ZAŠTITA KOMPANIJSKIH PODATAKA U MREŽNOM I INTERNET OKRUŽENJU

COMPANY'S DATA PROTECTION IN THE NETWORK AND IN THE INTERNET ENVIRONMENTS

Andreja Aleksić

MUP R. Srbije P.U. Bor, Bor, Srbija

©MESTE

JEL kategorija: **D5, L86**

Apstrakt

Ovaj članak je namenjen, prvenstveno, menadžerima kompanija i njihovim I.T. menadžerima, sa ciljem da ih upozna sa opasnostima, neophodnošću i načinima zaštite računara, kao i celokupne kompanijske mreže od raznovrsnih pretnji koje sa sobom donosi elektronsko poslovanje u mrežnom i Internet okruženju. Krađe podataka od strane konkurentskih kompanija ili uništavanje podataka kompanije, stalne su pretnje svim kompanijskim računarskim mrežnim sistemima. Pritom je svejedno da li je mreža lokalnog karaktera ili je povezana sa Internetom. Neophodnost zaštite računara i računarskih mreža još uvek je marginalna tema u svesti mnogih menadžera. Problem leži u tome što ulaganje u opremu i softvere za mrežnu zaštitu, kao i njihovo unapređivanje, ne donosi vidljivu zaradu kompanijama. U mnogim zemljama, čak i kod ljudi na najvišim menadžerskim nivoima u kompanijama, zaštita se smatra nebitnom i, čak, bespotrebnom, naravno, dok se ne dogodi problem. Tada je već kasno, kompanija trpi štetu u finansijskim ili drugim oblicima. U radu su prikazani bitni elementi sistema zaštite računara i računarskih mreža.

Ključne reči: računarska mreža, zaštitni sistemi, zaštita mreža, sigurnost računara, bezbedna mreža, zaštitni zid.

Abstract

This article is intended primarily for company managers and their IT managers, with the aim of familiarizing them with the danger, necessity and the ways to protect themselves and the entire company's computer network from different threats; threats that endanger online business and Internet environment. Theft by competitive companies or ruining of business-company's data are constant threats to all corporate computer network systems, regardless whether the network is of a local character or is connected to the Internet. The necessity to protect computers and networks is still the marginal issue in minds of many of managers. The problem is that investments in equipment and software for network protection, as well as their upgrading, don't bring any obvious benefit to the company. In many

Adresa autora:

Andreja Aleksić

andrejaaleksic@gmail.com

companies, managers even at the highest management level consider the protection as unimportant and unnecessary, of course - until the problem appears. But, then, it is too late for the company not to suffer the damage in the financial and/or other ways. This work describes essential elements and methods of the computer system's protection and protection of computer networks.

Keywords: *computer network, protection systems, protection of networks, computer security, secure networks, firewall.*

1 UVOD

Moderan tržišni način poslovanja, čak i manjih kompanija, podrazumeva postojanje određenog broja računara koji su međusobno povezani nekom vrstom računarske mreže. Računari su svojom pojavom, sada sa već velikim kapacitetom memorije, brzinom rada, multimedijalnošću i jakom softverskom podrškom, u svim sferama poslovanja drastično ubrzali i olakšali rad, kao i međusobnu komunikaciju zaposlenih u kompaniji. Omogućili su neprestano praćenje aktivnosti i rezultata, ali i brzo i efikasno korigovanje svih segmenata kompanije. Sam način poslovanja često diktira obavezu povezivanja tih istih računara na globalnu mrežu – Internet. Poslovanje kompanije u mrežnom i Internet okruženju podrazumeva korespondenciju među kompanijama kroz razmenu elektronske pošte, ponudu dobara i/ili usluga koje kompanija nudi, Internet prezentaciju istih, brze i efikasne elektronske Internet bankarske usluge, pretraživanje, praćenje i anketiranje tržišta u sferi poslovnih interesa kompanije, kao i mnoge druge benefite koje Internet nudi.

Internet, uz sve prednosti koje pruža, poseduje i svoju mračnu stranu, koja se ogleda u nastojanju hakera da, pomoću zlonamernih programa i veština, dopru do kompanijskih podataka, koje potom prodaju konkurenciji, unište trajno ili zaključaju (šifriraju podatke ključem na način koji samo oni znaju) i nakon toga iznude novac za njihovo otključavanje. Ne mora haker da se usredsredi na određenu kompaniju. Postoji mnogo malih zlonamernih programa koji se prenose elektronskom poštom – prikačeni su čak i na zvanične sajtove velikih, u svetu poznatih, kompanija ili jednostavno "lutaju" Internetom, pa je dovoljno da jedan računar u unutrašnjoj mreži bude zaražen. Zlonamerni programi su kreirani tako da se sami prenose na druge računare u

mreži, pa svi računari u mreži bivaju zaraženi, te otvaraju put hakerima, uništavaju ili šalju podatke na neki spoljni računar.

Moramo biti svesni činjenice da poslovni podaci kompanije predstavljaju poslovnu tajnu i da iznošenje tih podataka iz kompanijskih okvira, bilo javnim objavljivanjem na Internetu ili dostavljanjem istih konkurentskim kompanijama, može naneti ogromne gubitke kompaniji, a može dovesti i do kraha kompanije.

Kompanijski računari moraju biti zaštićeni:

- instaliranim legalnim operativnim sistemima,
- antivirusnim programima i
- programima zaštitnog zida (firewall).

Ova tri softverska paketa moraju se redovno ažurirati u cilju zaštite od najnovijih oblika zlonamernih softvera.

