatičke podatke. Tako je Microsoft u svojem programu postavio osnovne postavke za pohranu, slanje, te rad i zaštitu u mrežnom okruženju Windows od nepoželjnih upada neovlaštenih osoba, tj. hakera.

Ključne riječi: *sigurnost, umrežena računala, hakeri, mamac*

Proučivši obrambenu zaštitnu funkciju sigurnosti u tehnološkom smislu umreženih računala pod operativnim sustavom Windows došlo se do spoznaje da razvojem tehničkih mogućnosti računala postoji potreba da se ta ista umrežena računala istovremeno i zaštite na najbolji, najsigurniji i najsuvremeniji tehnički način.

Ne mogu se samo tehničkim rješenjima polučiti značajniji rezultati kao ni proučiti i doseći sve dimenzije rizika. Tako su se tehničkim i usko ekonomskim shvaćanjem obuhvaćali samo neki elementi rizika, a izostajale su antropološke, psihološke i socijalne dimenzije. Socijalna teorija rizika kao kompleksno zahvaćanje u cjelini problematike, koji rizici u suvremenom svijetu stavljaju gotovo pred svakog člana zajednice, jest nužnost koja mora nadići mnogobrojna ograničenja usko tehničkih uočavanja rizika *(Čaldarović, 1994.).*

Kao najveći i najčešći oblik rizika kod umreženih računala pod operativnim sustavom Windows predstavljaju hakeri koji ne prezaju ni pred čim i za koje ne postoje nikakve granice da bi ostvarili svoje zamišljene ili slučajne i često sulude ideje samo da bi poremetili normalno funkcioniranje računala, ne razmišljajući pri tome koju i kakvu materijalnu i nematerijalnu štetu su spremni učiniti.

Kada kažemo haker, olako taj pojam povezujemo s računalnim kriminalcima, a istina je posve suprotna. Naziv haker skovan je koncem 60-ih godina prošlog stoljeća od pripadnika pasioniranih programera koji su sami sebe željeli nazvati nekim određenim imenom. Da te iznimne ljude ne bismo pobrkali s piscima virusa i uljezima koji se neovlašteno uvlače u informacijske sustave, hakeri su ih prozvali *Creckerima*. Po općeprihvaćenoj definiciji u svakodnevnom okruženju haker predstavlja osobu koja pokušava probiti zaštitu na računalnom sustavu, pristupajući mu s udaljene točke, obično preko lozinke koju je na neki način dobio (npr. preko virusa ili trojanca).

* Ivica Mrđen, dipl. ing. sig., 35214 Donji Andrijevci.

Kada haker provaljuje mrežu, pronalazi sustav koji će napadati, zatim nalazi ulaz u sustav pogađajući lozinku, te iskorištava slabosti konfiguracije sustava za postizanje svojih ciljeva i potreba, te na kraju uklanja svoje tragove *(www.superknjizara.hr/recenzije)*.

Projektanti programa i izrade sigurnosti umreženih računala u Windows programu posvetili su maksimalnu pozornost samoj sigurnosti programa.

Sigurnost je kompaktna defendološka znanost koja se bavi obranom, zaštitom i sigurnosti te njihovom međusobnom povezanošću koja u sebi sadrži raspon svih aktera, uvjeta i djelovanja. Defendologija kao znanost potječe od latinske riječi *defendo, defendare, defendi, defensum*, što znači odbiti, odvratiti, braniti, štititi, te od grčke riječi *logos,* koja znači nauku, odnosno znanost. Sukladno navedenom, defendologija se može definirati kao opća znanost o obrani, zaštiti i sigurnosti, odnosno kao znanost koja izučava zakonitosti postojanja, ostvarivanja i razvoja obrambeno-zaštitne funkcije i sigurnosti uopće i u konkretnom društvu *(Javorović, 1995.)*.

Analizirajući sve aspekte rizika i same sigurnosti koju hakeri mogu proizvesti, programeri sigurnosnog sustava kod umreženih računala pod Windows programom razvili su konfiguraciju internetskog protokola sigurnosti prema osnovama IPSec.

