CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Sigurnosni model mreže računala

CCERT-PUBDOC-2009-01-253

+CERT.hr u suradnji s LSS

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada je i ovaj dokument, koji je nastao suradnjom CARNet CERT–a i LS&S–a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr

Nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.LSS.hr

Laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Tokom 20. stoljeća tehnologija se razvijala u smjeru prikupljanja, obrade i distribucije informacija. Između ostalog, razvijene su svjetske telefonske mreže, radio i televizija, osobna računala i komunikacijski sateliti. Kao rezultat ubrzanog tehnološkog napretka spomenuta su područja međusobno konvergirala i razlike između prikupljanja, prijenosa, pohrane i obrade informacija nestaju. Organizacije sa stotinama ureda rasprostranjenih po cijelom svijetu redovno očekuju da imaju mogućnost pregleda stanja svojih poslovnica na pritisak tipke. Kako mogućnosti prikupljanja, obrade i slanja informacija rastu, sve brže rastu i zahtjevi za sve više profinjenim metodama obrade informacija.

Iako je računalna industrija još uvijek relativno mlada u usporedbi s ostalim industrijama, kao što je npr. automobilska, postignut je vratoloman napredak u vrlo kratkom vremenu. Tokom prva dva desetljeća postojanja, računalni su sustavi bili strogo centralizirani i obično su se nalazili u velikoj, posebno zaštićenoj i čuvanoj prostoriji. Ideja da će u idućih dvadeset godina računala postati manja od poštanskih marki te da će se masovno proizvoditi bila je tada u domeni znanstvene fantastike.

Spajanje računala i komunikacija imalo je duboki utjecaj na organizaciju računalnih sustava. Stari model jednog računala koje je pružalo svoje računarske usluge cijeloj organizaciji zamijenjeno je velikim brojem međusobno povezanih računala. Takve sustave zovemo distribuiranima, a povezuju ih računalne mreže.

Razvojem i širenjem računalnih mreža te pojeftinjenjem opreme i njenim širenjem u sve pore društva, počeli su i sigurnosni problemi. Domena koja je do tada bila rezervirana za uski krug znanstvenika, tehnologa, tehničara i privilegiranih korisnika, u kratkom vremenu se otvorila za široke mase koje su u nju donijele i svoje oblike ponašanja. Stoga je bilo potrebno i razviti mrežnu sigurnost. Sigurnost računalnih mreža je složena tema kojom se, opet tradicionalno, bavio uzak krug specijaliziranih stručnjaka. Međutim kako se sve više ljudi umrežuje, raste i broj ljudi koji moraju razumjeti osnove mrežne sigurnosti. Javila se potreba za dobro osmišljenom organizacijom sigurnosti u mrežama računala. U ovom dokumentu opisan je sigurnosni model računalne mreže prema institutu SANS, te ISO/OSI referentni model mreža računala na kojem on počiva i koji je osnova za shvaćanje rada i organizacije računalnih mreža.

2. Računalna mreža

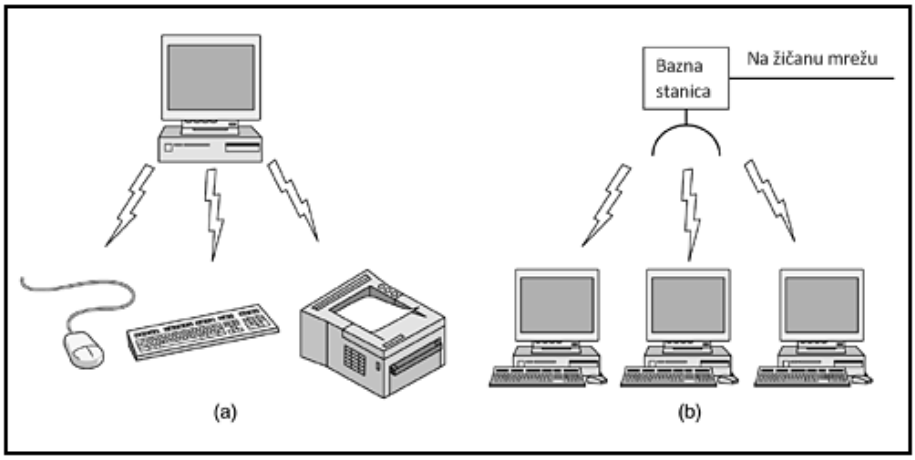
Mrežu računala čini skupina međusobno povezanih računala. Mreže se mogu razvrstati prema veličini, načinu povezanosti, funkcionalnoj vezi i arhitekturi.

Prema veličini mreže se dijele na:

- LAN (eng. Local Area Network) – mreža računala koja pokriva malo područje, kao što je dom, ured, mala skupina zgrada (škola, aerodrom, itd.). U principu, LAN ima jednog vlasnika.
- MAN (eng. Metropolitan Area Network) – mreža koja povezuje dvije ili više LAN mreža te je ograničena na područje grada ili sveučilišnih ustanova. MAN može imati jednog vlasnika, nekolicinu vlasnika koje veže međusobni dogovor ili nekolicinu vlasnika i jednog pružatelja usluga koji je vlasnik infrastrukture koja povezuje LANove.
- WAN (eng. Wide Area Network) – mreža koja pokriva veće geografsko područje, npr. bilo koja mreža čije se komunikacijske veze protežu do regionalnih ili državnih granica. Tipično, WAN ima jednog ili nekoliko pružatelja komunikacijskih usluga. U posebnim slučajevima WAN može imati samo jednog vlasnika, no to mogu samo financijski vrlo moćne organizacije.
- Intranet – skupina mreža računala koja za komunikaciju koriste TCP/IP (eng. Transmission Control Protocol/Internet Protocol) protokole i alate za rukovanje mrežom. Mreže se nalaze pod jednim administrativnim entitetom.
- Internet – mreža računala koja za komunikaciju koriste TCP/IP protokole, a koja povezuje različite mreže u svijetu, odnosno čine ju diljem svijeta međusobno povezane vladine, akademske, javne i privatne mreže raznih vlasnika. Iako u svijetu postoje i druge privatne i javne mreže, zasnovane na TCP/IP ili nekim drugim protokolima, koje su ili bi mogle biti međusobno potpuno odvojene, danas se za javnu razmjenu informacija koristi mreža koju nazivamo „Internet“. Zato se njeno ime i piše velikim početnim slovom.

Prema načinu povezanosti mreže se mogu razvrstati prema sklopovlju kojim su računala povezana te prema programskim paketima koji se pritom koriste. Na primjer, računala mogu biti povezana:

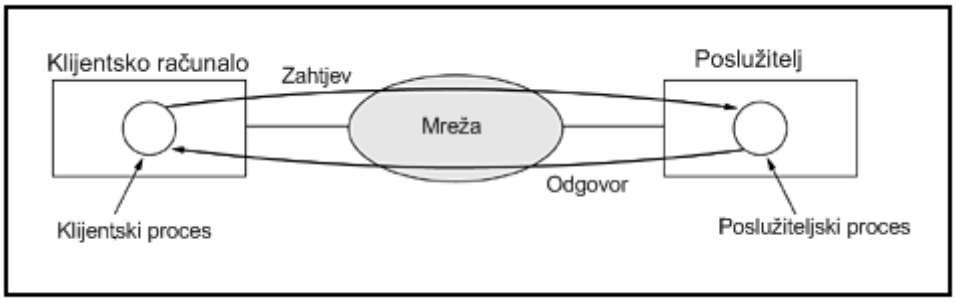
- optičkom mrežom,
- *Ethernet*-om (IEEE 802.3) – definira brojne standarde za fizičko umrežavanje računala, kao i standarde za signalizaciju za fizički sloj ISO/OSI referentnog modela mreže računala ili
- bežičnim LAN-om (eng. Wireless Local Area Network) – tehnologija za bežično umrežavanje računala na ograničenom području. Omogućuje korisnicima i mobilnost.