Potrebno je zaštititi unutrašnju kompanijsku mrežu od lutanja virusa i neželjenog prenosa podataka kroz pravilno kreiranje parametara mreže i unutrašnjih sistema zaštite, a na obodu mreže, mestu ili mestima gde je unutrašnja mreža povezana na Internet, potrebno je postaviti višeslojne uređaje zaštitnog zida.

2 VRSTE I NAČINI NAPADA NA MREŽNE SISTEME

Da bi se bolje razumela potreba za postavljanjem i pravilnim podešavanjem zaštitnih sistema, neophodno je dobro poznavati štetne programe čiji je cilj da se provuku kroz zaštitne sisteme, "inficiraju" računar(e) u mreži i unutar mreže obave funkciju zbog koje su kreirani. Pod inficiranim računarom podrazumevamo računar u kome se nalazi neki od malicioznih softvera i koji je u mogućnosti da „uključiti“ svoje izvršenje u postupak izvršenja nekog programa instaliranog i operativnog u računaru. Osim virusa postoje i drugi štetni – zlonamerni programi. Ovde će biti

razmotrene neke najčešće grupe štetnih programa:

1. trojanski konji (engl. Trojans, Trojan downloaders, droppers),
2. crvi (engl. worms),
3. logičke bombe (engl. logic bombs)
4. zadnja vrata (engl. backdoors) i
5. virusi.

Trojanski konj – trojanac je program koji naizgled služi za neku drugu operaciju od one za koju je napravljen. Trojanski konj bi na primer bio program koji izgleda kao neki tekst procesor, a zapravo jednom pokrenut briše određenu ekstenziju sa hard diska. Autori virusa često koriste trojance kako bi olakšali razmnožavanje samog virusa. Trojanci predstavljaju jednu od komponenata malvera koja se ne razmnožava. (Klein & Godunov, 2006)

Crv je program koji se širi umnožavanjem samog sebe (Klein & Godunov, 2006) u kompjuterskim mrežama. Crv je samostalan i, za razliku od virusa, ne treba mu program domaćin da bi se aktivirao. Takođe, crva pokreće i kontrolu nad njim vrši sam autor.

Logička bomba je metoda aktivacije procesa na osnovu zadovoljavanja logičkog uslova – postojanja ili nepostojanja nekog podatka, protoka, određenog vremena ili po sistemu aktiviranja – u određeno vreme. Logička bomba, u suštini, predstavlja princip delovanja, a ne celoviti mehanizam. Logičke bombe su veoma često sastavni deo mnogih kompjuterskih virusa, ali se same ne razmnožavaju. (Klein & Godunov, 2006) Logičke bombe mogu i da budu način kojim se administratori bore protiv napadača. Administratori ponekad namerno ostave „pseudo greške“ (engl. pseudo flaws), takođe poznate kao medeni tokeni (engl. honey tokens), očigledne rupe u operativnom sistemu, koje izgledaju ranjive na napade, ali u stvarnosti deluju kao alarmi ili pokretači automatskih radnji kada uljez pokuša da iskoristi grešku. (sgi, 2003)

Zadnja vrata predstavlja posebnu "nevidljivu" funkciju programa koja se može pokrenuti na unapred određen način ili nakon određenog perioda (recimo prestanak besplatnog perioda korišćenja nekog programa). Takođe, programeri koji pišu programe često ubace posebnu lozinku

ili sekvencu znakova, koja kada se ukuca omogućava pristup do nevidljivih funkcija programa. Zadnja vrata se mogu postaviti kao pratilac Trojanaca ili crva. (Dabić, 2010)

Virus se može posmatrati kao deo nekog programskog koda koji je sposoban za izvršenje samokopiranja (infekcija) dodavanjem svog sadržaja u druge programe ili delove operativnog sistema. Primećuje se zaista velika sličnost između kompjuterskih i bioloških virusa. Virus se obično sastoji od dva dela. Prvi deo je samokopirajući kod, koji omogućava razmnožavanje virusa, a drugi deo je korisni teret (payload) koji može biti bezopasan (benigni) ili opasan (destruktivan, maligni). Kreatori virusa koriste uglavnom ove tri osnovne tehnike kojima nastoje da prikriju postojanje virusa u računaru:

- **enkripciju** – šifriranje dela virusnog koda,
- **polimorfizam** - preoblikovanje izvršnog koda, na način da se očuva funkcija virusa, ali istovremeno bitno promeni izgled virusa i
- nevidljivost, samosakrivanje (**stealth**)".

Definicije štetnih programa su preuzete sa Internet stranice (Sunnis, 2003, 08 23) .

Iz prethodnog dela vidimo da vrlo često sami autori korisnih programa, zbog zaštite svojih prava, uz instaliranje korisnih programa postavljaju i zamku – logičku bombu, ili, ponekad, i kompletan virus. Osim ovog načina, u današnje vreme se dva načina inficiranja smatraju za najčešći vid inficiranja računara, i to:

- putem Interneta (surfovanje Internetom, razmena mejlova, deljenje podataka iz samog računara, omogućavanje direktnog pristupa putem programa (dameware, remote desktop i sl.)) i
- putem prenosivih medija (flash usb, CD, DVD, prenosivi hard-diskovi i sl).