IPSec je standardna metoda dokazivanja autentičnosti i enkriptiranja prometa između IP računala. IPSec osigurava IP paket i protokole nužne za automatsku razmjenu ključeva između računala, kao i za pregovore oko enkripcije i sigurnosti protokola. IPSec izvodi dvije osnovne funkcije primjenom dvije dodatne karakteristike:

- **Sigurno (vjerodostojno) zaglavlje** *(Authenticated Headers - AH)* digitalno enkriptira IP zaglavlje (dio paketa koji sadrži izvor i odredište adrese) i *payload* (dio paketa koji sadrži korisnikove podatke) kako bi bili sigurni da nisu bili modificirani u bilo kojem trenutku njihova prijenosa između računala. AH ne enkriptira promet.
- **Sigurnosno omatanje korisničkih informacija** *(Encapsulating Security Payload - ESP)* enkriptira pakete i primjenjuje novo neenkriptirano zaglavlje kako bi omogućio usmjeravanje *(Strebe, 2003.)*.

Ove dvije metode mogu se primjenjivati zajedno kako bi omogućile autentično zaglavlje i učitavanje enkriptiranih podataka. Programeri istovremeno razvijaju i ESP Mod-Encapsulating Security Payload model sigurnosti.

ESP funkcionira na dva načina, te može biti određen traženom funkcionalnošću i sposobnošću metode IPSec da prepozna računala ili usmjerivače:

- **Transportni modalitet** *(Transport mode)* u kojem se podaci u paketu korisničkih podataka (neenkriptiranom zaglavlju) enkriptiraju, ali zaglavlje ostaje nepromijenjeno. Transportni modalitet namijenjen je enkriptiranju podataka između dvaju računala koji poznaju IPSec i sposobni su dekriptirati paket korisničkih podataka direktno kao kod Microsoft Windows sustava.
- **Tunelski modalitet** *(Tunnel mode)* u kojem je cijeli originalni paket enkriptiran i postaje paket korisničkih podataka novog paketa koji se onda prenosi između usmjerivača koji poznaju IPSec. Tunelski modalitet omogućuje ruterima, koji poznaju IPSec, enkapsulaciju i enkriptiranje mrežnog prometa od računala koja ne poznaju IPSec, preko neosigurane mreže i onda ga dekriptiraju za upotrebu na ciljanoj mreži drugih računala koje ne poznaju IPSec. Tunelski modalitet u Windowsu nalazi se isključivo zbog interoperativnosti sa trećom stranom kada se Windows programi upotrebljavaju kao usmjerivač *(Strebe, 2003.)*.

Poznavajući psihologiju hakera, programeri su predvidjeli mogućnost rizika za sigurnost rada umreženih računala. Stoga su programirali i razvili poseban sustav sigurnosti RRAS (Routing and Remote Access – usmjeravanje i daljinski pristup) te nekoliko vrsta i metoda napada kako bi korisnici umreženih računala bili što sigurniji pri njihovoj uporabi. RRAS ne samo da omogućuje pristup mreži s udaljenih lokacija nego služi i kao krajnja točka VPN (virtualna privatna mreža) koneksija koje primjenjuju enkripciju da bi sigurno spojile privatne mreže preko svjetske mreže kao što je internet. Budući da je svaka udaljena pristupna točka potencijalno mrežno rizična, potreban je poseban oprez kako bi se RRAS učinio što sigurnijim.

Windows uključuje nekoliko alata koji mogu pomoći u konfiguriranju sigurnosnog RRAS sustava. Na serveru se nalaze sljedeći alati:

– **Pravila udaljenog pristupa** (Remote Access Policies) dopuštaju ili ne dopuštaju pristup svim korisnicima na server u skladu s točno određenim uvjetima.

– **Internetska provjera valjanosti** (Internet Authentication Service - IAS) omogućuje centralno upravljanje sigurnošću udaljenog pristupa. Pravila pristupa na ISA-u omogućuju zaštitu i sigurnost za svaki broj RRAS servera.

Za korisnika su dostupni sljedeći alati:

– *Daljinski pristup svojstvima* korisničkog računa (Remote Access Properties of User Accounts) dopuštaju ili ne dopuštaju pristup individualnim korisnicima. Ova dozvola odnosi se na sve oblike pristupa uključujući i spajanje na mrežu, te VPN.

– *Uspostava menadžerske veze* (Connection Manager Administration Kit - CMAK) dopušta kreiranje prilagođene programske podrške za pristup klijenta za dial-up ili VPN pristup mreži *(Strebe, 2003.).*

Sama vrsta napada predstavlja ozbiljan hakerski napad koji se ogleda u tome da li je žrtva nasumce odabrana ili se radi s točno ciljanim napadima što predstavlja veliki rizik od samih hakera. Ozbiljnost hakerskih napada određuje se prema tome da li je korisnik žrtva nasumičnog ili točno ciljanog napada.

