Sjemenarstvo 19(2002)1-2 UDK: 378.663(045)=862
Stručni rad

ZAŠTITA RAČUNALNIH RESURSA POMOĆU INTERNET FIREWALL

Dubravka ŠIMUNOVIĆ

Agronomski fakultet Sveučilišta u Zagrebu
Zavod za matematiku i informatiku

Faculty of Agriculture University of Zagreb
Department of Mathematics and Informatics

SAŽETAK

Internet je najveći izum u povijesti čovječanstva koji je ostavio najdublji trag u 20. stoljeću, a definitivno i obilježio budućnost. Sve više postaje metafora svjetske pismenosti, tj. vještine i znanja pomoću kojeg se do informacija dolazi na najbrži i najlakši mogući način, bez obzira gdje se nalazila.

Svakodnevno se raspravlja o zlouporabi Interneta, ali najčešće se rasprave vode o upadima vandala, hackera, takmičara i špijuna u sigurnosne sustave vlade, sustave zaštite, te "sijanju" virusa po različitim sajtovima i na elektronsku poštu. Takve pojave nisu za podcjenjivanje, ali računala imaju svoje obrambene mehanizme kojima se takvi ispadi mogu djelomično ili potpuno ograničiti

Jedan od takvih mehanizama je i firewall, komponenta ili skupina komponenata koje ograničavaju pristup između zaštićene mreže i Interneta, ili između dva međusobno odvojena dijela mreže. FireWall je siguran način zaštite mreže, koji segmentira i štiti našu internu mrežu od opasnosti i mogućih uljeza od strane Interneta, ima nekoliko osnovnih namjena, a najčešće predstavlja točku pomoću koje se interna mreža spaja na Internet. Iako je Firewall jako dobar oblik zaštite od mogućih hakera iz vanjskoga svijeta, ipak ne predstavlja kompletno sigurnosno rješenje, stoga se za maksimalnu zaštitu koriste kombinacije tehnika zaštite.

Ključne riječi: firewall, hakeri, vandali, takmičari, špijuni, rizik, resursi, reputacija, Packet Filtering system, host, proxy servisi, Bastion Hostom, usmjerivači, Screen Subnet Architecture, računalo utvrda.

1. UVOD

Internet danas predstavlja veliki tehnološki napredak, omogučuje pristupi objavljivanje neograničenog broja informacija, ali isto tako predstavlja i opasnost jer pruža mogučnost za uništenje informacija na puno sofisticiranije novije, načine, pa je to jedan od razloga zašto se s vremenom počinje razmišljati i o zaštiti vlastitih informacija, odnosno samog računala. Pri tome moramo imati na umu da se svakako uz pitanje sigurnosti vežu i pitanja tipa:

što želimo zaštiti na našem sustavu, kakav tip napada možemo očekivati i koji tip zaštite možemo primjeniti?

No, prije nego kažemo sve što možemo s vatrozidom (engl. Firewall) trebamo znati zbog čega nam je potreban, a prije nego ga počnemo koristiti potrebno je znati što u stvari želimo zaštititi? Zapravo, posve je sigurno kad smo spojeni na Internet izloženi su riziku naši podaci u računalu, samo računalo, a također i naša reputacija.

Isto tako bitno je znati protiv čega se želimo zaštititi. Postavljaju se jednostavna pitanja, kao na primjer, što nas u stvari zabrinjava, koje su to vrste napada s kojima se na Internetu možemo susresti, o kakvim je napadačima riječ, zatim što je s nezgodama koje su uzrokovane ljudskom glupošću i neznanjem. Obzirom na vrstu napada postoji mnogo vrsta i načina na koje se ti napadi mogu provesti, no imamo tri osnovne kategorije, a to su: neovlašteni pristup, blokiranje servisa i krađa informacija. Što se tiče vrsta napadača, razlikujemo: hakere iz zabave, vandale, takmičare i špijune. Neovlašteni pristup koji je uzrokovan ljudskom glupošću i nezgodama, također je nešto od čega se želimo zaštititi.

Firewall predstavlja komponentu ili skupinu komponenata koje ograničavaju pristup između zaštićene mreže i Interneta, ili između dva međusobno odvojena dijela mreže. U daljem tekstu istaknut ćemo protiv čega nas vatrozid može i protiv čega nas ne može zaštititi.

2. VRSTE RIZIKA

2.1. Podaci

Naši podaci posjeduju tri karakteristike koje bi trebalo zaštititi, a one su: t*ajnost* - ne želimo da svi raspolažu našim informacijama. Pojedine informacije na našem sistemu za nas predstavljaju iznimno značenje i ne želimo ih djeliti s drugima, i*ntegritet* – ne želimo da se naši podaci neovlašteno mijenjaju te r*aspoloživost* – sigurno želimo koristiti naše resurse u potpunosti, a ne dijeliti ih s nekim nepozvanim.

Mnoge organizacije važne tajne drže na svojim korporacijskim serverima (dizajn proizvoda, patenti, financijski podaci, podaci o osoblju,..) što predstavlja često veoma veliki rizik. Međutim ponekad je relativno jednostavno razdvojiti podatke po stupnju važnosti, pa ih tako i tretirati. Pretpostavimo da to možemo bezbolno napraviti i da podatke koji nam ne predstavljaju tajnu, izložimo bez ikakvih zaštita prema okolini. Međutim i tada moramo razmišljati o slijedeća dva faktora, a to su resursi i reputacija.

Iako podaci nisu tajni, ne želimo da netko naše podatke mijenja ili briše. U tom slučaju mogu neželjene informacije dospjeti na naše računalo, kao što se podaci mogu i obrisati što dovodi do financijskih troškova i nedostupnosti željenim informacijama.