Na slici 1 se vidi da virusi na računarskim mrežama ne predstavljaju najveći sigurnosni rizik modernog kompanijskog poslovanja danas, a najverovatnije ni u budućnosti. Primat su preuzeli drugi oblici napada, pre svih Trojanci i crvi. Crvi su štetni programi koji se šire računarskim mrežama i računarima, a da pritom ne inficiraju druge programe. Crvi upotrebljavaju računarsku mrežu da bi se širili, danas najčešće na adresu.

primaoca stižu u vidu dodatka poruke elektronske pošte. Drugi način širenja crva je da oni za svoje

širenje koriste različite sigurnosne probleme za koje ne postoje "zakrpe"

Slika 1 Najčešće blokirane vrste malvera u svetu u prvoj polovini 2014.

Izvor: Autor na osnovu (statista, 2015)

Osim do sada opisanih vrsta zlonamernih programa, metoda infekcije i širenja štetnih programa, postoje i mnoge druge metode napada. Zahvaljujući multimedijalnosti Internet okruženja, zaštitni sistemi moraju da dozvole prolaz novim vrstama servisa, tj. Internet usluga, a samim tim otvaraju se vrata novim načinima širenja zlonamernih programa.

3 CRYPTOWALL – PRIMER DESTRUKTIVNOG TROJANSKOG KONJA

Trojanski konj pod imenom cryptowall se više od pola godine nalazio u vrhu liste opasnih malvera, destruktivnog po kompanijske elektronske podatke, čiji kod nije bio "otvoren" skoro godinu dana. Kao zlonamerni program prvi put je detektovan od strane antivirusnih programa na računarima juna 2014. godine.

Cryptowall svoj sadržaj maskira u naizgled bezopasni fajl ili bezopasnu aplikaciju. Prenosi se masovnim spam kampanjama, elektronskom poštom, ili pristupom sajtovima koji nude naizgled bezopasne dodatke, malicioznim dodacima ili drugim malverom. (O'Brien & Morparia, 2014)

Kada se jednom aktivira na računaru domaćinu, virus radi u dva pravca. Sa jedne strane, nepredvidivim redosledom traži udaljene servere gde bi preneo svoj sadržaj i umnožavajući sebe širio zarazu. Sa druge strane, virus napada sve vrste ekstenzija na računaru domaćinu, menja – kriptuje ih, i samim tim onemogućava dalji pristup tom dokumentu. Virus koristi 2048-bitni RSA ključ.

Pri pokušaju otvaranja zaražene datoteke, aktivira se Internet veza (HTML link) koja korisnika zaraženog računara dalje vodi po sistemu korak po korak načinu plaćanja. Uglavnom se prvo dolazi do cifre od 500\$/€ koju je potrebno uplatiti da se dobije ključ za otvaranje zaraženih fajlova na računaru. Ovaj ključ važi samo za taj jedan računar. Period u kome je moguća uplata 500\$ traje tri dana, ako se ne uplati u tom roku, sledeći iznos je 1000\$, i daju se još sedam dana za uplatu. Nakon ovog perioda, u slučaju da se ne uplati traženi novac, zaražena ekstenzija postaje trajno neupotrebljiva – uništena.

Slika 2 Geografska zastupljenost virusa cryptowall

Izvor: (O'Brien & Morparia, 2014)

Kao što vidimo na slici 2 virusom Cryptowall je zaraženo najviše računara u SAD-u, Japanu i

nešto manje u Australiji, to nam govori da je kreator virusa targetirao bogata tržišta na kojima „nastupa“. Ostatak sveta mu nije interesantan, te za skoro godinu dana kreator virusa maltene nije širio virus na finansijski slabija tržišta. Opšte poznata činjenica je da se u ekonomski slabijim tržištima ili ulaže malo ili ne ulaže uopšte u sredstva za zaštitu računarskih sistema, te su računari tih zemalja podložniji širenju virusa.

Do sada nijedna antivirusna kompanija nije objavila da je uspela da „razbije“ osnovni kod virusa, što znači da ne može da zaštiti računare svojih klijenata od uništavanja podataka. Većina kompanija koje nude, u okviru svojih antivirusnih programa, program (removal tool) za uklanjanje virusa, je u drugoj polovini prošle godine poslala upozorenje svojim klijentima sa ukazivanjem na opasnost i destruktivnost ovog virusa. Poslali su i preporuku da se sva bitna elektronska dokumenta sačuvaju (backup), i da se sigurnosna kopija dokumenata drži na nekom drugom računaru ili na dvd, cd i drugim spoljašnjim skladišnim uređajima. To je jedini mogući i pravilni način zaštite podataka. Ova preporuka važi i sada.

4 KOMPANIJSKI ZAŠTITNI SISTEMI

Na nivou kompanije zaštita celokupnog računarskog sistema može se podeliti u tri osnovne celine:

- Zaštita samog računara, servera, radne stanice.
- Zaštitni mehanizam unutrašnje kompanijske mreže.
- Zaštita kompanijske mreže po obodu ka Internetu.

4.1 Zaštita kompanijskih računara

Ova zaštita se smatra najnižim nivoom zaštite u sistemu. I pored ovakvog statusa potrebno joj je posvetiti dosta pažnje iz više razloga. Sastoji se od pravilno izabranog antivirusnog programa i instaliranog zaštitnog zida. Oba segmenta zaštite samog računara moraju biti pravilno podešena od strane sistem administratora tako da štite računar, a ne blokiraju rad kompanije, kao celokupnog računarskog sistema.

Pod pravilnim podešavanjem se podrazumeva da korisnik preko svog računara može neometano da pristupi dozvoljenim datotekama na drugim računarima, serverima kompanije, da vrši unos podataka na kompanijske servere, kao i da se dozvoli pristup određenim datotekama na samom računaru kroz izuzeća u zaštitnom zidu. Podrazumeva se da je operativni sistem računara legalan i da mu je dozvoljeno ažuriranje. Isto važi i za antivirusni, kao i za softver zaštitnog zida računara.