Nasumični napad (Random Attack) ne predstavlja ciljanu malicioznu namjeru protiv neke tvrtke. Nema puno razloga za odgovorom na takve napade.

Ciljani napad (Targeted Attack) je posebno pripremljen protiv neke tvrtke. Zahtijeva budnost i istragu kako bi se utvrdilo tko je (ili tko bi mogao) izvršiti napad.

Korisnici ili tvrtke posebno se moraju pripremiti za ove tri vrste napada:

– *Automatizirani napadi* (Automated Attacks), još nazvani i ''crvi'', izvršavaju se pomoću programske podrške koji se ponašaju kao virus, iskorištavaju poznate slabosti na određenim programskim podrškama internet-servisa kao što su mrežni serveri ili serveri elektroničke pošte. Ta vrsta napada postoji od početka primjene interneta i utječe na sve veće operativne sustave. Budući da je Windows popularan operativni sustav, glavna je meta ove vrste napada. Kada se jednom osigura servisna programska podrška protiv virusa, mogu se ignorirati buduća upozorenja.

– *Meta prigodnih napada* (Target of Opportunity Attacks). Nasumične mete prigodnih napada su tipični hakerski napadi koji se javljaju na internetu. Te napade izvode uglavnom hakeri-početnici koji nemaju što izgubiti. Hakeri u biti pokušavaju iskoristiti jednu ili dvije slabe točke za koje su nedavno saznali. Od takve vrste napada lako se možemo obraniti primjenom vatrozida (*firewallsa)*, sigurnosnih proksija i usluga koje se mogu naći na internetu zajedno s najnovijim sigurnosnim ''zakrpama''. Nasumični napadi ne zahtijevaju ozbiljnije istraživanje jer se javljaju rutinski i usmjereni su protiv svih koji se nađu na internetu.

– *Ciljani napadi* (Targeted Attacks) su posebno usmjereni protiv neke tvrtke. Rijetki su, ali mnogo ozbiljniji. Malo je vjerojatno da će se takvi napadi dogoditi većini tvrtki, ali napadači su uporniji i upotrijebit će sva sredstva kako bi dobili pristup ili uzrokovali pad servisa. Takvi napadi su uvijek veoma ozbiljni i najčešće ih izvode nezadovoljni zaposlenici, ideološki aktivisti, nezakoniti konkurenti ili ucjenjivači.
U iznimno rijetkim slučajevima napade mogu izvesti iskusni hakeri koji žude za tehničkim izazovima *(Strebe, 2003.).*

Istovremeno hakeri primjenjuju i određene metode i vektorske napade kako bi onemogućili rad umreženih računala u Windows programu.

Postoje tri osnovna načina napada:

– *Napadi otkazom poslužitelja* (Denial of Service (DoS) Aattacks) primjenjuju prirodu internetskog protokola kako bi legalnim korisnicima spriječili pristup uslugama. Ti napadi ne pokušavaju dobiti pristup sustavu; oni jedino nastoje spriječiti druge

da ga upotrebljavaju. Tipične metode čine poplavljivanje servisa informacijama kako bi se pretrpao, stvaranje velikog broja lažnih koneksija kako bi se iskoristili resursi servera ili slanje posebno izobličenih zahtjeva koji pokreću crva koji će srušiti server. Bez obzira jesu li to ideološki hakeri ili ucjenjivači, oni gotovo uvijek izvode DoS napade.

– *Eksploatacijski napadi* (Exploitation Attacks) još se zovu i *buffer overruns*. Kod ove vrste napada pokušava se anonimno spojiti na servis i podići razina napadačevih privilegija na sustavu na razinu koju ima provjeren korisnik ili administrator. Takav napad iskorištava slabosti na serverskom kôdu i dopušta napadaču da ubaci svoj kôd na servis. Kada se nađu u sustavu kao administratori, mogu činiti sve kako bi ubuduće kompromitirali sustav. Ta vrsta napada izvodi se pomoću ''crva'' koji se automatski šire kroz "ranjive sustave".

