Baze podataka u zatvorenim mrežnim sustavima

Delbianco, Ivan

Sveučilište Jurja Dobrile u Puli
Fakultet ekonomije i turizma
Dr. Mijo Mirković

IVAN DELBIANCO

BAZE PODATAKA U ZATVORENIM MREŽNIM SUSTAVIMA

Završni rad

Pula, rujan 2016. godine.

Sveučilište Jurja Dobrile u Puli
Fakultet ekonomije i turizma
Dr. Mijo Mirković

IVAN DELBIANCO

BAZE PODATAKA U ZATVORENIM MREŽNIM SUSTAVIMA

Završni rad

JMBAG: 468-E, izvanredni student
Studijski smjer: Poslovna Informatika

Predmet: Baze Podataka
Znanstveno područje: Društvena Znanost
Znanstveno polje: Ekonomija
Znanstvena grana: Poslovna Informatika

Mentor: prof. dr. sc. Vanja Bevanda

Pula, rujan 2016. godine

IZJAVA O AKADEMSKOJ ČESTITOSTI

Ja, dolje potpisani Ivan Delbianco, kandidat za prvostupnika poslovne informatike ovime izjavljujem da je ovaj Završni rad rezultat isključivo mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na objavljenu literaturu kao što to pokazuju korištene bilješke i bibliografija. Izjavljujem da niti jedan dio Završnog rada nije napisan na nedozvoljen način, odnosno da je prepisan iz kojega necitiranog rada, te da ikoji dio rada krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za koji drugi rad pri bilo kojoj drugoj visokoškolskoj, znanstvenoj ili radnoj ustanovi.

Student

_____

U Puli, 14.09.2016. godine

IZJAVA

o korištenju autorskog djela

Ja, Ivan Delbianco dajem odobrenje Sveučilištu Jurja Dobrile u Puli, kao nositelju prava iskorištavanja, da moj završni rad pod nazivom BAZE PODATAKA UNUTAR ZATVORENOG MREŽNOG SUSTAVA koristi na način da gore navedeno autorsko djelo, kao cjeloviti tekst trajno objavi u javnoj internetskoj bazi Sveučilišne knjižnice Sveučilišta Jurja Dobrile u Puli te kopira u javnu internetsku bazu završnih radova Nacionalne i sveučilišne knjižnice (stavljanje na raspolaganje javnosti), sve u skladu s Zakonom o autorskom pravu i drugim srodnim pravima i dobrom akademskom praksom, a radi promicanja otvorenoga, slobodnoga pristupa znanstvenim informacijama.
Za korištenje autorskog djela na gore navedeni način ne potražujem naknadu.

U Puli, 14.09.2016. godine

Potpis

_____

SADRŽAJ

Uvod

U poslovnom okruženju, neovisno o veličini poduzeća, najbitnija su dva faktora: sigurnost i baze podataka. Informacijski sustavi, odnosno baze podatka pruže pravovremene i konzistentne podatke koji daju konkurentsku prednost u tržišnom okruženju. Takav sustav zahtjeva visoke standarde kvalitete mreže i sigurnosti, kontrole pristupa, raspoloživosti korisnicima te oporavka u slučaju prekida rada baze, kvarova ili u najgorem slučaju napadaja na sustav.

U ovom radu objašnjeni su temeljni informatički sustavi koji se nalaze unutar poslovnog okruženja. U prvom poglavlju opisane su sastavnice radnog okruženja: baze podataka i mrežna arhitektura. Tu su obuhvaćene zatvorene i otvorene mreže, baze PostgreSQL, Oracle, te mrežna arhitektura.

U sljedećem poglavlju opisuju se načini spajanja na zatvorene informatičke sustave kao što su remote desktop connection i virtualizacija. Treće poglavlje bavi se arhitekturom mreže, serverima i sigurnošću. Fokus je na sigurnosti podataka unutar mreže, opasnostima koje se mreža izlaže i načinima zaštite sustava i samih baza.

Sigurnost i ponašanje Oracle i PostgreSQL baza unutar mrežnih sustava i njihova hijerarhija te stupnjevi sigurnosti obrađuje se u četvrtom i posljednjem poglavlju.

Cilj ovoga rada je proučiti i opisati zatvorene mrežne sustave, njihovu sigurnost i sigurnost baza podataka unutar takvih sustava.

1. OTVORENI I ZATVORENI MREŽNI SUSTAVI

1.1. Otvoreni mrežni sustavi

Otvoreni mrežni sustavi su često sinonim za sustave bez strukture i sa niskim stupnjem sigurnosti. Temeljni LAN odnosi bez kontroliranog okruženja spadaju u taj pojam. Najčešće se tu radi o jednostavnim mrežama u malim radnim mjestima ili privatnim domovima.