Dobra opcija je kupovina antivirusnog i programa zaštitnog zida na nivou kompanije sa licencama za potreban broj računara. U tom slučaju bi dnevno ažuriranje ovih programa preuzimao kompanijski server, dok bi radne stanice preuzimale ažuriranje sa tog servera. Na taj način se rasterećuje unutrašnja mreža (i protok ka Internetu), i ne otvaraju se dodatna izuzeća u kompanijskom zaštitnom zidu.

Nekoliko godina unazad prodaju se i alati (tipa HitmanPro Removal Tool, W32.Pasobir Removal Tool, W32.Ramnit Removal Tool, Kaspersky Virus Removal Tool i slični), namenjeni uklanjanju štetnih (spyware, malware...) programa kojima je cilj slanje podataka na Internet, a sa kojima antivirusni programi ne mogu da se izbore. Ovakvi programi rade tako što se prilikom uključivanja računara, odmah nakon podizanja sistema, kreće sa radom i alat – program koji izvrši skeniranje svih programa koji pokušavaju da izađu na mrežu i nakon poređenja sa svojom bazom, u kojoj je lista štetnih programa, uklanja ih iz operativnog sistema računara. Nakon skeniranja (koje traje obično manje od pet minuta) i eventualnog uklanjanja pretnji po sistem, program se u potpunosti isključuje i ne opterećuje resurse računara, do narednog uključivanja ili drugog termina skeniranja zavisno od podešavanja.

Koristan je i alat koji uvek prilikom priključivanja USB memorijskih uređaja pretražuje iste u potrazi za štetnim programima (USB scan tool) i, ukoliko je neophodno, blokira ih. Ovaj alat je stalno aktivan u pozadinskim procesima, zauzima veoma malo resursa računara. Problem je taj što korisnike nervira čekanje nakon priključivanja USB uređaja, posebno ako je uređaj većeg memorijskog kapaciteta. (Notenboom, 2011)

4.2 Zaštitni mehanizam unutrašnje mreže

Pri kreiranju sigurne kompanijske mreže moramo mnogo faktora uzeti u obzir. Osnovni faktori su: veličina mreže (broj radnih stanica, računara, servera), razuđenost mreže, potreba za VPN servisima, sama struktura delatnosti kompanije, pristup Internetu kroz jedan ili više pravaca, postojanje fax – 56K modema u računarima...

Najbitniji deo zaštite računarskih mreža je zaštitni zid. Zaštitni zid je u suštini softver ili hardver koji proverava informacije koje dolaze sa Interneta ili neke druge mreže, bilo otvorenog ili zatvorenog tipa, i zatim ih blokira ili im dozvoljava da prođu do računara, u zavisnosti od postavki zaštitnog zida i mesta na mreži na kom je postavljen uređaj. Zaštitni zid sprečava zlonamerni softver ili hakere da pristupe računaru putem unutrašnje mreže ili Interneta. On takođe sprečava računar u pokušaju slanja zlonamernog softvera na druge računare. Na ovaj način kroz svoje protokole zaštitni zid vrši kontrolu rada mreže.

Bitan faktor zaštite unutrašnje mreže je taj da se podaci (datoteke) bitni za rad kompanije ne nalaze na računarima koji vrše ulogu radnih stanica, već su smešteni na kompanijskim serverima. To su namenski računari koji skladište kompanijske podatke i na kojima su kreirane baze podataka. Programi instalirani na radnim stanicama koriste baze podataka smeštene na serverima u redovnom obavljanju radnih zadataka. Kompanijski serveri vrše redovno rezervno skladištenje baza podataka smeštenih na njima. Takođe, serverski računari se prave tako da omogućavaju brz mrežni pristup podacima, a stabilnost u radu ovih računara je daleko veća u odnosu na obične radne stanice. Većina njih u sebi sadrži po nekoliko mrežnih kartica, po dva ili više procesora na matičnoj ploči, a hard diskovi su velikog kapaciteta, brzi i u paralelnom (raid) režimu rada.

Neophodno je da se za korisnike sistema, ljude koji pristupaju mrežnim resursima preko svojih ličnih ili kompanijskih računara, kreiraju korisnički nalozi sa precizno utvrđenim nivoima i dozvolama za pristup serverima, bazama podataka i aplikacijama. Na serveru bi se čuvali podaci o vremenu prijavljivanja (log fajlovi) na mrežu, odjavljivanja sa nje, a pamtilo bi se svako

pristupanje podacima koji se smatraju za kompanijski poverljive podatke.

Glavna čvorišta mreža i mrežni serveri smešteni su u čistim i klimatizovanim prostorijama. Na strujno napajanje vezani su preko uređaja koji omogućavaju neprekidno i stabilno napajanje, u slušaju nestanka struje i strujnih udara. Pristup ovim prostorijama i samim uređajima ima isključivo stručno osoblje.

Osim dobro tehnički koncipirane unutrašnje mreže, najbitnije je da sistem administrator(i) budu tehnički kvalitetno obučeni zbog pravilnog podešavanja sigurnosnih parametara na svim komponentama unutar mreže. Sistem administratori moraju redovno da prate i primenjuju izmene koje nude proizvođači softverskih i hardverskih rešenja zaštitnih uređaja. To se postiže kroz periodične obuke koje organizuju proizvođači ili distributeri opreme i programa, sa testiranjem i dobijanjem odgovarajućih sertifikata. Obaveza je sistem administratora da prate i primenjuju u što je moguće kraćem roku preporuke proizvođača zaštitnih sistema.

