Zaštitimo se

Sigurnost servera i računala općenito apsolutno je nužna u modernom informatičkom svijetu. Globalne komunikacije, stalne veze prema Internetu, brz razvoj softvera, sve to čini sigurnost vrlo bitnom stavkom u planiranju bilo kakvog sustava. Kako inherentno nesigurni Internet sačinjava velik broj Linux računala, praktički nam je obaveza u jednoj seriji članaka napisati nešto više o tome što bi mogao očekivati Linux administrator i protiv koga i čega bi se morao boriti. U sljedećim brojevima ćemo opisati i nekoliko programa koji se bave mrežnom sigurnošću i nadzorom. Iako će vam se članci činiti okrenuti naprednim korisnicima, trudit ćemo se dati najbolji omjer između jednostavnosti i količine informacija, dati što više praktičnih savjeta i uputa.

Njihova mjesta okupljanja su IRC (*Internet Relay Chat*), a najčešće veći znalci iskorištavaju mlađe kako bi za njih obavljali prljave poslove, nadajući se da će s vremenom postati *uber*-hakeri.

Bez sumnje su najgori profesionalci koji to rade iz materijalnih pobuda. Njihove žrtve su financijske institucije ili bilo koja tvrtka s resursima bilo koje vrste, a poslodavci ljudi s neograničenim sredstvima. U posljednje vrijeme agencije koje šalju *spam* zapošljavaju beskrupulozne ljude koji zauzvrat traže načine kako provaliti u računala i koristiti ih za slanje još više nepoželjnih *mailova*. Tako je primjerice i nastao virus Sobig-F, možda i najčešći virus u 2003.

Svi protiv jednog, jedan protiv svih

Što bi jedan administrator mogao sam napraviti protiv takvih zlih individua ili korporacija? On naravno nije sam, već iza njega stoji tvrtka koja je proizvela operacijski sustav, ili *Open Source* zajednica, radi li se o besplatnom sustavu poput Linuxa. Oni promptno izdaju nove verzije softvera za koji se pojavi rupa (*exploit*), ili daju upute kako zaštititi sustav.

Naravno, niti jedan sustav nije apsolutno siguran niti bi ikada mogao biti. Moguće je jedino otežati situacije koje bi netko mogao iskoristiti za provalu. S druge strane, što je sustav sigurniji, to ga je teže koristiti. Potrebno je naći pravu mjeru između ta dva oprečna pojma, ovisno o namjeni sustava. Svakako da je za kućno računalo potrebno definirati drugačiju sigurnosnu politiku od one za neko vojno ili financijsko. Pogrešno je razmišljanje da je sustav premalen ili da ne posjeduje nikakve korisne informacije za koje bi netko mogao biti zainteresiran. Provalnici žele ugroziti što više sustava, bez obzira na veličinu.

Pri postavljanju pravila korištenja bitno je da ih i korisnici sustava poštuju, pod prijetnjom otkaza ili krivičnog gonjenja. Jedan korisnik - koliko god bio pouzdan - može ugroziti cijeli sustav omogućivši nekom drugom pristup, namjerno ili ne. Zato treba jasno postaviti granicu: sve što nije eksplicitno dozvoljeno, zabranjeno je. Razni Linux sustavi, primjerice, mogu različitim korisnicima dodijeliti različita prava za pokretanje programa, zauzeće procesora, diska i slično. Osim servera, to korisnike štiti od njih samih i na *desktop* računalima, budući da ne mogu zabunom sami nešto pokvariti (bez uloženog truda). Nije preporučljivo niti instalirati previše ponuđenih dodatnih programa, već samo najnužnije, i to one koji nisu ozloglašeni po nesigurnosti.

Onemogućavanjem korisnika zaštitit ćemo prvenstveno lokalno računalo. Njegova sigurnost svakako je primarni cilj i posljednja linija obrane. Odabirom sigurnih lozinki, redovitim skidanjem najnovijih zakrpi i pažljivim praćenjem rada taj se zadatak može svesti na relativno jednostavni proces.

Sigurnost mreže je skoro jednako bitna. Heterogeni sustavi s više stotina raznorodnih računala i administratorima različitog stupnja ekspertize vrlo su zahvalna meta napada. Već i jedan provaljen sustav može biti iskorišten za napad na ostale, a tad prestaje vrijediti sigurnost na razini lokalne mreže zaštićene *firewallovima* i nedostupnošću.

Zanimljiv je i koncept engleskog naziva *security through obscurity*. Njegova je osnova sigurnost koja se dobiva sakrivanjem nekog dijela sustava na nestandardno mjesto. Konkretno, ako se web server standardno nalazi na portu 80, mi ga možemo premjestiti na neki atipični kako ga skripte koje periodički pretražuju cjelokupni Internet ne bi našle. Taj pristup ima očit nedostatak jer većini ljudi onemogućavamo pristup ako ih unaprijed nismo uputili u promjene. Osim toga, dovoljno odlučan haker će ih prije ili kasnije nekako pronaći.

Nakon što smo vam dali dovoljno razloga za brigu, u idućim ćemo vam brojevima reći nešto o fizičkoj sigurnosti i metodama kako zaštititi višekorisničko Linux računalo. No, najviše ćemo prostora potrošiti na zaštitu umreženog računala.

▲ **Sredinom devedesetih malo se znalo o velikim računalnim sustavima, a ovako su predstavljani filmskoj publici u "Hackerima"**

Kevin Mitnick

Kevin Mitnick bez sumnje je najpoznatiji haker današnjice, onaj kome je dodijeljeno najviše medijske pažnje uopće. On je 1995. počeo provaljivati u razne servere u Americi, pa i neke vladine ili visoko profilirane servere, poput Yahooovih i Sunovih. Namjera mu nije bila nikakva direktna šteta, niti je to radio iz financijskih pobuda. Jednostavno je išao od sustava do sustava zadovoljavajući svoju intelektualnu radoznalost.

Otkriven je kad je ušao u računalo T. Shimomure, također vrsnog hakera, koji ga je uspio locirati. Slijedilo je uhićenje, a nakon dugog čekanja na suđenje osuđen je na zatvorsku kaznu od 5 godina i još godinu zabrane spajanja na Internet (po nekima, to je gore od zatvora). Osuđen na neprimjerenu i preveliku kaznu, trebao je poslužiti kao žrtveno janje i upozorenje svim budućim hakerima u doba kad je Internet još bio relativna nepoznanica. Ipak, postao je idol cijele jedne generacije. Bezbrojne stranice provaljene su u njegovu "čast", a na njih je postavljena poruka "Free Kevin". Naknadno je osnovao tvrtku koja se bavi konzaltingom u sigurnosti. U njegovu čast snimljena su i dva filma: "Takedown", koji ga je pokušao prikazati kao kriminalca, i realniji, nagrađivani dokumentarac "Freedom Downtime".

▲ **Kevin Mitnick, jedan od najeksponiranijih hakera današnjice**