Kompjuterski kriminal je u mnogome drugačiji od ostalih oblika kriminala zato što je ponekad samu radnju veoma teško detektirati. Ponekad će nam trebati jako puno vremena da otkrijemo da nam je netko neovlašteno pristupio sistemu, a nekada to nećemo niti saznati. Čak i ako netko neovlašteno pristupi i ne učini ništa, potrošiti ćemo vremena i vremena da provjerimo da on stvarno nije ništa učinio. Ako napadač uništi sve, znamo da je bio, utvrdimo način upada u sistem i otklonimo ga, dignemo back up, popravimo šta se popraviti da i radimo dalje.

2.2.Resursi

Većina nas želi koristiti samostalno svoje računalo. Ako pak damo slobodno na korištenje kompjutersko vrijeme ili diskovni prostor, obično očekujemo dobar publicitet i zahvalu za to. Ako mi potrošimo svoje vrijeme i novac na svoje kompjuterske resurse, naše je i pravo da njima slobodno raspolažemo.

Napadači se obično brane da koriste samo višak resursa, a njihov upad žrtve ne košta. Kao prvo ove tvrdnje su potpuno nesuvisle jer je nametniku jako teško odrediti koji su resursi za vlasnika višak, tako da se samo oni koriste. Nametnik nam ne može vratiti naše resurse kada ih trebamo nazad. (slična je situacija kad npr. posjedujemo neki predmet koji trenutno ne koristimo, ali to nije razlog da nam ga netko uzme, jer nam taj predmet može zatrebati svaki trenutak.) Drugo, ako i ne koristimo naše resurse to ne znači da ih netko ima pravo koristiti kao da su prirodni resursi, ili resursi koje svakako treba koristiti jer će inače propasti neiskorišteni.

2.3. Reputacija

Nametnik se pojavi na Internetu s našim identitetom, pa sve što radi izgleda kao da mi radimo. Koje su posljedice? Vlasnici hostova ili njihovi advokati počinju tu osobu nazivati i pitati zašto pokušava ući nepozvano u njihov sistem. Poneki sajtovi su počeli ozbiljno razmišljati o zaštiti svojih strojeva kada je njihovo administratorsko osoblje počelo dobivati upite od vojnih i policijskih članova društva o problemu upada u vojni sistem s njihova računala. Nametnik koji se predstavlja kao mi može jednostavno poslati poruku elektroničkom poštom kao da smo je mi poslali. Ako neke osobe prihvate i vjeruju tim porukama, mogu nam uzrokovati dosta štete, a mi ćemo potrošiti jako puno vremena i živaca da sve sudionike uvjerimo u lažnost te poruke. Sve to predstavlja jako veliko narušavanje naše reputacije.

Ako nametnik i ne koristi naš identitet, sam neovlašteni pristup našem računalu nije dobar za našu reputaciju. To ruši povjerenje korisnika prema sigurnosti i postojanosti naših podataka. Mnogi nametnici mogu iskoristiti naše računalo kao izvor distribucije različitog piratskog i pornografskog materijala, što također može nesagledivo utjecati na našu reputaciju.

Danas, na svjetskoj računalnoj mreži postoje različiti načini ugrožavanja, od kojih nam se valja zaštititi, a to je od: napada, napadača i neovlaštenog pristupa.

3. NAPAD

Danas postoji mnogo tipova napada na sustav, kao i mnogo načina da ih kategoriziramo, a za potrebe ovog rada razvrstati ćemo ih u tri osnovne kategorije, i to: *neovlašteni pristup, blokiranje servisa, krađa informacija.*

3.1. Neovlašteni pristup

Najčešća vrsta napada na naš sustav je neovlašteni pristup, kod kojega napadač može nesmetano koristiti naše računalo. Većina napadača koristit će naše računalo kao standardni tip korisnika. Napadači raspolažu s više mogućih načina dobivanja pristupa računalu:

Socijalne grupe napada - napadač otkrije ime nekoga tko visoko kotira u kompaniji, nazove sistem administratora, pretvara se da je ta osoba, te traži hitnu promjenu lozinke, radi nekog bitnog i neodgodivog posla.

Jednostavni pokušaji pogađanja naziva i lozinka - isprobaju se sve moguće kombinacije naziva i lozinki.

Kompleksni način - kod kojih ne trebamo znati ni naziv ni lozinku.

Firewall pomaže pri prevenciji neovlaštenih pristupa u velikom broju slučaja. Idealno gledano, može spriječiti sve vrste pristupa za koje ne treba koristiti naziv računala i lozinku. Propisno konfiguriran on smanjuje broj računala kojima se može pristupiti izvana, pa su stoga osjetljivi na pogađanje i socijalni napad. Mnogi koriste firewall da bi implementirali jednom korištene lozinke, čime se onemogućuje pogađanje lozinke kao i prisluškivanje paketa, te njihovo ponovno slanje. Ako se i ne koristi ova opcija firewall će nam predstavljati kontrolno mjesto preko kojega ćemo moći detektirati napade pogađanjem.

3.2. Blokiranje servisa

Premda neki slučajevi elektroničke sabotaže obuhvaćaju destrukciju ili shut down opreme i podataka, znatno češće se javlja zasipanje opreme nekorisnim informacijama. Nametnik zasipa sistem ili mrežu s porukama, procesima ili mrežnim upitima tako da se ni jedan stvaran i normalan posao ne može obaviti. Sistem ili mreža troši sve svoje vrijeme odgovarajući na poruke i zahtjeve, nemajući vremena i mogućnosti da bilo koju od njih zadovolji..