Slika 1. WLAN a) komponente komuniciraju pomoću Bluetooth tehnologije b)računala komuniciraju preko Wireless LAN tehnologije

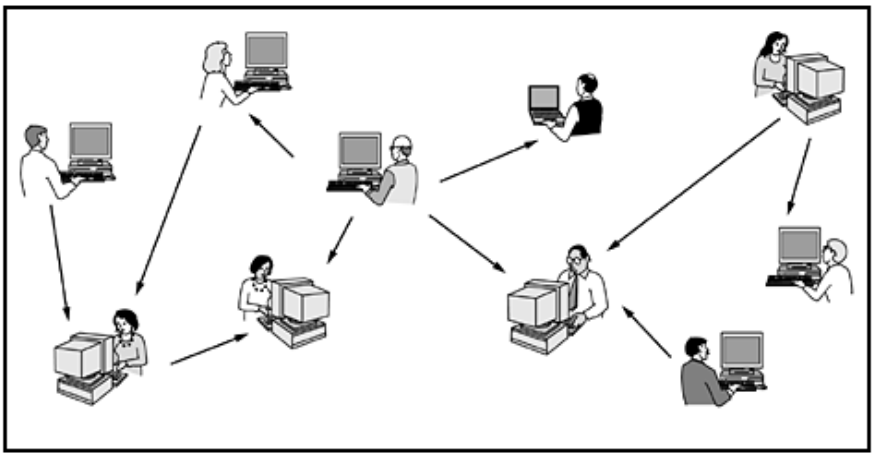
Ukoliko se računala klasificiraju prema funkcionalnoj vezi, tada se misli na mreže kao što su:

- Klijent-poslužitelj



Slika 2. Klijent-poslužitelj arhitektura

- P2P (eng. Peer-to-peer) – koristi raznoliku povezanost između sudionika mreže i kumulativnu brzinu mreže sudionika. Mreža nije centralizirana i ne koristi mali broj poslužitelja, već su sudionici mreže međusobno povezani *ad hoc* u čvorove. Obično se koristi za dijeljenje datoteka.

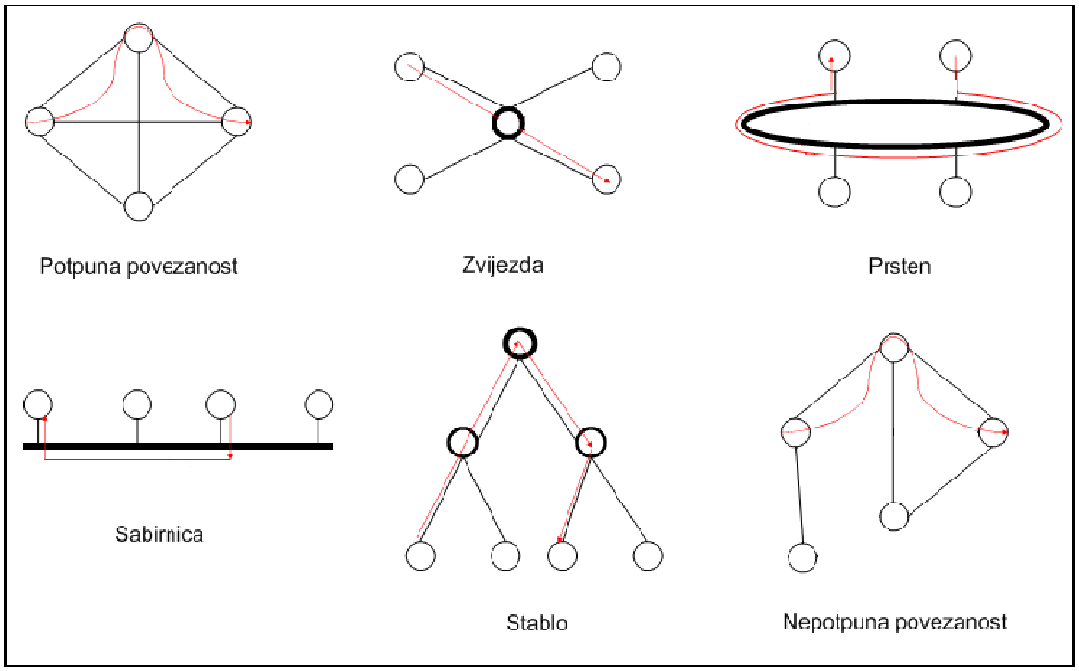


Slika 3. P2P mreža

Kada se računalne mreže klasificiraju prema arhitekturi obično se podrazumijeva neka određena topologija mreža računala pri čemu topologija definira način na koji su računala povezana u odnosu na njihove međusobne logičke veze. Topologija mreže je neovisna o fizičkim vezama u mreži. Čak i ako su umrežena računala povezana nekom sabirnicom („posložena u ravnu liniju"), topologija mreže može izgledati i sasvim drugačije. Podjela računalnih mreža prema topologiji:

- Potpuna povezanost – izravna veza svaka dva čvora u mreži. Primjena: umjereni broj čvorova i/ili ograničeno područje zbog troškova povezivanja (manje mreže).
- Zvijezda – središnji čvor na koji su spojeni svi ostali čvorovi posreduje pri komunikaciji između njih. Primjena: ograničeno područje (lokalna mreža, priključak korisnika na mrežu).
- Prsten – zajednički prijenosni medij stvara zatvoreni put koji povezuje sve čvorove. Primjena: lokalna mreža, mreža velikog kapaciteta (optičke mreže).
- Sabirnica – slično prstenu, na zajednički prijenosni medij priključeni su svi čvorovi. Primjena: lokalna mreža.
- Stablo – hijerarhijska struktura, komunikacija nadređenog i podređenog čvora je izravna, a svaka druga zahtijeva posredovanje jednog ili više čvorova. Primjena: međunarodna -nacionalna - regionalna povezanost.

- Nepotpuna povezanost – neki čvorovi imaju više veza od ostalih, odnosno kod nekih čvorova ne postoji izravna veza svaka dva čvora. Primjena: umjereni broj čvorova i/ili ograničeno područje (manje mreže).



Slika 4. Topologije

2.1. ISO/OSI referentni model

ISO/OSI (eng. International Standards Organization (ISO)/Open Systems Interconnect (OSI))referentni model definira sedam komunikacijskih slojeva i sučelja među njima. Razvijen je kao korak prema standardizaciji protokola koji se koriste u različitim slojevima. Svrha modela je omogućiti modularnost oprema (sklopovlja i programskih paketa) u komunikacijskom lancu i interoperabilnost opreme različitih proizvođača. Razlog uslojavanja računalnih mreža je njihova složenost u primjeni i upotrebi. ISO/OSI model definira funkcionalnosti svakog od sedam slojeva. Slijedeća slika pokazuje sedam slojeva i njihovu hijerarhiju.

Slika 5. ISO/OSI referentni model

Svaki sloj ovisi o uslugama koje pruža sloj ispod, sve do najnižeg fizičkog sloja, odnosno mrežne kartice i medija (žica, radio valova i sl.) koje povezuju računala. Ideja je da svaki sloj komunicira isključivo sa

slojem neposredno ispod i iznad sebe i da nikada ne „preskače“ slojeve. Time se osigurava modularnost, tj. svaka se komponenta u „stogu“ (eng. stack) može zamijeniti nekom drugom komponentom, nekog drugog proizvođača koja ima istu funkcionalnost i radi na istom sloju ISO/OSI modela. Također, svaki sloj razmjenjuje informacije isključivo sa slojem na istoj razini kod sugovornika. Oni to rade koristeći odgovarajući protokol. Sva funkcionalnost koja se javlja u komunikaciji grupira se u slojeve koji se potom nezavisno razvijaju. Komunikacija između slojeva, vertikalna i horizontalna, točno je propisana. Model se može usporediti s telefonskim sustavom. Ljudi već desetljećima koriste telefon za komunikaciju na daljinu. Da bi ta komunikacija bila moguća, svatko tko želi telefonirati treba imati uređaj, odnosno telefon. (U ISO/OSI modelu to bi bio aplikacijski sloj). Telefoni su naravno beskorisni ako nemaju mogućnost pretvaranja zvuka u električne impulse koji se mogu prenijeti putem žice (ovakve funkcije omogućavaju slojevi ispod aplikacijskog sloja). Na koncu svega dolazi se do fizičkih veza te činjenice da telefon mora biti uključen u utičnicu koja ga povezuje u telefonski sustav.