– *Napadi lažnim predstavljanjem* (Impersonation Attacks) javljaju se kada korisnik bez valjanog pristupa primjenjuje provjereni korisnički račun sa ciljem da dobije pristup otkrivanjem lozinke. Takve napade najčešće izvode nezadovoljni bivši zaposlenici ili nelegalni suparnici, ali i hakeri koji tragaju za izazovom. Ti napadi veoma su ozbiljni jer su usmjereni direktno protiv tvrtke *(Strebe, 2003.).*

Računala nisu "ranjiva" od nasumičnih napada bez obzira odakle dolaze. Postoji samo nekoliko načina pomoću kojih napadač može doći do računala:

– *Direktni napad* (Direct Attack) javlja se kada haker namjerava iskoristiti računalo direktno s konzole računala. Takvi napadi su iznimno rijetki i najčešće ih izvode nezadovoljni zaposlenici ili zaposlenici koji se žele našaliti s onima koji ostavljaju svoja računala logirana. Moderni sustavi logiranja su jače zaštićeni protiv takve vrste napada i uz malo administrativnog napora administratori ih mogu eliminirati kao opasnu prijetnju.

– *Bežični napadi* (Wireless) događaju se kada se hakeri direktno povezuju u mrežu koristeći se bežičnim servisima koji su namijenjeni legalnim korisnicima i počnu napadati iz mreže. Nekad su bili rijetki, ali su uznapredovali uz pomoć bežične tehnologije koja je omogućila hakerima pristup mreži uporabom bežičnih pristupnih točaka.

– Napade spajanjem na mrežu hakeri su prvobitno primjenjivali za spajanje u slučaju kad su udaljeni od mreže. Takvi napadi su postali rijetki od kako je tehnologija bivala zamijenjena internetskom povezanošću i mogu biti spriječeni stavljanjem *Routing and Remote Access Service* (RRAS) servera izvan perimetra i spajanjem na mrežu kao internetske koneksije.

– Internet se najčešće napada. Većina tvrtki i velik broj korisnika diljem cijelog svijeta imaju pristup internetu. Ovaj stupanj konektivnosti i anonimna priroda niskog stupnja internetskog protokola stvorili su savršeno okruženje za hakere. Budući da su direktni napadi rijetki, bežični i spajanjem na mrežu, mogu biti smješteni izvan vatrozida, pa se ne mogu tretirati kao internetski napadi. Internetski napadi su jedini oblik napada autsajdera na pravilno postavljenu mrežnu infrastrukturu kojih se treba bojati *(Strebe, 2003.).*

Programeri su poznavajući psihološku i stručnu stranu hakera nakon dugogodišnjih praćenja i razvijanja svih oblika mogućih rizika i posljedica, te sigurnosnih aspekata išli za time da predvide koji su to sve mogući mrežni upadi u sami sustav.

Napadači koji pokušavaju dobiti pristup nekoj mreži bez poznavanja mrežne osnove primjenjuju standardni slijed napada. Počnu s prikupljanjem podataka, zatim namjeravaju iskoristiti poznate slabosti i nastave s težim dijelom, napadom lažnim predstavljanjem koje se sastoji od pokušaja uzimanja identiteta validnog korisnika pogađanjem ili krađom imena računa i lozinke, krađom ''smart'' kartice ili prilagođavanjem certifikata.

Da bi dobili informacije o nekoj tvrtki, većina hakera koja namjerava započeti slijed napada na mrežu će:

– provjeriti javne DNS zabilješke kako bi odredili IP adrese internetskog servera
– primijeniti port-skenere kako bi skenirali internetske servere i identificirali usluge
– istražiti sve usluge koje nađu kako bi odredili koji će napade iskoristiti protiv tih usluga.

Kada jednom dođu do ovih informacija, oni će:

– započeti napade virusima na zajedničke servise sa ciljem da dobiju udaljeni administrativni pristup (takvi napadi obično šalju izvršni kôd zajedno s izobličenom porukom dizajniranom da izvrši poslani kôd)
– pokušati napasti oponašanjem identiteta
– izvesti razne padove servisa ako ne uspiju dobiti pristup.

Znati kako hakeri rade je prvi korak u otkrivanju i zaustavljanju njihovih napada. Kada se razumije osnovni proces koji hakeri primjenjuju u napadu na mrežu, može se razlikovati njihov način upotrebe od načina regularnih korisnika *(Strebe, 2003.).*

Poznavajući hakerske poteze, programeri umreženih računala pod Windows programom pokušali su mrežne upade hakera smanjiti na najmanju moguću mjeru za samu sigurnost i uporabu umreženih računala te tako istovremeno umanjiti i posljedice eventualnih upada, pa su iz tih razloga programirali i posebni sigurnosni server, tj. tzv. server mamac.