Skoro je nemoguće zaštititi se od svih vrsta onemogućenja upotrebe servisa. Na primjer mnoga računala blokiraju korisničke račune nakon određenog broja neuspješnih prijava. To onemogućava napadače da pogađaju

naziv računa i lozinku dok je ne pogode. Na drugi način daju napadačima lagani način onesposobljavanja servisa, onesposobljavajući sve accounte na računalu pomoću određenog broja neuspješnih pokušaja.

Ovaj tip napada obično koriste nametnici koji su ljuti na nas ili željni osvete, a takvih na svu sreću nema puno.

3.3. Krađa informacija

Neki oblici napada dopuštaju napadaču da dobije podatke bez da je ikada direktno pristupio našem računalu. Napadači koriste Internet servise za iznuđivanje informacija, pomoću kojih nagovaraju korisnike servisa da daju im povjerljive informacija ili da ih daju krivim ljudima. Mnogi su Internet servisi dizajnirani za korištenje na LAN i nemaju nivo sigurnosti koji bi trebali imati da bi se mogli bez opasnosti i sigurno koristiti preko Interneta.

Postoje dva načina krađe informacija:

Aktivna krađa informacija - osobe koje žele doći do osobnih informacija mogu jednostavno nazvati i pitati (pretvarajući se da su netko tko bi to trebao znati).

Pasivna krađa informacija – kad osoba koja želi doći do podataka prisluškuje našu telefonsku liniju.

Slično osobe koje žele doći do elektroničkih informacija, mogu: *aktivno ostvariti upit za njih*, tj. pretvarajući se da su sistem ili osoba koja im ima pristup, *pasivno osluškivati mrežu,* tj. čekajući da se pojavi željena informacija.

Prisluškivanje telefona donjeti će nam poneku interesantnu informaciju, ali globalno gledano jako puno utrošenog vremena s mnoštvom nekorisnih informacija. Isto tako osluškivanje mreže (sniffers) je veoma efektno kod otkrivanja lozinke, ali se znatno rijeđe koristi za dobivanje drugih tipova informacija. Dobivanje specifičnih informacija zahtjeva znatno veću pažnju i strpljenje, ili informaciju o tome kada će se određeni tip informacija pojaviti na određenom mjestu.

Prisluškivanje kompjuterskih mreža znatno je jednostavnije od prisluškivanja telefonskih linija. Promet koji se uspostavlja s Internetom prolazi kroz veliki broj lokalnih mreža i svaka od njih može predstavljati moguću točku rizika. Davaoci usluga priključenja na Internet i javno dostupni sistemi predstavljaju veoma popularne mete za nametnike. Programi za osluškivanje smješteni su tamo gdje mogu dati jako dobre rezultate pošto je jako velik protok informacija na takvim mjestima.

Postoji nekoliko uspješnih načina zaštite protiv krađe informacija. Propisno konfigurirani firewall predstavlja jako dobru zaštitu od ljudi koje žele pristup informacijama koje mi ne želimo dati. Jednom kada odlučimo dati određene informacije na Internet jako ih je teško zaštititi. Firewall štiti informacije unutar mreže, a ne može zaštititi informacije koje idu izvan nje.

4. NAPADAČI

Postoji mnogo različitih načina na koje možemo grupirati vrste napadača. Bez obzira na grupiranje svi napadači djele neke zajedničke karakteristike. Oni ne žele biti uhvaćeni, pa se skrivaju. Ako uspiju probiti sistem svakako će željeti sačuvati mogućnost pristupa sistemu, kreirajući dodatni način pristupa, da u slučaju otkrivanja, njihov način probijanja zaštite ostane alternativni način pristupa sistemu.

Hakeri. Oni iz zabave predstavljaju grupu ljudi koja neovlašteno pristupa tuđim kompjuterima iz čiste dosade. Oni pristupaju tražeći interesantne podatke, ili jednostavno zato što im je zabavno koristiti tuđe računalo. Najčešće unište podatke, ili naprave štetu iz neznanja ili želje da prikriju svoju prisutnost, a najčešće napadaju javno dostupna računala*: davatelje Internet usluga, državne institucije, javne web stranice*

Vandali. Oni najčešće neovlašteno pristupaju tuđim računalima i žele nanjeti što veću štetu, zato što uživaju u tome ili im se vlasnik iz nekog razloga zamjerio. U većini slučaja brisanje podataka i oštećenje opreme i nije najgora stvar koju nam neko može učiniti. Ponekad je znatno nezgodnije prikriveno i dugotrajno djelovanje koje je teško detektirati i popraviti. Nažalost, gotovo je nemoguće zaustaviti otkrivenog vandala, tj. ako vam netko želi nauditi prije ili kasnije će naći način na koji može to učiniti, ako posjeduje potrebno znanje i upornost. Pojedini tip napada je atraktivan za vandale, ali ne i za druge tipove hakera. Na primjer onemogučenje rada servisa je interesantno vandalima, ali ne i hakerima kojima je interesantnije da je vaš stroj u pogonu i nesmetano radi.