Neka Ivan i Luka žele komunicirati putem telefona. Ivan nazove Luku, Ivan podigne slušalicu i bira Lukin broj. Birani broj određuje kojem se središnjem uredu šalje Ivanov zahtjev i tada koji telefon iz tog središnjeg ureda treba nazvati. Jednom kad se Luka javi na telefon počinje razgovor, a time i sjednica. Konceptualno računalne mreže funkcioniraju na isti način. Ivan i Luka će razgovarati na jednak način bez obzira prenose li se njihovi glasovi bakrenom žicom, svjetlovodom ili radio vezom. S druge strane, bakrenom žicom će ići električni signali istih električnih karakteristika bez obzira govore li Ivan i Luka hrvatskim, engleskim ili nekim drugim jezikom. Štoviše, mogli bismo reći da je na vrhu ovakve komunikacije, u aplikacijskom sloju, zapravo svrha zbog koje njih dva razgovaraju. Pa će modul za komunikaciju i odgovarajući protokol biti bitno drukčiji ako oni razgovaraju privatno, kao prijatelji, nego ako jedan naručuje, a drugi kupuje ili jedan daje intervju, a drugi postavlja pitanja. Ovisno o svrsi razgovora, sasvim su drugačije poruke (protokol) koje oni razmjenjuju.Nije potrebno zapamtiti sve slojeve ISO/OSI referentnog modela, ali je korisno znati da postoje i da svaki sloj ne može funkcionirati bez sloja ispod.
Principi prema kojima su definirani slojevi:

1. Sloj se treba stvoriti kada je potrebna nova razina apstrakcije.
2. Svaki sloj treba obavljati dobro definirane funkcije.
3. Funkcija svakog sloja treba se odabrati tako da je moguće definirati internacionalne standardizirane protokole.
4. Granice između slojeva trebaju biti određene tako da se smanji tok informacija križanjem sučelja.
5. Broj slojeva treba biti dovoljno velik, tako da se ne javlja potreba za stavljanjem različitih funkcionalnosti u isti sloj.

2.1.1. Fizički sloj

Fizički se sloj brine o prijenosu bitova preko komunikacijskog kanala. Osigurava da kada jedna strana pošalje bit 1, druga strana i dobije taj bit kao 1, a ne kao 0. Uobičajena pitanja su koliko volta je potrebno za definiranje simbola „1“, a koliko za simbol „0“, koliko nanosekundi signal treba trajati za siguran prijenos jednog simbola, može li prijenos biti istovremen u oba smjera, kako se uspostavlja početna veza i kako se prekida, kako izgleda i koliko kontakata treba imati mrežni konektor i za što se koristi koji kontakt. Dizajnerski su problemi uglavnom vezani uz mehanička, električna i vremenska sučelja te uz medij za fizički prijenos informacija.

2.1.2. Podatkovni sloj

Glavna je zadaća podatkovnog sloja prijenos podataka između dva susjedna čvora i predaja mrežnom sloju. Prijenos se obavlja tako da pošiljatelj rastavi ulazne podatke u podatkovne okvire (eng. frame) (obično veličine par stotina, do par tisuća byte-ova) i prenese okvire slijedno, jedan za drugim. Ako se od ovog sloja traži tzv. pouzdani prijenos, primatelj potvrđuje da je dobio ispravne podatke u svakom okviru slanjem potvrdnog okvira pošiljatelju.

Drugi problem kojim se bavi podatkovni sloj je tok podataka i njegova regulacija. Moguća je pojava brzog pošiljatelja i sporog primatelja. U tom slučaju primatelj će biti zagušen podacima te je potrebno regulirati promet postavljanjem međuspremnika.

2.1.3. Mrežni sloj

Mrežni sloj određuje kako se paketi usmjeruju (kojim će putem ići) od izvora do odredišta. Usmjeravanje se može obavljati prema statičkim tablicama koje su ugrađene u mrežnu opremu i rijetko se mijenjaju. Također, tablice se mogu odrediti na početku svakog razgovora, kao što se to događa kod prijave na udaljeno računalo. Tablice usmjeravanja mogu biti vrlo dinamične te se mogu postavljati pri slanju svakog novog paketa.

Ako je previše paketa istovremeno prisutno u nekom mrežnom uređaju ili namijenjeno za neki prijenosni put može nastati usko grlo. Mrežni sloj kontrolira takva zagušenja, kao i kvalitetu usluge.

Kada paket putuje iz jedne mreže do druge da bi došao do svog odredišta može naići na mnogo problema. Adresiranje u jednoj mreži može biti drugačije od onog u drugoj mreži. Druga mreža ne mora primati pakete, protokoli mogu biti različiti itd. Ovakve probleme rješava mrežni sloj te omogućuje povezivanje različitih mreža.

2.1.4. Transportni sloj

Osnovna funkcija transportnog sloja je prihvaćanje podataka od gornjih slojeva, njihova podjela u manje jedince ako je potrebno, prosljeđivanje mrežnom sloju i osiguravanje da svi dijelovi stignu ispravno na drugi kraj. Sve nabrojano mora biti obavljeno učinkovito na način da se izoliraju gornji slojevi od promjena u tehnologiji sklopovlja.

U transportnom se sloju određuje koji će se tip usluge pružati sjedničkom sloju, a time i korisnicima mreže. Najpopularniji tip prijenosne veze je *error-free point-to-point* kanal (frekvencija pogrešaka je dovoljno mala tako da se može smatrati kao da ih uopće nema) koji dostavlja poruke ili byte-ove u poretku kojim su poslani. Međutim postoje i drugi kanali kojima se prenose poruke i koji ne jamče poredak dostave te slanje poruka višestrukim odredištima. Tip usluge se određuje kad se uspostavi veza. Transportni sloj određuje prijenos podataka s kraja na kraj, cijelim putem od izvora do odredišta. U prethodnim se slojevima komunikacija obavlja između svakog računala i njihovih najbližih susjeda, a ne između krajnjeg izvora i krajnjeg odredišta kao što je to u transportnom sloju.

U tom smislu može se reći da su slojevi 1do 3 lančani, a 4 do 7 s kraja na kraj (eng. end-to-end).

2.1.5. Sjednički sloj

Sjednički sloj omogućuje korisnicima na različitim računalima uspostavljanje sjednice. Sjednice nude različite usluge, uključujući i kontrolu razgovora (praćenje čiji je red na prijenos podataka), upravljanje značkama (sprečavanje da dvije strane pokušaju izvesti istu kritičnu operaciju u isto vrijeme) i sinkronizacija (provjeravanje po točkama dugih prijenosa omogućujući njihov nastavak u slučaju prekida sjednice).

2.1.6. Prezentacijski sloj

Za razliku od nižih slojeva, koji se uglavnom bave prijenosom bitova, prezentacijski se sloj brine o sintaksi i semantici informacija koje se prenose. Kako bi bilo moguće da računala s različitim predstavljanjem podataka komuniciraju, podatkovne strukture koje se trebaju razmijeniti mogu se definirati na apstraktni način uz upotrebu standardnih metoda kodiranja. Prezentacijski sloj upravlja apstraktnim strukturama i omogućuje razmjenu podatkovnih struktura viših razina (npr. bankovni zapisi).