Menadžeri kompanija moraju imati sluha i za neophodne izmene na mrežnim uređajima i softveru, kao i na periodičnu zamenu samih zaštitnih uređaja kada više ne mogu da odgovore najnovijim pretnjama ili počnu da usporavaju rad drugih komponenti ili cele mreže. Tehnologije na I.T. tržištu veoma brzo zastarevaju, u proseku na pet do sedam godina potrebno je obnoviti celokupan sistem, pre svega iz dva razloga – jedan je tehnička zastarelost i nemogućnost te opreme da svojim softverom odgovori potrebnim novonastalim zahtevima, a drugi je tehnička nepouzdanost opreme kojoj je radni vek, po fabričkim podacima, do sedam godina. Postoji mnogo primera gde zbog jedne mrežne komponente, čija cena ne prelazi 20\$, staje ogroman sistem čiji se gubici (kad ne radi) mere mnogo većim iznosima po minuti blokade. Menadžeri kompanija na zapadu su odavno shvatili da takav luksuz sebi ne smeju da priušte.

Preporuka je da se unutar kompanijske mreže na tačkama preseka postave hardverski uređaji zaštitnog zida koji bi onemogućili umnožavanje crva i ispitivanja portova, da ne bi došlo do

preopterećivanja, kočenja ili oscilovanja unutrašnje mreže.

4.3 Zaštita kompanijske mreže po obodu ka Internetu

Kompanijski računari, kao i cela kompanijska (unutrašnja) mreža, moraju da poseduju zaštitni zid na tački povezivanja sa Internetom. Zaštitni zid svojom kompleksnošću i pomoću više slojeva zaštite (kreiranje VPN krypto-tunela i drugi servisi) pruža jedinu pravu zaštitu računarskih sistema.

Zatvorene kompanijske mreže su prošlost. Danas je nezamislivo poslovanje kompanija u svim sferama tržišnog poslovanja bez korišćenja usluga koje nam pruža Internet. Pokušaji krađa elektronskih podataka od strane konkurentskih kompanija su nešto sa čim se kompanije moraju pomiriti, ali je veoma bitno da pravilnim izborom i podešavanjem parametara zaštitnog zida konkurenciji i hakerima ostave samo bezuspešne pokušaje ulaska u sistem.

Slika 3 Ilustracija uređaja zaštitnog zida
Izvor: (Tutoriali.org, 2014)

Zaštitni zid je softverski ili hardverski uređaj koji je praktično usko grlo, odnosno most između unutrašnje mreže i Interneta. Hardverski zaštitni zidovi se koriste za kreiranje kontrolnih tačaka bezbednosti (check points) na granicama unutrašnjih, odnosno privatnih kompanijskih mreža ili na samom računaru (softverski zaštitni

zid), koji je priključen na Internet kao primarna zaštita od napada hakera. Pravilno konfigurisan zaštitni zid je u mogućnosti da ispita svaki protokol kome je dozvoljen prolaz, a da ne sadrži ozbiljnije greške. Na taj način se unutrašnja mreža štiti od nepotrebnih rizika.

Zaštitni zidovi održavaju Internet konekciju što je moguće bezbednijom tako što ispituju i, nakon provere, odobravaju ili odbijaju svaki pokušaj povezivanja unutrašnje mreže i spoljne mreže, konkretno Interneta. Snažni zaštitni zidovi štite mrežu na svim softverskim nivoima (slojevima) - od sloja podataka do aplikativnog sloja.

Na slici 3 je prikazano pozicioniranje hardverskog zaštitnog zida u međumrežnoj komunikaciji, a slikovito je i opisana svrha postojanja zaštitnog zida. Zaštitni zid funkcioniše preko tri osnovna servisa i to:

1. filtriranje paketa – vrši se odbacivanje TCP/IP paketa neautentifikovanih postova, kao i pokušaji povezivanja na neautentifikovane servise,
2. prevođenje IP adresa (engl. network address traslation - NAT) unutrašnjih računara i na taj način sakrivanje od spoljašnjeg praćenja. Ovaj metod se zove i maskiranje/sakrivanje IP adrese,
3. Proksi (proxy) servisi – uspostavljaju se konekcije na visokim aplikacionim nivoima za unutrašnje računare, u cilju kompletnog prekida konekcija mrežnog sloja između unutrašnjih i spoljašnjih računarskih sistema.

Neki zaštitni zidovi obezbeđuju dodatne servise, koji mogu biti zasnovani na pretplati ili su kupljeni u paketu sa opremom, i nisu striktno povezani sa primarnom bezbednošću mreže, ali mogu biti i te kako korisni za kompanijsko poslovanje:

- filtriranje prema sadržaju – unutrašnjim korisnicima se vrši blokiranje pristupa određenim tipovima sadržaja prema kategorijama, npr. – pornografiji, sadržaju koji propagira govor mržnje, društvenim mrežama,
- skeniranje virusnih definicija – štetnih programa – zaštitni zid pretražuje dolazne nizove podataka u potrazi za virusima. Ovaj drugi servis zbog svog ažuriranja liste virusa

uglavnom zahteva pretplatu kod proizvođača zaštitnog zida.

O filtriranju paketa saobraćaja i prevođenju adresa smo ukratko rekli suštinu, dok podizanje i sam rad proksi servera zbog svoje kompleksnosti zavređuje da mu posvetimo nešto više pažnje u radu.