*Takmičari.*To je grupa hakera koja iz čisto takmičarskih pobuda neovlašteno pristupa sistemima, hvaleći se brojem razbijenih sistema i različitošću njihovih operativnih sistema. Oni obično odabiru sisteme od što većeg značenja, da bi njihov neovlašteni pristup dao veliki publicitet, a samim time i njih proslavio u hakerskoj zajednici. Također oni neovlašteno pristupaju svemu čemu se može pristupiti, tragajući za kvantitetom, a ponekad i kvalitetom. Njih ne zanima ništa što imamo na svojem sistemu, niti o kojoj se vrsti sistema radi. Sigurno je da kradu informacije i pokušavaju ih naknadno upotrijebiti, na primjer razmjenjujući ih s hakerima. Ostavljaju si obično otvoreni put za naknadni neovlašteni pristup. To je tip hakera kojeg ćemo otkriti dugo nakon njegova neovlaštena pristupa našem sistemu. Otkriti ćemo to postepeno, zamječujući različite najasne stvari na našem računalu ili ćemo shvatiti kada će nas druga firma ili vladina institucija optužiti za neovlašteni pristup s našega računala, ili će nam pak netko poslati kopiju naših privatnih podataka, koju je netko našao na hakerskom računalu na drugoj strani svijeta.

Špijuni. Većina ljudi koja krade, to radi da bi došla do novaca, ili vrijednosti koje se mogu dobro unovčiti. Ako nađu tajne za koje misle da ih mogu dobro unovčiti, mogu to pokušati napraviti, ali to nije njihov glavna djelatnost. Špijune je znatno teže otkriti nego klasičan neovlašteni pristup ostalih napadača. Krađa

informacija ne ostavlja nikakav ozbiljniji trag i špijune je jako teško detektirati odmah. Netko tko pristupi našem sistemu, kopira podatke i napusti ga bez ikakve štete jako je teško zamjetljiv. Praktički gledano, mnogim organizacijama jako je teško onemogućiti špijunsko djelovanje u bilo kojem obliku. Mjere opreza koje je potrebno preduzeti da bi se zaštitile osjetljive informacije na računalima su veoma kompleksne, skupe i teške, pa se koriste na mjestima gdje se nalaze stvarno kritično osjetljive informacije. Mjere opreza uključuju elektromagnetsko oklapanje, potpunu kontrolu pristupa te ne dozvoljavaju nikakvo spajanje na nesigurne mreže.

5. NEOVLAŠTENI PRISTUP

Često se može dogoditi da naivni i neupučeni korisnici uzrokuju blokadu sustava ili zabunom obrišu važne informacije ili pošalju krive informacije na krivu adresu.

Firewall-ovi nisu konstruirani i ne mogu štititi kompanije od takvih tipova incidenata, uzrokovanih ljudskim greškama ili nestručnošću. Na žalost često rezultati slučajnih grešaka, kao i neovlaštena pristupa hakera mogu dovesti do istih kobnih rezultata, kao što je gubitak informacije ili davanje informacija krivim osobama.

Osim što se moramo zaštititi od mogućih vanjskih napada od strane neovlaštenih osoba, moramo se maksimalno zaštititi i od grešaka uzrokovanih ljudskim neznanjem i nestručnošću. Da bi se ti tipovi grešaka otklonili moramo posvetiti maksimalnu pažnju školovanju djelatnika, kao i unutarnjoj sigurnosnoj regulativi.

6. METODE ZAŠTITE RAČUNALA

6.1. Model bez zaštite

Najjednostavniji način zaštite je da se sistem ostavi bez ikakve dodatne zaštite, odnosno ostavi se samo minimalna zaštita koju dobivamo po defaultu s operativnim sistemom.

6.2. Zaštita temeljena na neznanjima

Koristeći ovaj način, pretpostavljamo da je sistem siguran iz čistoga razloga zato što za njega nitko ne zna (ne zna za njegovo postojanje, sadržaj, mjere sigurnosti i sve ostalo). Ovaj model često je kratkotrajan, iz jednostavnog razloga što postoji jako mnogo načina da se stroj na mreži nađe i prepozna kao zgodna meta.

Mnogi ljudi smatraju da i ako ih mogući hakeri vide na mreži neće ih dirati iz čistoga razloga jer se radi o malim kompanijama ili privatnim računalima, dok u stvari realnost je potpuno drugačija. Većina hakera ne mari mnogo o tipu mete, nego o njihovoj raznolikosti i količini. Za njih male kompanije i kućna računala predstavljaju lake mete. Vjerojatno se na takvom računalu neće zadržati dugo, ali samim neovlaštenim pristupom i njegovim prikrivanjem, mogu izazvati veliku štetu.

Za normalno funkcioniranje računala na bilo kojoj mreži, a tako i Internetu, administrator mora proći kroz minimalnu proceduru registracije, a samim time te minimalne informacije postaju dostupne skoro svakome tko je prisutan na mreži.

Svaki put kada ta ista računala koriste servise koji stoje na raspolaganju na Internetu, vlasnici tih servisa dobiti će informaciju o dotičnom računalu. Hakeri motre na sva takva nova računala nadajući se da ona nemaju još provedenu potpunu sigurnosnu zaštitu. Mnoga računala također u pozdravnoj poruci ispisuju i naziv operativnog sistema, te njegovu verziju, što uvelike olakšava posao eventualnome hakeru.

Hakeri stoga imaju dosta vremena da isprobaju sve moguće načine obstrukcije računala, tako da za ovu metodu ne možemo reći da je pametan sigurnosni izbor.

6.3. Zaštita računala

Najvjerojatnije, najčešće korišteni model kompjuterske sigurnosti je zaštita računala. Sa ovim modelom možemo nezavisno osigurati zaštitu za svako računalo posebno. Možemo otkloniti sve poznate standardne nedostatke vezane za pojedini operativni sistem.

No, glavna smetnja efikasnom korištenju metode zaštite računala je suvremeno kompjutersko okruženje koje obuhvaća:

Računala od različitih proizvođača, svaki sa svojim operativnim sistemom, a samim time svaki sa svojim vlastitim sigurnosnim problemima.