2.1.7. Aplikacijski sloj

Aplikacijski sloj sadrži različite protokole koje korisnici svakodnevno koriste. Jedan od takvih protokola je HTTP (eng. HyperText Transfer Protocol), koji je temelj Interneta (World Wide Web). Kada web preglednik otvara web stranicu, tada šalje naziv stranice koju želi dohvatiti s poslužitelja putem protokola HTTP. Uz HTTP, koriste se i drugi aplikacijski protokoli za prijenos datoteka, elektroničke pošte, pregled diskusijskih grupa i dr.

2.2. Sigurnosni rizici računalne mreže

Važno je razumjeti da kod pitanja sigurnosti, korisnik ne može jednostavno reći „koji je najbolji vatrozid?“. Sigurnost ne čini samo jedna stvar, već čitavo mnoštvo elemenata. Postoje dva ekstrema – potpuna sigurnost i potpuni pristup. Jedino potpuno sigurno računalo je računalo isključeno iz računalne mreže, iz struje, zaključano u sefu i bačeno na dno oceana. Još bi pomoglo i da je neispravno. Na nesreću, računalo u takvom stanju nije uopće korisno. Računalo s potpunim pristupom je prikladno. Učinit će štogod mu zadate bez prigovora, autorizacije, zaporki i ostalih sigurnosnih mehanizama. No ni takvo računalo nije praktično, Internet je loš „kvart“ sada i vrlo brzo će zlonamjerni napadač zapovjediti računalu da učini nešto poput samouništenja, nakon čega ono nije ni od kakve koristi. Stoga svatko mora pronaći svoju „srednju vrijednost“, kompromis između ove dvije krajnosti.

U svakodnevnom životu ljudi donose odluke o rizicima koje su voljni prihvatiti. Na primjer, kod vožnje automobilom na posao postoji određeni rizik da će doći do sudara. Većina ljudi ima mentalnu sliku o tome što je prihvatljivi rizik i neće ga prijeći u većini situacija.

Svaka organizacija mora odlučiti između dvije krajnosti: potpune sigurnosti i potpunog pristupa. Što znači da je potrebno donijeti određena pravila, politiku, model sigurnosti koji definira sigurnosne mjere i rizike.

3. Koncept sigurnosti računalne mreže

Mrežna se sigurnost sastoji od postavljanja sigurnosnih mjera i politika. Njih donosi uprava organizacije na prijedlog nadležne službe u organizaciji. Može ih izraditi kompetentna služba ili osoba u organizaciji ili specijalizirani konzultant. Mjere zaštite provodi administrator mreže kako bi spriječio neovlašteni pristup računalnim resursima. Uz to, potrebni su stalni nadzor i mjerenje učinkovitosti sigurnosnog sustava. Mrežna sigurnost počinje prepoznavanjem (eng. identification) i provjerom (eng. authentication) korisnika, uobičajeno je to korisničkim imenom i zaporkom. Jednom kada je korisnik autenticiran, vatrozid (eng. firewall) postavlja pravila pristupa (eng. access control), kao na primjer kojim servisima mrežni korisnik može pristupiti. Vatrozid je sigurnosna komponenta koja sprečava neovlašteni pristup, ali ne provjerava potencijalno štetan sadržaj, kao što su računalni crvi i virusi. Sustav za sprečavanje provala u računalnu mrežu (eng. Intrusion Prevention System – IPS) pomaže u otkrivanju i sprečavanju takvih štetnih programa. IPS također prati sav mrežni promet i pokušava prepoznati sumnjivi prema sadržaju, volumenu i anomalijama u svrhu zaštite računalne mreže od napada kao što je napad uskraćivanja usluga (eng. Denial of Service). Kao dodatna mjera zaštite, komunikacija između dva računala domaćina preko mreže može biti kriptirana. Moguće je postaviti računala-mamce koja će napadači napasti misleći da su legitimna korisnička računala ili poslužitelji te analizirati sigurnost na temelju napada na njih.

Sve spomenute metode zaštite korisnici imaju na raspolaganju i mogu ih primijeniti. No sigurnost mreže računala nije standardizirana (nije definirano što se kada i kako mora primijeniti) i još je uvijek područje intenzivnog istraživanja.

3.1. Svojstva sigurnog računalnog okružja

Učinkovita sigurnosna strategija mora zadovoljiti pet osnovnih elemenata sigurnosti:

- Povjerljivost – podacima koji se prenose mogu pristupiti samo ovlaštene osobe,
- Autentikacija – proces provjere identiteta izvora i odredišta,
- Neporecivost – dokaz prijenosa i primitka podataka i
- Kontrola pristupa – dozvola ili zabrana pristupa temeljena na parametrima koji uključuju identitet izvora i odredišta

3.2. Zašto je potreban sigurnosni model

Dobro osmišljen sigurnosni model računalne mreže omogućuje sigurnosnoj zajednici (profesionalcima koji se bave uspostavom sigurnosti informacijskih sustava) metode istraživanja, primjene i održavanja mrežne sigurnosti koja se može primijeniti na bilo koju mrežu. Kod istraživanja može se koristiti kao alat za analizu mrežne sigurnosti podjelom po slojevima. Prilikom postavljanja mrežne sigurnosti, model se može iskoristiti za stvaranje mrežne arhitekture koja će osigurati da nisu propušteni važni detalji sigurnosnih mjera. U smislu održavanja postojećih mreža može se koristiti za razvoj rasporeda pregleda

sigurnosnih mjera. Također može se upotrijebiti za otkrivanje neovlaštenih provala te za smanjivanje mogućnosti da se oni ponovno pojave.

4. Sigurnosni model prema institutu SANS

Predloženi mrežni sigurnosni model ima sedam slojeva kojima je zadatak postavljanja sigurnosnih mjera podijeljen u sedam upravljivih cjelina. Model je općenit i može se primijeniti na sve sigurnosne sustave i uređaje. Razvoj spomenutog sigurnosnog modela važan je jer je potrebno osigurati sklad u osiguravanju računalnih mreža. Kada napadač uspješno zlouporabi računalnu mrežu, lakše je pronaći i popraviti problem upotrebom sigurnosnog modela.

Kod analize napada obično se pregledava mreža računala po ISO/OSI slojevima odozdo prema gore. Na isti je način osmišljen i sigurnosni model mreže računala. Posljedice napada analiziraju se od nižih prema višim slojevima. Kada se ustanovi koji je sloj zatajio, poznato je da su i svi slojevi ispod njega zatajili te će stručnjak brzo moći utvrditi koja su sve računala zahvaćena napadom i osigurati ih od ponovnih napada.

1) Sloj IT odjela
2) Administrativni sloj
3) Korisnički sloj
4) Programski sloj
5) ACL sloj
6) VLAN sloj
7) Fizički sloj

Slika 6. Sigurnosni model mreže računala

4.1. Fizički sloj

U fizičkom se sloju definira fizička sigurnost koja se primjenjuje za sprečavanje neovlaštenog pristupa napadača resursima pohranjenim na poslužiteljima, osobnim računalima ili nekim drugim medijima. Fizički je sloj prvi sloj jer je to najslabija točka bilo koje mreže. U bilo kojem scenariju napada, ako je fizički sloj napadnut, nikakav vatrozid neće pomoći u sprečavanju napada. Ukoliko zataji fizički sloj, napadač može neovlašteno pristupiti podacima. Na primjer, nije potrebno nikakvo znanje o računalnoj sigurnosti i vrlo malo vremena i novca za uspješan napad, ako napadač može pristupiti ciljanom računalu i iz njega izvaditi hard disk te ga nesmetano odnijeti. Osim fizičke, nikakva druga zaštita tu neće pomoći.

Fizička sigurnost uključuje projektiranje sigurnosti ustanove, postavljanje uređaja za kontrolu pristupa, alarma i kamera.