Prevođenje adresa (NAT) rešava mnoge probleme internet konekcije, ali ne i potpunu kontrolu prolaska podataka kroz zaštitni zid. Uz pomoć mrežnog monitoringa moguće je pregledati sav saobraćaj koji prolazi kroz zaštitni zid, na osnovu dobijenih informacija lako se može doći do informacija da zaštitni zid prevodi adrese i drugih računara. Hakeri na ovaj način mogu dobiti informacije za pristup TCP konekcijama ili za prolaz kroz zaštitni zid lažnom TCP konekcijom.

Proksi server aplikativnog sloja ovo u potpunosti sprečava. On omogućava potpunu zabranu protoka podataka protokola mrežnog sloja i daje dozvolu saobraćaju isključivo protokolima viših slojeva, kao što su HTTP, FTP i SMTP. Proksi server je specifična klijentsko-serverska kombinacija za odgovarajući protokol koji se koristi. Mrežni proksi je kombinacija mrežnog servera i mrežnog klijenta. Serverski deo protokola proksija prihvata konekcije klijenata unutar mreže, dok se klijentski deo protokola povezuje na javni server – Internet. Na slici 4 vidimo kako funkcioniše proksi server u praksi.

Slika 4 Proksi server

Izvor: (Tutoriali.org, 2014)

U poslovanju kompanija koje nisu smeštene u „krugu fabrike“, već imaju udaljene poslovne objekte ili jednostavno potrebu da uspostave komunikaciju sa udaljenim lokacijama – postoji više rešenja. Ranije su se takva povezivanja vršila zakupom „kanala ili vodova“, gde je to bilo moguće. Velika cena ovakvog povezivanja, kao i ne baš velika pouzdanost ovih veza, bili su razlozi da se iskoristi dostupnost, niska cena i pouzdanost Interneta za stvaranje virtualne privatne mreže” (VPN) uređaja. Ova vrsta zaštitnog zida je veoma popularna jer se sada već ne kupuje dodatna oprema kod krajnjih korisnika (računara na udaljenoj lokaciji), već se instalira softver zaštitnog zida koji u sprezi sa zaštitnim zidom u kompaniji podiže i kreira krypto tunel. Kripto tunel se kreira po principu korisnik-korisnik ili korisnik-kompanijska mreža kroz zaštitni zid na obodu mreže. Nije moguće povezivanje trećeg zaštitnog zida, te se postojanje trećeg korisnika smatra nedozvoljenim upadom i blokira se dalji saobraćaj. VPN zaštitni zidovi su ranjivi jedino prilikom uspostavljanja kriptotunela, ali to je izuzetno kratak period, i kroz višeslojne protokole, nakon uspostavljanja krypto tunela, haker se eliminiše. Slika 5 prikazuje povezivanje dve kompanijske mreže preko krypto tunela.

VPN mreže rade preko tri protokola i to PPTP, IPsec i L2TP protokola.

Metod šifrovane autentifikacije, posebno u kombinaciji sa drugim protokolima, pruža visok nivo bezbednosti kako unutar kompanijske mreže, tako i u komunikaciji sa udaljenim lokacijama.

Slika 5 Kripto tunel

Izvor: Autor

Šifrovana autentifikacija dozvoljava spoljnim korisnicima na Internetu da dokažu svoj identitet autorizovanih korisnika zaštitnom zidu i da tako ostvare konekcije kroz taj zaštitni zid ka unutrašnjoj mreži. Za šifrovanu autentifikaciju se mora koristiti neki od bezbednosnih autentifikacionih protokola. Kada se veza uspostavi može biti, a i ne mora, šifrovana, što zavisi od zaštitnog zida koji se koristi, i da li je instaliran dodatni softver na klijentu u cilju da se podrži krypto tuneliranje.

Ovaj vid zaštite se najčešće koristi u elektronskom bankarstvu kroz sigurnosni (https) mrežni protokol ka fizičkim i pravnim licima. Zbog moguće krađe uređaja krajnjeg klijenta (krađa laptop računara, sigurnosnog tokena, kartice...) koriste se dodatne zaštite kao što su sigurnosne kartice, tokeni, kao i više sigurnosnih lozinki koje se primenjuju u fazi uspostavljanja konekcije na različitim nivoima autentifikacije korisnika. U ovom slučaju konekcija meri vreme mirovanja i automatski vrši prekid konekcije nakon zadatog vremena, ukoliko se korisnik nepravilno isključi ili dođe do neplaniranog prekida konekcije. Vreme automatskog prekida uspostavljene konekcije u slučaju mirovanja nije duže od nekoliko minuta.

Kod elektronskog bankarstva, u slučaju hakerskog napada na krajnjeg klijenta i preuzimanja konekcije od strane hakera, kao dodatna mera zaštite se primenjuje zahtev za ponavljanjem (potvrđivanjem) elektronskog potpisa koji je uslovljen sigurnosnim protokolom, a koji je vezan za računar klijenta, tako da (teoretski) haker ne može da vrši transakcije po računaru, već može da ima samo trenutni uvid u stanje računa, bez prava na izmenu bilo čega vezanog za klijenta. Sadržaj ovog segmenta rada je urađen na osnovu dva tutorijala pruezetih sa (Tutoriali.org, 2014) (N/A, 2014) (Tong, 2011).

5 SMERNICE ZA POSTAVLJANJE EFIKASNOG ZAŠITNOG ZIDA

Pravni subjekti u današnje vreme, da bi održali nivo efikasne bezbednosti rada svojih unutrašnjih mreža, trebalo bi da postave zaštitne zidove na mrežnim granicama koji bi trebalo da imaju tri osnovne funkcije zaštitnog zida i to: Prevođenje adresa, Proksi i Filtriranje paketa.