Server "mamac" (još nazvan i *honeypot server*) je server koji radi na neosiguranoj (ili slabo osiguranoj) verziji istog operativnog sustava kao i produkcijski server. Teorija je jednostavna: svi oblici pristupa se prosljeđuju ''mamcu'' osim onih koje se žele javno pokazati, oni se prosljeđuju pravom serveru. Autsajderu dva računala izgledaju kao jedno računalo, ali sve vanjske usluge se usmjeravaju na ''mamac'' radije nego na pravi server.

Stvaranje "mamca" je jednostavno, ali zahtijeva vatrozid ili proksi server. Na vatrozidu ili sigurnosnom proksiju može se proslijediti računalu ''mamcu'' TCP portove incidentnih usluga koje se ne primjenjuju, ali koje su dostupne na neosiguranim serverima. Računalo ''mamac'' trebao bi biti lociran na DMZ, ali konfiguriran tako da blokira izlazne koneksije. Cilj ovog računala je da bude napadnut, iskorišten i da upozori korisnika na svaki pristup. U isto vrijeme može se primjenjivati sigurnosni proksi za prosljeđivanje TCP portova s pravog javnog servisa na produkcijsko računalo u mrežnom perimetru *(Strebe, 2003.).*

Programiranjem i postavljanjem samog server mamca programeri su onemogućili hakere u njihovim naumima i htijenjima te je s tim serverom postignuta maksimalna zaštita umreženih računala pod Windows programom, a samim time je i rizik uporabe umreženih računala doveden na najmanju moguću razinu.

ZAKLJUČAK

Primijenjenim metodama u razvoju tehnologije informacijske sigurnosti vidljivo je da je koncept sigurnosti koju je razvio Microsoft u svojem programu WINDOWS maksimalan doprinos zaštiti prijama, slanja te pohrane podataka i usluga, kao i samih osoba koje rade s umreženim računalima na zavidnoj razini.

No, kako sve ono što je danas sigurno, za sutra već postoji mogućnost i pretpostavka da nije, svaki korisnik osobnog računala mora pratiti razvoj informacijske tehnologije. Kako se one svakodnevno usavršavaju, istodobno je potrebno da se prate i primjenjuju sve moguće sigurnosne komponente umreženih računala i podataka kojima manipulira, tako da se ne bi dogodilo da korisnik nije pripremljen na moguće upade pojedinaca i skupina u sigurnosni sustav programa, a da toga nije bio svjestan ili da nije znao primijeniti najnovija sigurnosna načela u radu s osobnim računalom.

Iz ovog članka vidljivo je da je proizvođač računalnog programa maksimalno primijenio sve elemente zaštite kod tog istog programa, te premda postoje i oni koji će taj program pokušati onesposobiti i zlouporabiti, ostaje obveza korisnika programa držati se programskih uputa proizvođača pri radu s ovim programom.

LITERATURA

Čaldarović, O.: Socijalna teorija rizika, *Revija za sociologiju,* 25, 1994., 3-4, str. 213-215.

Javorović, B.: *Defendologija,* DEFIMI, Zagreb, 1995.

Strebe, M.: *Implementing and Administering Security in a Microsoft Windows 2000 Network,* Microsoft Corporation, New York, 2003.

http://www.*superknjizara.hr/recenzija*.php?id_knjiga=804212.08.2005.g.

COMPUTER NETWORK SECURITY IN WINDOWS

SUMMARY: At the time the Internet was emerging as an experimental network, its security programmers did not foresee the possibility of abuse of the computer systems and did not focus on computer security for the individual user, for the institutions using computer network programs and for the society as a whole which might be harmed as a result of computer networking. The technological risk and the development of Microsoft's personal computer programs have created the need to protect computer programs from unwanted individuals and groups who may wish to abuse their data. Microsoft has designed a program with the basic guidelines for the storing, forwarding, operation and protection of Windows network from unwanted break-ins of unauthorised persons, i.e. hackers.

Key words: *security, computer network, hackers, bait*

Professional paper
Received: 2006-02-01
Accepted: 2006-03-17