Fizički je sloj najlakše osigurati jer ne zahtjeva napredne tehničke koncepte. Moguće je unajmiti tvrtku koja će postaviti alarmni sustav te zaposliti zaštitara.

4.1.1. Elementi fizičkog sloja

Prvi element fizičkog sloja je projektiranje sigurnosti ustanove što uključuje organizaciju postavljanja uređaja u okolini ustanove, s vanjske strane zgrada. To na primjer mogu biti ograde, bodljikave žice, znakovi upozorenja, metalne i betonske barijere, reflektori. Ovakav oblik sigurnosti nije uvijek praktičan i treba se primijeniti samo ako ustanova rukuje vrlo osjetljivim podacima.

Drugi element fizičke sigurnosti sastoji se od uređaja za kontrolu pristupa. To mogu biti na primjer vrata i brave koje su ili mehaničke ili elektroničke. Postavljanje brava može se činiti kao zastarjela

metoda osiguravanja prostora, ali to je sigurnosna komponenta koja zahtjeva najmanje novčanog troška. Sigurnosne se brave trebaju postaviti svugdje gdje se nalaze poslužitelji i računala s podacima koji se žele zaštititi.

Treći oblik fizičke sigurnosti je alarm. Alarmni je sustav jedna od najvažnijih komponenti fizičkog sloja jer će se oglasiti ukoliko je netko provalio u štićeni prostor organizacije te će odrediti gdje je u ustanovi došlo do provale. Također, obavijestit će policiju i administratora mrežne sigurnosti da je netko neovlašteno pristupio podacima.

Posljednji oblik fizičke sigurnosti je kamera. Kamere su najbolji način da se utvrdi kako, gdje i kada je počinitelj provalio u organizaciju i neovlašteno pristupio podacima. To je korisno u analizi napada jer se mogu spriječiti budući slični napadi uklanjanjem slabih točaka sigurnosti. Također, moguće je identificirati počinitelje sa snimke. Prostorija u kojoj bi uvijek trebale biti kamere je prostorija s poslužiteljima.

Unajmljivanje zaštitara je jedini oblik fizičke sigurnosti koji se može smatrati kontrolom pristupa i mjerom nadzora. Zaštitari mogu prijaviti sumnjivu aktivnost u blizini ustanove, dozvoliti pristup zaposlenicima i najavljenim posjetiteljima. Iako je postavljanje zaštitara jedna od najboljih sigurnosnih mjera fizičkog sloja, obično je vrlo skupa i ne isplati se manjim organizacijama.

4.2. VLAN sloj

VLAN (eng. Virtual Local Area Network) sloj bavi se stvaranjem i održavanjem vitrualnih lokalnih mreža. Osnovni razlog primjene VLAN mreža je grupiranje zajedničkih računala iz sigurnosnih razloga. Na primjer, stavljanje odjela računovodstva na jednu VLAN mrežu, a odjela marketinga na drugu VLAN mrežu je pametna odluka zbog toga što odjeli ne dijele iste podatke. Mreža računala se razbija na manje sigurna i više sigurna područja.

4.2.1. Primjena

Prvi korak u primjeni VLAN mreže je određivanje javnih i privatnih mreža. Bilo koji uređaj kojim se pristupa izvan Intraneta treba biti u javnoj VLAN mreži. Na primjer web poslužitelji, vanjski FTP i DNS poslužitelji. Idući je korak postavljanje uređaja u privatni VLAN koji se može podijeliti na unutarnji korisnički VLAN i unutarnji poslužiteljski VLAN. Posljednji korak u primjeni je podjela unutarnjih korisničkih i poslužiteljskih VLAN mreža po odjelima i grupiranje podataka respektivno.

4.2.2. Zašto je VLAN sloj važan?

VLAN je ključan sloj za sigurnosni model računalne mreže jer mreža koja nije podijeljena sadrži neorganizirane skupine poslužitelja i uređaja. VLAN mreže se koriste za implementaciju liste kontrole pristupa (eng. Access Control List – ACL) koje se koriste kako bi se zaštitili podaci od korisnika koji im ne bi smjeli pristupiti. Iako se VLAN i ACL mogu postaviti nezavisno jedan od drugoga, važno je primijetiti da zajedno pojačavaju sigurnost mreže. Obično se dodaje lista kontrole pristupa VLAN mreži u svrhu ograničavanja ili dozvoljavanja pristupa određenom dijelu mreže. Glavni razlog zašto su VLAN sloj i ACL sloj odvojeni je zato što bi se promjene u VLAN sloju trebale obaviti bez mijenjanja ACL sloja i obratno.

VLAN mreže su izvrstan način za pronalaženje ugroženog računala. Ugroženo računalo je ono računalo koje je napadnuto ili sadrži sigurnosne ranjivosti. Pregledom povećanog prometa koji dolazi s određene VLAN mreže, administrator mrežne sigurnosti može smanjiti opseg te VLAN mreže kako bi pronašao s kojih vrata (eng. port) dolazi infekcija te koje je računalo u mreži napadnuto.

4.3. ACL sloj

ACL (eng. Access Control List) sloj definira stvaranje i održavanje popisa koji definiraju kontrolu pristupa. Takve liste se postavljaju na usmjerivače (eng. router) i vatrozidove. Stvaraju se kako bi se dozvolio ili zabranio pristup među računalima na različitim mrežama. Ta ih zadaća čini neophodnima u području mrežne sigurnosti. Dobrom definicijom popisa kontrole pristupa, administrator mrežne sigurnosti može spriječiti mnoge napade prije nego što ih napadač i pokuša izvesti. Postavljanje listi pristupa čovjeku se može činiti kao dosadan i naporan posao. Kod složenih organizacija to je i vrlo složen posao i vrlo je lako napraviti greške u brojnim popisima na brojnim uređajima, naročito kad se rade izmjene u sustavu.

Mnogo je toga što treba uzeti u obzir prilikom postavljanja listi kontrole pristupa, kao što su povratni promet ili svakodnevni promet koji je ključan za rad mreže. Ako se liste ne naprave kako treba, ACL može dozvoliti neovlašteni promet i/ili zabraniti ovlašteni promet.

4.3.1. Primjena

Kod stvaranja „dobrih" listi kontrole pristupa treba jednako razmatrati dolazni promet kao i odlazni promet. Male si tvrtke mogu dozvoliti stvaranje kratkih listi kontrole pristupa dozvoljavajući dolazni promet na vratima 80 i 443 za HTTP i HTTPS (eng. Hypertext Transfer Protocol over Secure Socket Layer) poslužitelje. Osim toga morat će omogućiti osnovnu web aktivnost za odlazni promet na vratima 80, 443 i 53 za HTTP, HTTPS i DNS (eng. Domain Name Server) poslužitelje respektivno. Mnoge srednje i velike tvrtke trebaju imati servise kao što je VPN, otvorene za tvrtke koje su partneri ili kupci te za udaljene korisnike.

Većina se administratora koncentrira na stvaranje listi kontrole pristupa koje zabranjuju pristup mreži tvrtke s Interneta. Kod stvaranja listi kontrole pristupa potrebno je usredotočiti se na takve tipove listi koje su primjenjive jednako za odlazni i dolazni promet. Administrator mora znati kojim vratima treba omogućiti pristup izvan Intraneta, kao i u Intranet. To uključuje izvorišna i odredišna vrata. Na primjer, potrebno je znati da su vrata veća od 1023 jedina izvorišna vrata koja ulaze u DMZ (eng. Demilitarized Zone) s Interneta s odgovarajućim odredišnim vratima koja su ekvivalentna servisima koji su dozvoljeni DMZ područjem. Isto vrijedi i za vrata koja izlaze iz DMZ područja. DMZ područje je dio mrežnog prostora u kojem je dozvoljen pristup vanjskim uslugama i većoj nepovjerljivoj mreži, kao što je Internet.