Da bi funkcije zaštitnog zida dobro radile mora se redukovati broj servisa na zaštitnom zidu. Na ovaj način se redukuje kompleksnost softvera koji rade na računaru a samim tim se smanjuje mogućnost pada bezbednosti zbog grešaka operativnog sistema ili softvera za bezbednost. Kod Windows operativnih sistema se preporučuje isključivanje svih nepotrebnih servisa i podešavanje da se ručno startuju. Ne preporučuje se gomilanje servisa kao što su HTTP, FTP, Telnet i sličnih, na jednom računaru. Gomilanje servisa može biti opasno ako hakeri nađu slabosti u zaštitnom zidu. Bitno je sakriti i koji operativni sistem koristi vaš zaštitni zid.

Preporučuje se da se politika zaštitnog zida vrši preko jedne kontrolne tačke. Ukoliko postoji veći broj zaštitnih zidova u kompaniji, oni moraju biti identično konfigurisani. Veliku pomoć ovome daju osobine softvera za monitoring i upravljanje zaštitnim zidovima na nivou kompanije.

Većina savremenih zaštitnih zidova se koristi kao pre-konfigurisani računar sa odgovarajućim operativnim sistemom. Zaštitni zid dolazi kao konfigurisani uređaj, dok će možda biti potrebno da mu se podesi specifična politika bezbednosti kompanije u kojoj je postavljen. Zaštitni zidovi se proizvode da odgovaraju svim tipovima mreža.

Glavna prednost u korišćenju rasprostranjenog operativnog sistema kao osnove za zaštitni zid je ta što će njegov kod koristiti, a na taj način i proveriti i milioni korisnika. U ovom slučaju se greške u kodu brzo i lako pronalaze, a ispravke se pojavljuju mnogo brže. Manji proizvođači zaštitnih zidova ne mogu rešavati svoje greške ovako brzo, jer nemaju tehničkih uslova za to.

Međutim, uobičajeni operativni sistemi, posebno operativni sistemi Windows, trpe česte i teške udarce usled napada hakera zbog svog monopolskog uticaja u svetu. To postavlja Windows operativne sisteme na mesto broj 1. kao najkompromitovanije operativne sisteme, iako uniks i linux operativni sistemi nemaju bolju bezbednost.

Administrator mreže bi trebalo da bude upoznat sa korisničkim interfejsom i načinom da ispravno konfiguriše zaštitni zid. Novi zaštitni zidovi imaju mrežni grafički ili java interfejs, tako da se mnogo

lakše konfiguriraju od starijih zaštitnih zidova i moguće ih je konfigurirati sa udaljene lokacije.

Nijedna mreža povezana sa Internetom ne može biti potpuno sigurna. Zaštitni zidovi su naročito efektivni i zadržavaju hakere, međutim postoji mnogo različitih načina za zloupotrebu mrežnih konekcija, tako da nijedan metod nije apsolutno siguran. Velika greška mnogih administratora je u pretpostavci da će problem bezbednosti biti rešen ispravnim postavljanjem zaštitnog zida. Praksa je pokazala da nije tako. Zaštitni zidovi, takođe, ne mogu rešiti problem zaštite od protokola kojima je dozvoljen mrežni prolaz (recimo Windows IIS). Kada uspostave kontrolu na mrežnom serveru hakeri mogu koristeći taj server da napadnu kompanijsku unutrašnju mrežu, ukoliko ih ne spreči dodatna bezbednosna politika integrisana u zaštitnom zidu.

Još jedna pretnja bezbednosti računarske mreže ogleda se u skrivenim prolazima na granici ka Internetu, pomoću jeftinih *dial-up* 56K modema. U današnje vreme upotreba ovih modema je svedena na prijem i slanje fax dokumenata, što ne znači da modem ne može da se iskoristi od strane hakera.

Povremeno se rade izmene programa, koji su priključeni na Internet i dozvoljen im je pristup osetljivim sistemskim ekstenzijama u računaru korisnika, od kojih su neke kozmetičke, korisničke izmene, a druge izmene su u stvari zakrpe sa ciljem onemogućavanja neželjenog pristupa hakerima. Zakrpe se rade uglavnom tek kada se utvrdi da su hakeri pristupili nekom računaru (konkretno hiljadama računara). To su problemi koji su uvek novi i za koje je potrebno iznaći novo rešenje.

Takođe, ne treba deliti, odnosno dozvoliti pristup hard diskovima na radnim stanicama, ako za to ne postoji potreba, te treba blokirati aplikacije kao što su skajp, tviter, fejsbuk i slične, koje koriste trenutno prevlačenje podataka (streaming) ili razmenu podataka u realnom vremenu.

Da bi se ponudile informacije o kompaniji, bolje je koristiti FTP i mrežne servise javnih agencija, nego računare na unutrašnjoj mreži. Ovakav način kompaniju štiti od rizika neovlašćenog pristupa unutrašnjoj mreži.

U novije vreme pojavili su se takozvani „enterprise firewall“ proizvodi koji dele jednu centralnu politiku zaštitnog zida na više zaštitnih zidova. Ovi uređaji dozvoljavaju da se zadrži centralna kontrola bezbednosne politike, bez brige o tome da li je politika korektno implementirana na svakom zaštitnom zidu u vašoj organizaciji. Politika ovakvog zaštitnog zida je zasnovana na bezbednosti radne stanice, a zatim replikovana na svaki zaštitni zid organizacije, koristeći neke od metoda bezbednosne autentifikacije. Ovakva vrsta zaštite je veoma korisna kompanijama koje rade u više država/kontinenata zbog konstantne otvorenosti prema Internetu na mnogo različitih lokacija, jer je poznato da svaka država ima drugačiju politiku pristupa Internetu.