Računala od istoga proizvođača, često se događa da imaju isti operativni sistem, ali s različitim verzijama od kojih svaka dolazi sa svojim specifičnim sigurnosnim problemima.

Računala od istog proizvođača, s istim operativnim sistemom, istom verzijom operativnoga sistema, često su različito konfigurirana, (neki servisi rade, a neki ne) što ponovo može dovesti do različitih vrsta problema.

Iako su sve mašine potpuno identične njihova količina čini čitav posao administracije dosta teškim. Može se dogoditi da tokom te administracije dođe do greške, ali ako i do njih ne dođe i dalje se javlja otvoreno pitanje da li su stvarno svi problemi otklonjeni ili će se vremenom javiti neki novi, koji će zahtjevati dodatnu zaštitu i administriranje.

Model zaštite računala je dobar oblik zaštite za male korporacijske mreže ili korporacije s izvanrednim sigurnosnim zahtjevima. Svakako bi svaka kompa-

nija trebala uključiti određeni stupanj zaštite računala u svoj sigurnosni model. Glavni problem samoga modela zaštite računala je što uz malu cijenu koštanja unosi velika ograničenja korisnicima i velike administrativne zahtjeve.

Iako se zalažemo za model mrežne sigurnosti preporučamo jako dobro provedenu zaštitu računala koja su od većeg značenja za kompaniju, kao i ona koja su spojena direktno na Internet.

6.4. Zaštita mreža

Kako naša mreža raste tako raste i kompleksnost administriranja svih računala. Osnovna odlika mrežnoga modela sigurnosti je kontrola pristupa mreži, koja obuhvaća kontrolu pristupa pojedinim računalima, kao i servisima s određenih destinacija te gradnju firewall-a, pri čemu želi zaštititi svoje interne resurse i mrežu.

6.5. Metoda zaštite putem Internet Firewall

FireWall je veoma siguran način zaštite mreže, koji segmentira i štiti našu internu mrežu od opasnosti i mogućih uljeza od strane Interneta, a ima nekoliko osnovnih namjena: *ograničava ljude da mogu ući u našu mrežu samo kroz strogo kontroliranu točku, spriječava hakere da se približe ostalim oblicima zaštite unutar mreže, ograničava ljude da izlaze iz lokalne mreže kroz strogo kontroliranu točku*

Najčešće predstavlja točku pomoću koje se interna mreža spaja na Internet. Sav dolazni i odlazni promet prema i od Interneta prolazi kroz firewall. Koristeći se tom činjenicom koristimo ga kao slavinu ili filter kojim ćemo kontrolirati, te propuštati ili ne specifičan tip prometa. Kada god dođe do bilo kojeg zahtjeva za specifičnim tipom prometa (mail, ftp, telnet) takav promet se propušta ili blokira zavisno o predefiniranim pravilima koja pak ovise o politici zaštite određene kompanije. Politika zaštite je ovisna o specifičnostima određene kompanije i različita od kompanije do kompanije.

Firewall predstavlja separator, filter i analizator. Fizička implementacija ovisi od kompanije do kompanije, a najčešće objedinjuje niz hardverskih (router-a, kompjutera) i softwerskih komponenti (specijalni programski paketi). Postoje različiti načini konfiguracije opreme, a oni ovise o politici zaštite, te raspoloživim sredstvima.

Firewall je jako rijetko fizički jedan elemenat opreme, iako su se u novo vrijeme pojavili novi komercijalni produkti koji teže za time da se svi elementi dobroga firewall-a objedine u jednom fizičkom uređaju.

Najčešće firewall predstavlja niz nezavisnih uređaja koji ne moraju imati isključivu namjenu za sigurnost mreže. Iako se u većini slučajeva koristi za zaštitu od Interneta, kod velikih kompanija mogu se koristiti i za separaciju pojedinih znatno osjetljivijih dijelova mreže.

6.5.1. Uloga Firewall-a

Firewall može napraviti mnogo na zaštiti računala od toga da zaštitu mreže fokusira u jednu mrežnu točku, koristi zaštitu kroz ograničenje korisnika i servisa te zaštite koja podrazumjeva bilježenje svih aktivnosti iz mreže i u mrežu.

Zaštita mreže fokusirana u jednoj mrežnoj točku. Firewall nam daje velike mogućnosti kontrole prometa koji prolazi kroz tu jedinstvenu točku mreže. Fokusiranje sigurnosti na takvu jednu pristupnu točku znatno olakšava administraciju.

Zaštita kroz ograničenje korisnika i servisa. Mnogi servisi koje ljudi žele koristiti na Internetu često su dosta nesigurni. Korištenjem firewall-a mi ograničavamo korištenje servisa na samo one koji su sigurni i provjereni, te odgovaraju definiranoj politici zaštite kompanije.

Zaštita bilježenjem svih aktivnosti iz mreže i u mrežu. Pošto firewall predstavlja jedinstvenu točku kroz koju se ostvaruje promet iz mreže i prema mreži, on predstavlja dobro mjesto skupljanja informacija o prometu prema vanjskoj mreži i od nje.

6.5.1.1. Mane Firewall-a

Firewall je jako dobar oblik zaštite od mogućih hakera iz vanjskoga svijeta, ali ne predstavlja kompletno sigurnosno rješenje. Ako želimo potpunu zaštitu moramo objediniti različite tipove zaštite u jedanu jedinstvenu cijelinu: *zaštita računala + fizička zaštita + obrazovanje korisnika.* No, Firewalla vas ne može zaštititi od: nestašnih korisnika unutar mreže, veza koje ne idu preko njega, novopronađenih načina provale i virusa.