4.3.2. Zašto je ACL sloj važan za sigurnost?

Liste kontrole pristupa važan su dio sigurnosnog modela mreža računala jer imaju mogućnost zabrane ili dozvole prometa za usluge koje su vidljive, odnosno nisu vidljive izvan Intraneta. Liste kontrole pristupa također štite programski sloj blokiranjem pristupa ranjivim servisima. Kada se dogodi napad, liste kontrole pristupa mogu se iskoristiti za određivanje kompromitiranog računala i umanjivanje štete učinjene tom računalu.

4.4. Programski sloj

Programski je sloj usredotočen na programske pakete i njihovo ažuriranje, primjenu zakrpa i ispravljenih inačica u svrhu smanjivanja njihove ranjivosti. Administratori mrežne sigurnosti moraju biti upoznati s programima koji se nalaze na računalima u mreži i održavati ih u smislu primjene novih i ispravljenih inačica. Također trebaju znati točno što koja zakrpa čini kada se instalira te znati ukloniti neželjene programe.

4.4.1. Primjena

Primjena programske sigurnosti uključuje primjenu ažurnih nadogradnji i zakrpa za instalirane programe. Tako se smanjuje broj ranjivosti koje napadači mogu iskoristiti za ugrožavanje računala na mreži. Vrlo je važno održavati programe na poslužiteljima koji koriste HTTP i HTTPS jer se koriste za pristup Internetu. Također i korisnički se programi trebaju prikladno ažurirati kako bi se računala zaštitila od napada s klijentske strane. Na primjer, ako je na poslužitelju pokrenuta aplikacija za pružanje web usluga, administrator mora održavati aplikaciju ažurnom kako bi osigurao da su otklonjene novootkrivene ranjivosti te da je smanjena mogućnost napada na poslužitelj.

Poznavanje usluga koje moraju biti pokrenute na poslužitelju je bitan dio programskog sloja. Ako administrator zna koje su usluge pokrenute i praćenjem prometa ustanovi da postoje anomalije u prometu, znat će da nešto nije u redu te da je sustav možda ugrožen.

4.4.2. Zašto je programski sloj važan?

Programski je sloj važan za sigurnosni model zbog toga što ukoliko je taj sloj kompromitiran, napadač uspješnim napadom može neovlašteno pristupiti i mijenjati podatke na mreži računala. Ovo je prvi sloj u kojem napadač može preuzeti korisnički račun na mreži. Programski sloj pomaže u zaštiti korisničkog sloja. Ako je računalo u mreži postavljeno i ažurirano ispravno, napad na

korisnički sloj više neće biti učinkovit. Pravilno konfigurirani programski paketi bi trebali onemogućiti napad na korisnički sloj.

4.5. Korisnički sloj

Korisnički se sloj odnosi na uvježbavanje i prijenos znanja korisnicima o sigurnosti u računalnoj mreži. Korisnik mora razumjeti osnovne koncepte mrežne sigurnosti. Također trebaju naučiti koje aplikacije ne smiju pokretati ili instalirati na svojim sustavima. Osim toga, korisnici trebaju imati pojam o tome kako se ponaša njihovo računalo kada radi normalno i kako se ponaša kada to nije slučaj.

4.5.1. Primjena

Osnovni način primjene korisničke sigurnosti je obrazovanje korisnika o aplikacijama koje trebaju izbjegavati, kako se njihovo računalo ponaša kada radi normalno i kada to nije slučaj. Na primjer, korisnike treba upozoriti na opasnosti korištenja P2P aplikacija gdje datoteke koju preuzimaju mogu sadržavati virus, trojanski konj ili neki drugi štetan program. Ukoliko su korisnici upoznati s opasnostima štetnih aplikacija, to može pomoći pri umanjivanju mogućnosti ugrožavanja sigurnosti računala.

Važno je naučiti korisnike kako funkcionira njihov sustav jer ako to znaju, moći će i sami otkriti problem. Na primjer, ako se sustav na kojem rade odjednom znatno uspori, obrazovani korisnik može posumnjati da mu je računalo ugroženo i prijaviti administratoru problem.

4.5.2. Važnost korisničkog sloja

Ako je korisnički sloj ugrožen, ujedno je ugrožen i korisnički račun. Ukoliko napadač uspješnom zlouporabom ranjivosti preuzme korisnički račun, može prouzročiti veliku štetu na sustavu. Krađom domenskog korisničkog računa, napadač može, ovisno o ovlastima računa, mijenjati, kopirati ili brisati podatke pohranjene ne samo na jednom računalu već i na cijelom sustavu. Korisnički se sloj nalazi iznad administrativnog zbog toga što ako je ugrožen administrativni sloj, ugrožena je i sigurnost korisničkog sloja. Većina će napadača prvo napasti korisnički sloj jer obični korisnici imaju manje znanja o sustavu te će ih teže spriječiti.

4.6. Administrativni sloj

Administrativni sloj uključuje obrazovanje administratora sigurnosti mreže i svih korisnika koji upravljaju mrežom. Sličan je korisničkom sloju, ali su podaci kojima se rukuje na višoj sigurnosnoj razini. Kao i korisnike u korisničkom sloju, administratore mreže računala također treba obrazovati u smislu da znaju koje je aplikacije sigurno i bolje instalirati i pokretati, a koje ne. Također moraju potpuno razumjeti kako njihov sustav funkcionira u normalnim uvjetima. Uz to moraju znati otkriti probleme u korisničkom sloju te ih moći otkloniti.

4.6.1. Primjena

Primjena administrativnog sloja uključuje obrazovanje administratora mreže računala za opsežne vještine i znanja o mrežama računala te načinu rada sustava organizacije. Administratori moraju znati poučiti korisnike o sigurnosti računalne mreže te komunicirati s njima u smislu otklanjanja problema. Time se osigurava da će se problemi riješiti brzo i učinkovito.

4.6.2. Važnost administrativnog sloja

Ukoliko je ugrožena sigurnost administrativnog sloja, napadač može uspješnom zlouporabom ranjivosti preuzeti administrativni korisnički račun. To može imati pogubne posljedice za podatke u sustavu jer će ih napadač moći mijenjati, kopirati i brisati. Osim toga, moći će instalirati i pokretati programe po volji. Posebno je opasno što će moći stvoriti suptilne i teško vidljive ranjivosti i na nižim slojevima, koje kasnije može uspješno koristiti a da ne bude otkriven. Administrativni se sloj nalazi prije sloja odjela informatičkih tehnologija zbog toga što će napadači prije napasti administrativni sloj. Ako je sedmi sloj (sloj odjela za sigurnost informacijske tehnologije) kompromitiran ujedno je kompromitiran i administrativni sloj.

4.7. Sloj odjela za sigurnost informacijske tehnologije

U ovaj su sloj uključeni svi profesionalci iz područja mrežne sigurnosti, mrežni arhitekti i specijalisti za programsku podršku. To su svi oni ljudi koji omogućuju i održavaju rad računalne mreže. Svi članovi ovog sloja imaju administrativne korisničke račune za cijeli sustav, što znači da mogu pristupiti bilo kojem uređaju i servisu na mreži. Na primjer, korisnik s takvim ovlastima ima mogućnost čitanja, pisanja i promjene strukture baze podataka, a administrator i korisnici samo ovlasti čitanja, pisanja i promjene sadržaja baze podataka.

4.7.1. Primjena

Svaka osoba koja radi u odjelu sigurnosti informacijske tehnologije mora odlično poznavati mreže računala i metode njihove zaštite od zlonamjernih napadača i neželjenih posljedica. Osim toga, moraju znati popraviti štetu prouzročenu uspješnih napadom. Odjel sigurnosti informacijske tehnologije je odgovoran za implementaciju i održavanje svih slojeva sigurnosnog modela.