Ovo su osnovne preporuke koje imaju za cilj zaštitu unutrašnjih mreža od napada preko Interneta. Praksa pokazuje međutim, da je u današnje vreme, veoma teško ispoštovati ih u potpunosti, tako da kompanija mora da planira i ulaže sredstva za sigurnosne sisteme od kojih je zaštitni zid zasigurno najbitniji segment zaštite unutrašnjih mreža. (Goncalves, 1998)

6 ZAKLJUČAK

Poznato je da Internetom kruži ogroman broj štetnih programa – virusa, i da je njihov broj svakim danom sve veći. Internet kroz stalno otvaranje novih, nadogradnju i izmene postojećih servisa, hakerima stvara uvek nove načine da pristupe korisničkim računarima.

Zaštita kompanijskih i privatnih računara je duži niz godina unazad postala sastavni deo u svim operativnim sistemima.

Pravilno kreiranje kompanijskih mreža i mrežnog pristupa Internetu postao je preduslov za funkcionisanje kompanija danas. Kroz sisteme antivirusnih programa, višeslojnih, unutrašnjih i ka Internetu postavljenih hardverskih i/ili softverskih rešenja zaštitnih zidova, kao i kroz redovno kreiranje sigurnosnih kopija baza sa svojim (kompanijskim) podacima – omogućava se stabilno i operativno funkcionisanje svih segmenata i korisnika mreže.

Treba imati na umu da je pravilno konfigurisana i zaštićena mreža veoma bitan faktor za normalan

rad ogromnog broja kompanija, te da stvoriti nesagledive posledice kako na finansije, bezbednosni propusti na mrežnom nivou mogu tako i na ugled i reputaciju kompanije.

CITIRANI RADOVI

Dabić, I. (2010). *Malware*. Lulu.com.

Goncalves, M. (1998). *Firewalls Complete*. McGraw-Hill.

Klein, A., & Godunov, A. (2006). *Introductory Computational Physics*. Cambridge University Press.

N/A. (2014, 09 29). *Zastitni_zid_sa_Openbds*. Preuzeto sa Tutoriali.org: http://tutoriali.org/Zastitni_zid_sa_Openbds.html

Notenboom, L. (2011). *Internet Safety: Keeping your Computer Safe on the Internet*. Puget Sound Software.

O'Brien, L., & Morparia, J. (2014, Jun 19). *Trojan.Cryptowall*. Retrieved from symantec: http://www.symantec.com/security_response/writeup.jsp?docid=2014-061923-2824-99

sgi. (2003, 12 04). *Appendix A. Glossary of Computer Security Terms*. Retrieved from techpubs library: http://techpubs.sgi.com/library/tpl/cgi-bin/getdoc.cgi?coll=0650&db=bks&fname=/SGI_EndUser/TCMW_UG/apa.html

statista. (2015). *Most commonly blocked types of malware worldwide as of 1st half 2014*. Retrieved from statista - The Statistics Portal: <http://www.statista.com/statistics/204434/most-frequent-malware-propagation-methods/>

Sunnis, S. a. (2003, 08 23, 08 23). *Zastita tutorijal*. Preuzeto sa <http://www.scribd.com>: <http://www.scribd.com/doc/255814296/Zastita-Tutorijal-by-Sunnis#scribd>

Tong, A. (2011, April 11). *Cisco IPsec VPN – IOS site-to-site Virtual Tunnel Interface VTI*. Retrieved from alfredtong.com: <http://www.alfredtong.com/cisco/ipsec-vpn-cisco-ios-site-to-site-virtual-tunnel-interface-vti/>

Tutoriali.org. (2014, Oct 29). *Firewall_u_praksi*. Retrieved from tutoriali.org: http://tutoriali.org/Firewall_u_praksi.html

Datum prve prijave: 02.06.2015.

Datum prijema korigovanog članka: 11.09.2015.

Datum prihvatanja članka: 13.09.2015.

Kako citirati ovaj rad? / How to cite this article?

Style – APA Sixth Edition:

Aleksić, A. (2016, januar 15). *Zaštita kompanijskih podataka u mrežnom i Internet okruženju*. (Z. Čekerevac, Ur.) *FBIM Transactions*, 4(1), 1-12. doi:10.12709/fbim.04.04.01.01

Style – Chicago Sixteenth Edition:

Aleksić, Andreja. 2016. „Zaštita kompanijskih podataka u mrežnom i Internet okruženju.“ Urednik Zoran Čekerevac. *FBIM Transactions* (MESTE) 4 (1): 1-12. doi:10.12709/fbim.04.04.01.01.

Style – **GOST** Name Sort:

Aleksić Andreja Zaštita kompanijskih podataka u mrežnom i Internet okruženju [Časopis] // FBIM Transactions / ur. Čekerevac Zoran. - Beograd : MESTE, 15 januar 2016. - 1 : T. 4. - str. 1-12.

Style – **Harvard** Anglia:

Aleksić, A., 2016. Zaštita kompanijskih podataka u mrežnom i Internet okruženju. *FBIM Transactions*, 15 januar, 4(1), pp. 1-12.

Style – **ISO 690** Numerical Reference:

Zaštita kompanijskih podataka u mrežnom i Internet okruženju. **Aleksić, Andreja.** [ur.] Zoran Čekerevac. 1, Beograd : MESTE, 15 januar 2016, FBIM Transactions, T. 4, str. 1-12.