Firewall nas ne može zaštititi od nestašnih korisnika unutar mreže. Firewall može zaštititi sistem od slanja osjetljivih informacija mrežom izvan kompanije. Ali isti korisnik može željene informacije prebaciti na disk, traku ili ispisati na papir. Ako je haker stvarno unutar naše mreže, firewall nam ne može nikako pomoći. Korisnici koji se nalaze unutar naše mreže mogu lako ukrasti informacije, oštetiti resurse, bili hardwerske, bilo softwerske, modificirati program ili bazu, a da nikada ne pristupe firewall-u. Od uljeza iznutra treba se zaštititi internim mjerama sigurnosti, kao što je zaštita računala, fizička zaštita, te obrazovanje korisnika.

Firewall nas ne može zaštititi od veza koje ne idu preko njega. Iako on uspješno štiti i prati sve veze koje idu preko njega, ne može ništa učiniti s prometom koji ide mimo njega. Firewall ne može učiniti baš ništa ako haker uspije doći do naše kompanije preko računala povezanog preko modema. Zato nije čudno što većina kompanija zabranjuje spajanja PC putem modema na Internet. Tako je česta pojava da tehnički eksperti postavljaju, stražnja vrata u njihovu mrežu, pošto postoji veliki broj restrikcija takvoga pristupa preko Interneta. Međutim takve konekcije, ma koliko god bile tajne predstavljaju veliku opasnost sigurnosti mreže.

Firewall nas ne može potpuno zaštititi od novo pronađenih načina provale. Firewall je konstruiran tako da nas štiti od poznatih tipova provala, a često nas može zaštititi i od novih tipova, na način da propuštamo samo poznate i provjerene tipove servisa čime izbjegavamo mogućnost da korištenje nekog novog i nesigurnog servisa dovede do narušavanja sigurnosti. Periodično ljudi otkrivaju nove nedostatke i načine da iskoriste već uveliko korištene i pročešljane servise, kao i primjene nove tehnike i načine upada.

Firewall nas ne može zaštititi od virusa. Firewall ne može zaštititi našu mrežu i računala od mogućih virusa. Premda mnogi firewall-ovi skeniraju sav dolazni promet. To se uglavnom svodi na skeniranje zaglavlja paketa (određivanje porta i IP adrese), a ne samog sadržaja paketa. Ako koristimo i znatno sofisticiranije tipove firewalla (proxy), detekcija virusa bi bila jako dugotrajan i mukotrpan posao. Postoji previše različitih vrsta virusa i načina da se oni sakriju tako da bi to stvarno bilo jako teško odrediti. Detekcija virusa u slučajnom paketu koji prolazi kroz firewall također bi bila veoma teška, zato što:treba odrediti: *da li je paket dio programa, kako bi trebao program izgledati, da je promjena uzrokovana virusom*

Čak i prvi od zahtjeva predstavlja izazov. Većina firewall-a su "mašine" za zaštitu raznolikog tipa s raznolikim izvršnim formatima. Paketi poslani pomoću mail-a, ili usernet-a mogu također biti prisutni u nekoliko različitih formata.

Radi svih ovih razloga, firewall-u je jako teško detektirati viruse i oni se često prođu mimo njega bez obzira kako dobro on bio izveden.

Ako napravio savršenu zaštitu od virusa u sklopu firewall-a, i da ne postoji mogučnost da se virusom računala zaraze pomoću nekog drugog izvora zaraze. Ne možemo se nikako zaštititi od nekih znatno češćih izvora zaraze tipa: *skidanja softvera modemom, softwera donesenog na disketi ili disku od kuće ili s drugoga izvora, originalnog softwera koji je zaražen virusom u tvornici.*

Najpraktičniji način zaštite od virusa je zaštita vezana za računalo, tako da se na sva računala ili grupu računala od posebnog interesa postavi odgovarajuči softver za zaštitu od virusa, te pravovremena edukacija korisnika o opasnosti od virusa, njegovim posljedicama, te mjerama protiv njega.

7. KORIŠTENJE KOMBINACIJA TEHNIKA ZAŠTITE

Pravo rješenje za firewall je rijetko obuhvaćeno korištenjem jedne tehnike, nego najčešće obuhvaća niz tehnika, čija bi kombinacija omogućila riješenje većine znanih nedostataka i problema. Vrsta problema uvelike ovisi o tome koje servise želimo osigurati našim korisnicima i koji nivo rizika pritom želimo preuzeti. Neke protokole (Telnet, SMTP) moguće je znatno bolje štititi koristeći filtriranje paketa, dok neke tipa (FTP, WWW, Archie, Gopher) znatno bolje je izvesti pomoću proxy-ja. Proxy servisi su specijalizirane aplikacije ili serverski programi koji se izvršavaju na računalu u sklopu firewall-a, bilo da se radi o: *računalu s dva mrežna adaptera,* od kojih je jedan spojen na internu, a drugi na eksternu mrežu ili *računalu koji ima jedan mrežni adapter (*računala koja

posjeduju jako dobru zaštitu, jer su najizloženija otvorenom vezom prema Internetu - *bastion host*), kojem se može pristupiti i s Interneta i s interne mreže.