4.7.2. Važnost sedmog sloja

Ukoliko napadač izvede uspješan napad na sedmi sloj, imat će potpuni pristup svim uređajima u mreži. Dakle moći će upravljati usmjerivačima, vatrozidovima, posrednim računalima te VPN mrežom. Spomenuti napad je vrlo poguban jer napadač može potpuno paralizirati i onemogućiti mrežu. Posljedice znače financijske gubitke za tvrtku jer gube povjerenje klijenata. Primjer napada bi bilo kopiranje podataka o partnerima, korisnicima i suradnicima, neovlašteno brisanje relacija u bazi podataka, ili brisanje cijele baze podataka, što znači potpuno uništenje zapisa i informacija tvrtke.

5. Usporedba Sigurnosnog modela računalne mreže s ISO/OSI modelom

Svaki je sloj sigurnosnog modela računalne mreže izgrađen nad razinom ispod njega, slično ISO/OSI modelu. Ako je sigurnost jednog sloja ugrožena, ugrožena je i sigurnost slojeva ispod njega. Slijedeća slika prikazuje sigurnosni model računalne mreže paralelno s ISO/OSI referentnim modelom te daje njihovu usporedbu.

Sigurnosni model računalne mreže	ISO/OSI referentni model
Sloj IT odjela	Aplikacijski sloj
Administrativni sloj	Prezentacijski sloj
Korisnički sloj	Sjednički sloj
Programski sloj	Transportni sloj
ACL sloj	Mrežni sloj
VLAN sloj	Podatkovni sloj
Fizički sloj	Fizički sloj

Slika 7. Usporedba sigurnosnog modela računalne mreže i ISO/OSI modela

Prvi sloj je fizički sloj u oba modela. Oba modela opisuju fizički model s istog aspekta mreže. Fizički sloj sigurnosnog modela uključuje fizičku sigurnost (ograde, alarmi, kamere, zaštitari), a fizički sloj ISO/OSI modela rukuje fizičkim komponentama računalne mreže. Oba su sloja jasna sama po sebi i jednostavno je rukovati njihovim komponentama.

Drugi sloj sigurnosnog modela je VLAN sloj, dok je ISO/OSI modela podatkovni sloj. VLAN sloj sigurnosnog modela upravlja podjelom VLAN mreže te dijeli LAN mrežu preko preklopnika (eng. switch) i dijelova na temelju podatkovnog sloja ISO/OSI modela koji pokriva MAC adresiranje.

Treći sloj sigurnosnog modela je ACL sloj, a ISO/OSI modela je mrežni sloj. Oba sloja na sličan način rukuju IP adresama i LAN mrežom. ACL sloj rukuje primjenom listi kontrole pristupa koja se koristi za zabranu ili dozvolu pristupa i temelji se na mrežnom sloju ISO/OSI modela koji pokriva IP adresiranje.

Četvrti sloj je programski sloj, dok je u ISO/OSI modelu to transportni sloj. Oba sloja uključuju mrežni promet i međusobnu povezanost računala na mreži. Programski sloj je vezan uz primjenu zakrpa i nadogradnji programa koje pridonose većoj sigurnosti, a transportni sloj opisuje veze između računala krajnjih korisnika, odnosno programa na njihovim računalima.

Peti je sloj korisnički u sigurnosnom modelu, a u ISO/OSI je to sjednički sloj. Oba su sloja vezana uz krajnjeg korisnika. U korisničkom sloju osobe imaju mogućnost koristiti računalo, a sjednički se sloj bavi izravno mrežnim komunikacijama na tom računalu.

Šesti sloj je administrativni u sigurnosnom modelu, dok je u ISO/OSI modelu to prezentacijski sloj. Oba sloja obavljaju administrativne dužnosti. Administrativni sloj uključuje korisnike koji mogu osobama iz korisničkog sloja usmjeriti i obrazovati, a prezentacijski je sloj izravno vezan uz podatke.

Sedmi i posljednji sloj je sigurnosni IT odjel, a u ISO/OSI je to aplikacijski sloj. IT odjel održava i osmišljava sve ostale slojeve osiguravajući da cijela mreža radi ispravno prema sigurnosnom modelu, ali i prema ISO/OSI modelu. Aplikacijski je sloj ISO/OSI modela vezan uz prikaz podataka

6. Mogući napadi na sigurnosni model

6.1. Napad na fizički sloj

U ovom primjeru napadač provaljuje u organizaciju kroz zaključana vrata, obično po noći kada su svi zaposlenici napustili ustanovu. Neka osim zaključanih vrata nisu postavljene nikakve druge fizičke zaštitne mjere. Provalnik ima fizički pristup mreži i može iskoristiti računalo koje je povezano u mrežu. Može pretražiti lokalnu mrežu (LAN) za poslužiteljima te pristupiti podacima na njima. U ovom scenariju trebale su biti postavljene i druge fizičke sigurnosne mjere koje bi provalniku onemogućile napredovanje do računala povezanog na računalnu mrežu. U ovom slučaju sigurnost fizičkog sloja je ugrožena i potrebno je postaviti kamere, alarm i zaštitar.

6.2. Napad na VLAN sloj

Neka je napadač uspješno iskoristio ranjivost fizičkog sloja i dobio pristup računalu povezanom na lokalnu mrežu. Napadač traži računala s programima koja sadrže sigurnosni propust, kao što je MS03-026 - prepisivanje memorije u RPC (eng. Remote Procedure Call) funkcionalnosti koje napadač može iskoristiti za pokretanje proizvoljnog programskog koda. Kako napadač ima pristup računalu na lokalnoj mreži, pokušat će iskoristit ranjivost uređaja koji su povezani na njegovo računalo. Ukoliko napadne računala koja nisu na istoj podmreži kao i njegovo, postat će izložen otkrivanju. Ako poslužitelji nisu podijeljeni u različite homogene VLAN mreže, napadač može izravno pretraživati poslužitelje. Ispravno postavljanje VLAN mreže prisilit će napadača da pretražuje više mreža. Kada je sigurnost VLAN sloja ugrožena, poznato je da je narušena i sigurnost fizičkog sloja.

6.3. Napad na ACL sloj

Neka mrežni administrator postavi popis kontrole pristupa na računalu preko kojeg se pristupa Internetu i neka je to računalo web poslužitelj na kojem se nalazi baza podataka. Baza podataka sadrži podatke o ljudima koji su posjetili web stranicu na spomenutom računalu. Napadač pregledava koja su vrata (eng. port) na poslužitelju otvorena. Ako mrežni administrator nije dobro postavio popis kontrole pristupa, odnosno ako je ostavio otvorena vrata koja nije trebao, napadač može neovlašteno pristupiti bazi podataka na poslužitelju. Kako bi spriječio ovakav napad, administrator je trebao postaviti popis kontrole pristupa tako da se isključivo preko vrata 80 može pristupiti web poslužitelju.

6.4. Napad na programski sloj

Neka napadač pokušava neovlašteno pristupiti poslužitelju na kojem je pokrenut program Apache, web poslužitelj otvorenog koda namijenjen operacijskim sustavima Unix/Linux i Windows. Napadač iskorištava ranjivost kojom može pristupiti zaporkama. Ako administrator nije primijenio potrebnu zakrpu, napadač će uspješno zlouporabiti sigurnosni propust i preuzeti datoteku sa zaporkama. Upotrebom preuzetih zaporki može se prijaviti na web poslužitelj. Primjena zakrpa, nadogradnji i novih inačica mogla je spriječiti opisani napad. ACL sloj nije mogao spriječiti napad jer je napad izveo putem vrata 80 kojima je dozvoljen pristup na Internet.

