Zaštita računarskih sistema
Vrsta: Seminarski | Broj strana: 21 | Nivo: Fakultet informacionih tehnologija, Banja Luka

Uvod
Razvoj Interneta doveo je do toga da je velik broj informacija dostupan korisnicima kod kuće, na poslu, u obrazovanju, što za mnoge nije samo prednost već i nužnost. Ta globalna umreženost dovela je i do niza problema zaštite podataka i sustava od nepoželjnih i zlonamjernih korisnika. Spajanjem privatne mreže na Internet izlažemo tu mrežu mogućim upadima izvana i zbog toga moramo razmišljati o zaštiti važnih podataka i sustava od mogućeg gubitka, oštećenja ili krade.
U slučaju da želimo zaštititi svoju lokalnu računalnu mrežu koju spajamo na Internet, upotreba vatrozida (eng. firewall) je nezaobilazna.
1.Šta je Firewall ?
Mora da implementira politiku sigurnosti. Ako određeno svojstvo nije dozvoljeno, Firewall mora da onemogući rad u tom smislu.
Firewall treba da bilježi sumnjive događaje.
Firewall treba da upozori administratora na pokušaje proboja i kompromitovanja politike sigurnosti.
U nekim slučajevima Firewall može da obezbijedi statistiku korišćenja.
Firewall može biti softverski ili hardverski :
Softverski firewall omogućava zaštitu jednog računara, osim u slučaju kada je isti računar predodređen za zaštitu čitave mreže.
Hardverski firewall omogućuje zaštitu čitave mreže ili određenog broja računara.
Za razumijevanje rada vatrozida potrebno je poznavati tri stručna pojma, a to su IP adrese i TCP i UDP portovi. IP adresa: Sve što je povezano na Internet ima barem jednu jedinstvenu IP adresu. To može biti adresa računala ili routera preko kojeg je lokalna mreža spojena na Internet. Svaki paket koji putuje Internetom u sebi sadrži svoju izvorišnu i svoju odredišnu IP adresu, tako da
.....NAMERNO UKLONJEN DEO TEKSTA.....
o otvoreno i što je manje adresa kojima ste dozvolili pristup, to je mogućnost zlonamjernog pristupa računalu manja.
Za ispravan rad firewall-a, potrebno je precizno odrediti niz pravila koja definišu kakav mrežni promet je dopušten u pojedinom mrežnom segmentu. Takvom politikom se određuje nivo zaštite koji se želi postići implementacijom firewall usluge.
2.Podjela potencionalnih napadača
2.1.Zaštita lokalne mreže od štetnog djelovanja “napadača“
Firewalli koji nemaju čvrste i stroge politike prema dolaznim paketima podložni su različitim vrstama napada. Ukoliko firewall ne podržava kreiranje virtualnih privatnih mreža, a organizacija želi omogućiti pristup sa određenih IP adresa lokalnoj mreži, moguće je konfigurirati firewall da propušta pakete sa tačno određenim izvorišnim IP adresama. Ali takav način postavljanja sadrži brojne nedostatke. Na primer napadač se može domoći paketa ,te saznati logičku adresu sa kojom je dozvoljeno spajanje na lokalnu mrežu. Nakon toga napadač može kreirati pakete kojim kao izvorišnu stavlja logičku adresu računara kojem je dozvoljeno spajanje i tako pomoću posebno prilagođenih paketa nanijeti štetu lokalnoj mreži.
Firewall je potrebno konfigurisati tako da onemogućava različite postojeće napade.Većina današnjih proizvođača firewalla ponosno ističe na koje napade su njihovi firewalli otporni, ali nove vrste napada se svakodnevno razvijaju i sve su komplikovaniji i kompleksniji. Ipak svaki firewall bi trebao biti otporan na poznate napade kao što su :