Ti programi prihvaćaju korisnički zahtjev od starne Interneta (na primjer, FTP ili Telnet) i prosljeđuju ih, zavisno o sigurnosnoj politici do stvarnih servisa. Većina danas korištenih firewall-ova koristi kombinaciju ovih dvaju tehnika. Najčešće korištene arhitekture firewall-a danas su:

Računalo s dva mrežna sučelja. Takvo računalo predstavlja router između mreža koje su spojene na njegove interface-e i vrši usmjeravanje IP paketa s jedne strane mreže na drugu i obrnuto. Međutim ako želimo da takvo računalo radi kao firewall moramo onemogućiti opciju direktnog prosljeđivanja To praktički znači da računala s jedne i druge strane ne mogu direktno komunicirati nego samo preko proxy servera koji se nalaze implementirani u firewall-u na računalu. Direktan promet između njih je blokiran.

Mrežna arhitektura za firewall s računalom s dvije mrežne kartice je jako jednostavna i definirana je tako da se računalo nalazi između dvaju mreža (Intraneta i Interneta) i svaka od njih je spojena na jedan interface.

Screened Host Archicture. To je arhitektura koja se sastoji od routera koji djeli eksternu od interne mreže i računalom (bastion hostom) koji se nalazi unutar interne mreže. Kod ove arhitekture primarna zaštita osigurana je pomoću filtriranja paketa, gdje filtriranje paketa onemogućava komunikaciju mimo proxy servera. Bastion host se nalazi unutar interne mreže. Filtriranje paketa na ulaznom usmjerivaču je definirano tako da računala izvan interne mreže vide jedino bastion host i samo dio dopuštenih servisa. Bilo koji sistem koji pokuša pristupiti internim sistemima ili servisima mora se spojiti na ovo računalo.

Usmjerivač mora biti konfiguriran tako da za interna računala, te dio servisa koji nemaju proxy servere na bastion hostu dopuštaju direktan pristup na Internet, a za sve ostale servise ga onemogućuju. To se može kombinirati zavisno o vrsti servisa, te sigurnosnoj politici kompanije, tako da određeni servisi i računala imaju direktan pristup, a drugi samo preko proxy servera.

Međutim uspoređujući ovu arhitekturu s na primjer sljedećom opisanom nalazimo i neke nedostatke. Glavni od njih je, da ako napadač uspije probiti računalo utvrdu, ne ostaje ništa drugo od sigurnosne opreme i mjera na njegovom putu prema ostatku interne mreže. Screen Subnet Arhitecture. Ova metoda dodaje još jedan nivo sigurnosti na prethodno opisanu metodu. Sastoji se od dva usmjerivača i proxy servera među njima. Mreža koja se formira na taj način između njih naziva se perimeter mreža i predstavlja dodatan stupanj zaštite interne mreže od eksterne. Znači jedan usmjerivač spojen je na vanjsku mrežu i perimeter, a drugi na unutarnju i perimeter mrežu.

"Računalo utvrda" prestavlja najosjetljiviju točku naše mreže pošto je direktno izloženo prema potencijalnim napadačima. Bez obzira na sve naše napore da zaštitimo to računalo ono će biti napadano jer je samom arhitekturom predviđeno za to. Jednom kada se provali to računalo čitava

interna mreža ostaje nezaštićena, naravno osim zaštite samih računala koja je obično jako slaba.

Spajajući "računalo utvrdu" na obrambenu mrežu, te tako izolirati od unutarnje mreže, možemo smanjiti opasnost i rizik koji nastaje probojem na "računalo utvrdu". Probojem računala omogučujemo napadaču pristup dijelu servisa, ali ne svim.

Da bi se napadač kod ove arhitekture probio do interne mreže, treba probiti oba usmjerivača. Ako napadač nekako i probije "računalo utvrdu", nema direktni pristup na internu mrežu nego mora probiti i unutarnji usmjerivač.

Nivo obrambene mreže. Obrambena mreža je dodatni nivo sigurnosti između vanjske i unutarnje mreže. Ako napadač uspješno probije prvi stupanj zaštite naše mreže (prvi usmjerivač) na raspolaganju nam ostaje dodatna zaštita (drugi usmjerivač).

Kod većine mreža moguće je s bilo kojeg računala u mreži promatrati sav promet prema svim računalima u dotičnoj mreži. Naravno to ovisi o tipu mreže koji se lokalno koristi (Ethernet, Token-ring, FDDI), kao i o internoj organizaciji iste. Pošto se u većini slučajeva koristi jedan od gore navedenih tipova mreža, osluškivač (SNIFER) jako lagano može doći do velike količine informacija, kao što je npr. lozinka (naravno ako nije provedena enkripcija, a najčešće nije). Ako i ne može doći do lozinke on može jako lagano vidjeti sadržaj neke osjetljive datoteke, kojoj korisnici pristupaju ili je prenose mrežom.

Interni promet (između dva računala interne mreže) neće se pojaviti u obrambenoj mreži, pa će i interni promet biti znatno sigurniji u slučaju da dođe do probijanja "računala utvrde", dok će naravno promet od vanjske mreže i prema njoj i dalje ostati vidljiv.

"Računalo utvrda". Ovo računalo je spojeno na obrambenu mrežu i predstavlja glavnu pristupnu točku unutarnje mreže prema vanjskom svijetu (npr. za protokole kao što su FTP, SMTP, DNS). Veza prema vanjskom svijetu može biti izvedena na dva načina: *definiranjem filtriranja,* tako da unutarnja računala imaju direktni pristup prema vanjskim, *postavljanjem proxy servera na računalu utvrdi*, omogučujući internim klijentima da pristupaju vanjskim serverima posredno preko proxy-ja (pritom treba paziti da interna računala mogu komunicirati samo preko proxy-ja s vanjskim svijetom).