6.5. Napad na korisnički i administrativni sloj

Obrazovanje korisnika i administratora je osnova korisničkog i administrativnog sloja pa je napad na te slojeve jednak. Neka napadač presretne poruku elektroničke pošte koju je poslao IT odjel. Napadač promijeni izvornu poruku i napiše u njoj kako je zagubljena zaporka određenog korisnika te da ju treba promijeniti u „blah“. Zbog neznanja korisnik vjeruje lažnoj poruci elektroničke pošte i promijeni svoju zaporku u „blah“. Napadač time dobiva pristup mreži s ovlastima korisnika kojeg je prevario. Primjena sigurnosnih mjera programskog sloja nije mogla spriječiti ovaj napad. Napadač je iskoristio lakovjernost i pogrešku korisnika kako bi ukrao korisnički račun.

6.6. Napad na sedmi sloj

Neka napadač pošalje poštom CD koji navodno sadrži bazu podataka, lažno se predstavljajući da je „klijent X“. Mrežni administrator ažurira bazu podataka podacima s CD-a. Međutim čim počne kopirati

podatke u pozadini se s CD-a pokrene *rootkit* program. *Rootkit* predstavlja skupinu programa kojima je moguće sakriti tekuće procese, datoteke ili sistemske podatke od operacijskog sustava. Spomenuti program nakon nekog vremena šalje administratorska korisnička imena i zaporke napadaču. U ovom scenariju napadač ukrade korisnički račun koji ima sve ovlasti i pristup cijelom sustavu i svim servisima. Napadač može pristupiti uređajima na mreži, poslužiteljima i uslugama kojima obični korisnik i administrator ne mogu.

7. Postavljanje sigurnosnog modela računalne mreže

Svi se slojevi trebaju primjenom istovremeno i svakom sloju treba posvetiti jednako mnogo pažnje prilikom postavljanja. Ideja je da bi se osnovna razina sigurnosti trebala postaviti za svaki sloj u sigurnosnom modelu računalne mreže. Prvo se postavlja osnovna, tj. temeljna razina sigurnosti, a zatim se ona nadograđuje tokom životnog ciklusa sigurnosnog modela računalne mreže. Elementi fizičkog sloja trebaju se postaviti tako da spriječe moguće napade. Na primjer, mogu se postaviti nove brave koje koriste RFID za identifikaciju. Tako je moguće pratiti i autenticirati osobe koje pristupaju ograničenom području. VLAN i ACL slojeve potrebno je postaviti tako da su prilagođeni potrebama organizacije koja primjenjuje sigurnosni model.

Prvi korak u primjeni sigurnosnog modela je započinjanje obrazovanja IT odjela, administrativnog odjela i svih korisnika. Zatim je potrebno provjeriti jesu li svi programski paketi ažurirani na nove inačice i jesu li primijenjene odgovarajuće zakrpe. Kod ACL sloja provjerava se jesu li liste kontrole pristupa dobro postavljene. Ako jesu, potrebno je utvrditi ima li sigurnosnih propusta u njima. Ako nisu postavljene, administrator treba stvoriti općenitu listu kontrole pristupa. Zatim se provjerava je li u upotrebi VLAN mreža, kako je konfigurirana te je li postavljena mreža korisna. Ukoliko u računalnoj mreži nema postavljenih VLAN mreža, administrator ih treba osmisliti, stvoriti i organizirati. Na kraju sigurnosni administrator treba provjeriti je li dobro postavljena fizička sigurnost.

Drugi korak u postavljanju sigurnosnog modela je početak rada na slojevima u smislu postavljanja specifičnih dijelova sigurnosti. To znači da IT odjel, administratori i korisnici već primjenjuju svoje znanje u svakodnevnom radu. Također IT odjel može odlučivati koje programe treba ukloniti te koje se ovlasti u smislu dozvole i zabrane pristupa trebaju dodijeliti korisnicima i administratorima. Moguće je spojiti VLAN i ACL slojeve u jedan mrežni sloj jer se postavljaju zavisno jedan od drugoga prilikom postavljanja sigurnosnog modela. Trebaju se stvoriti i organizirati posebno prilagođene VLAN mreže te liste kontrole pristupa za upravljanje tokom prometa na mreži. Nije potrebno postavljati mjere sigurnosti računalne mreže po redu, nego je potrebno osigurati da su svi slojevi koordinirano postavljeni. Kako bi se ostvario željeni rezultat, zaštita mrežnog sustava, svi slojevi moraju ispravno funkcionirati.

8. Životni ciklus sigurnosnog modela

Nakon što je postavljen sigurnosni model računalne mreže počinje životni ciklus (eng. Life Cycle) mrežne sigurnosti. Proces uključuje provjere kojima se osigurava da svi slojevi pružaju optimalnu zaštitu. Životni ciklus počinje pregledom svih slojeva s tehničkog stanovišta. To znači da u postavljenom modelu treba otkriti sve probleme i poboljšati komponente sigurnosti za koje se pokaže potreba. Kontinuirano treba pratiti objavljene ranjivosti u programima te ih treba odmah ukloniti primjenom odgovarajućih zakrpa i nadogradnji.

Nakon toga, postavljenu sigurnost treba provjeriti probnim napadima kako bi se utvrdilo koje su slabe točke sustava. Ako se ispitivanjem otkriju sigurnosni propusti, potrebno ih je odmah ukloniti prije kako se ne bi dogodio stvarni napad.

Konačno, administrator sigurnosti mora osmisliti kako prilagoditi postavljeni sigurnosni model u slučaju širenja organizacije. Ovakva će strategija osigurati da se svi slojevi stalno poboljšavaju te da pružaju optimalnu zaštitu. Životni ciklus nema posebno vremensko ograničenje već ovisi o organizaciji u kojoj se postavlja sigurnosni model računalne mreže. Manje organizacije će imati dulji i dinamičniji životni ciklus jer je u njoj lakše i financijski učinkovitije odjednom promijeniti velike dijelove sigurnosnog modela računalne mreže. Veća će tvrtka imati kraći, ali statičan životni ciklus jer je u njoj lakše mijenjati manje detalje. Tako promjene neće ometati normalan rad sustava. Međutim, to nije pravilo, možda će manja tvrtka htjeti koristiti životni ciklus kakav bi koristila velika tvrtka. Na primjer, ako mala tvrtka radi 24 sata na dan, tada će biti potrebno koristiti životni ciklus primjeren velikoj tvrtki kako bi bilo što manje prekida u normalnom radu.

9. Zaključak

Sigurnost je vrlo složeno područje koje se još uvijek mnogo istražuje. Sigurnosni model računalne mreže je samo jedan od mogućih modela koji postoje. Organizacija sigurnosti po slojevima je svakako dobar način osiguravanja optimalne zaštite mrežnog sustava. Postoje različite ideje o tome što je , kako bi trebala izgledati sigurnost mreže i koji su rizici prihvatljivi. Ključ izgradnje sigurne mreže je definiranje značenja sigurnosti za svaku organizaciju. Sigurnosni model mreže računala nije standardiziran, ali pruža dobar okvir za postavljanje sigurnosti u različitim organizacijama. Također, model ostavlja dovoljno slobode organizacijama da ga prilagode svojim potrebama.

Važno je da se sigurnosni sustavi izgrađuju na takav način da su “nevidljivi“ tj. da ne podsjećaju korisnika na njihovu stalnu prisutnost. Sigurnost se tiče svih ljudi u organizaciji i samo međusobnom suradnjom te inteligentnim postavljanjem sigurnosnih sustava moguće je pružiti optimalnu zaštitu računalnim resursima.

10. Reference

[1] Network Security Model, Joshua Backfield, SANS Institute 2008

[2] http://en.wikipedia.org/wiki/Network_security , siječanj 2009., Mrežna sigurnost

[3] http://en.wikipedia.org/wiki/Network_topology#Mesh, svibanj 2008., Topologija računalnih mreža

[4] Computer Networks, Andrew S. Tanenbaum, Prentice Hall 2003, Fourth Edition