Na "računalu utvrdi" vrte se najčešće dvije vrste servera, a to su: specijalizirani proxy serveri za (FTP, HTTP,...) te standardni servisi sa vlastitim predefiniranim proxy serverom (SMTP).

Unutarnji usmjerivač. Unutarnji usmjerivači imaju usnovnu namjenu štititi unutarnju mrežu od vanjske i obrambene mreže. Na unutarnjem usmjerivaču provodi se većina filtriranja paketa našeg firewall-a. On dopušta komunikaciju selektiranih servisa iz vanjskog svijeta prema unutarnjem i obrnuto. To su servisi koje naša kompanija može nesmetano koristiti bez opasnosti koristeći samo filtriranje paketa, a ne i upotrebu proxy-a. Nivo sigurnosti i sama definicija

sigurnog korištenja servisa, jako je različita i nezavisna od kompanije do kompanije. Servisi koji se obično uključuju u direktnoj komunikaciji prema van su Telnet, Ftp, Wais, Archie, Gopher, SMTP.

Servisi koji su obično dopušteni između računala utvrde i interne mreže često nisu dopušteni i između Interneta i naše interne mreže. Razlog limitiranja servisa između "računala utvrde" i unutrašnje mreže su reduciranje broja računala, ali i servisa na njima koji mogu biti napadnuti od strane "računala utvrde" ako ono bude napadnuto.

Vanjski usmjerivač ili pristupni usmjerivač štiti obrambenu i unutarnju mrežu od vanjske, a propušta skoro čitav promet prema van. Najčešće su pravila filtriranja paketa skoro identična na oba usmjerivača, tako da se greške na jednome od usmjerivača jako često preslikavaju i na drugi usmjerivač.

Jedina posebna pravila na vanjskim usmjerivačima, su ona koja štite računala na obrambenoj mreži, a to su "računalo utvrda" i unutarnji usmjerivač. Međutim to i nije toliko bitno jer su sami strojevi jako dobro zaštićeni svojom internom zaštitom, premda redudancija uvijek dobro dođe.

Za podršku proxy servisa, unutarnji će usmjerivač dopustiti unutarnjim računalima slanje nekih protokola sve dok ona komuniciraju s "računalom utvrdom", a vanjski usmjerivač će propuštati promet prema van sve dok taj promet dolazi od "računala utvrde".

Jedan od sigurnosnih zadaća koje vanjski usmjerivač može uspješno provesti je blokiranje svih paketa koji dolaze iz vanjske mreže, a najčešće se javljaju radi krivotvorenih paketa ili paketa koji su pogrešno usmjereni kroz neki pozadinski kanal i pri tom zaobilaze firewall. Takvi se paketi pretvaraju da dolaze od strane unutarnje mreže, a ustvari dolaze od strane vanjske.

8. ZAKLJUČAK

Kod same zaštite sustava problem je u tome kako zaštititi sustav, jer sama zaštita može unijeti određena ograničenja u radu korisnika. Sam cilj dobre zaštite bio bi maksimizirati zaštitu uz minimalni utjecaj na komociju korisnika.

U cijeloj priči postoji još jedan faktor koji ne možemo izostaviti, a to je cijena same provedbe određenog nivoa zaštite samog sustava.

Možemo konstatirati da je u ljudskoj prirodi da stvarima koje nam nisu od direktnog utjecaja u radnom procesu ne pridajemo toliko važnosti koliko bi u stvari trebali. Većina ljudi probleme minorizira sve do trenutka dok se nešto ne dogodi, a tada je obično već kasno.

Mi ne želimo neovlašten pristup računalu i korištenje naših informacija koje se kasnije mogu prodati nekome špijunu ili konkurentskoj firmi. Stoga treba maksimalno zaštititi pristup našoj unutrašnjoj mreži od strane Interneta čime čemo maksimalno otežati pristup podacima, te učiniti pristup što skupljim i rizičnijim.

PROTECTION OF COMPUTING RESOURCE WITH INTERNET FIREWALL

SUMMARY

Internet is the biggest invention in a history of mankind which was annotated 20. century and for surely mark future. Internet became a metaphor of world literacy and knowledge that can give us informations in the most fastes and easiest way no matter where they are.

People talk every day about misuse of Internet, but we most discuss about attack of vandals, hackers and others attackers in a security system of government and "seeding" of viruses in an e-mail and websites. But computers have their defensive mechanism wich can localize and withhold that attacking. One of that mechanism is firewall, component or group of components which can localize an approach between protected network and Internet, or two separated parts of network. Firewall is very trust way of protection but firewall isn't complitely security solution and because that we must use combination of protection.

Key words: Firewall, proxy, hackers, vandals,spy, Bastion Hostom, Screen Subnet Architecture, risk, router, stronghold computer

9. LITERATURA - REFERENCES

1. Cheswick, W. R.; Bellovin, S. M. Firewalls and Internet Security: Repelling the Wily Hacker, Addison-Wesley, 1994. (20.04.2002.)
2. Chapman, D.; Zwicky, Elizabet D. *Building Internet firewalls*, O'Reilly & Associates, Inc. - http://www.oreilly.com/catalog/fire2/
3. Linux Network Administrators Guide, Chapter 9. TCP/IP Firewall, http://www.tldp.org/LDP/nag2/x-087-2-firewall.html

Adrese autora - Authors' addresses:
Dubravka Šimunović, dipl. ing.
Agronomski fakultet Sveučilišta u Zagrebu
Zavod za matematiku i informatiku
Svetošimunska 25
10000 Zagreb
Croatia

Primljeno - Received:
03. 02. 2002.