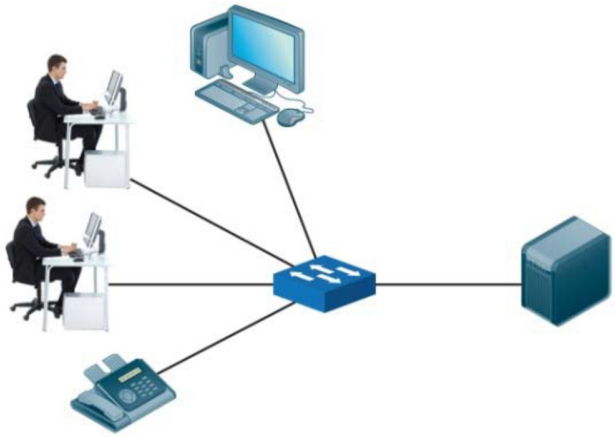
Sastoji se od najčešće routera, računala, printera, mobilnih uređaja, IPTV i sl. Takav sustav radi na principu WORKGROUP-e, nije dio domene, nema glavni server, vatrozid ili backup sustav osiguran. U domovima takvo okruženje je dio svakidašnjice, ali u poslovnom svijetu vrlo je nesiguran i pušta nas ranjivim pred napadima, virusima i krađom informacija.

Zaštita u takvom sustavu najčešće dolazi lokalno u vatrozidu računala, vatrozid-u routera i računalnom anti-virusu, doduše sve takve metode su prepuštene korisniku.

U većim sustavima ili sustavima sa osjetljivim informacijama traže se rješenja gdje postoji jedan veći, objedinjeni i siguran sustav koji sadrži zajedničku, višeslojnu kontrolu i administraciju u cjelini. Takvi sustavi su pod kontrolom jednog ili više servera i servisa i često se zovu zatvoreni mrežni sustavi, LAN u manjim sredinama, WAN u većim.

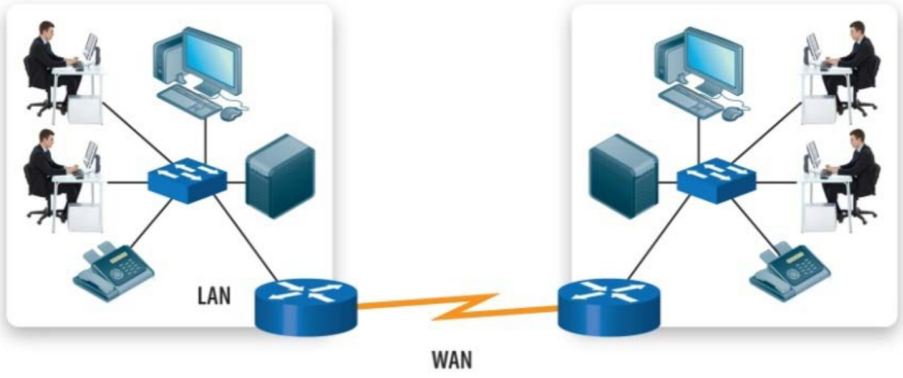
1.2. Zatvoreni mrežni sustavi

LAN – Lokalna mreža (engl. Local Area Network) je mreža uređaja pod kontrolom ovlaštenih osoba ili administratora koja regulira politiku sigurnosti i pristupa. Lokalnu mrežu čine uređaji povezani na maloj fizičkoj udaljenosti i obično obuhvaća jedno zemljopisno područje, pruža servise za korisnike u zajedničkoj organizacijskoj strukturi, kao što je tvrtka, ustanova ili regija.



Slika 1. LAN

WAN – mreža širokog područja (engl. Wide Area Network) je mreža koja spaja lokalne mreže koje su fizički na različitim geografskim područjima. U pitanju je mreža uređaja (engl. host) koji su povezani brzim i sporim vezama.



Slika 2. WAN

Kada tvrtka ima lokalne mreže koje su geografski odvojene, u pravilu moraju koristiti telekomunikacijske usluge odnosno usluge pristupa Internetu ISP-a (eng. ISP – Internet Service Provider) koji je obično i TSP (eng. TSP - Telecommunications Service Provider) kako bi se povezale. Veza između lokalnih mreža (LAN-ova) obično se ostvaruje preko zakupljenih telekomunikacijskih veza (vodova).

Dvije podskupine mreža koje na neki način možemo smatrati "hibridnima" i koje je u biti teško pravilno svrstati su:

Intranet (često nazvan „lokalni Internet“) međusobno koristi iste tehnologije kao i Internet, ali pristup imaju samo zaposlenici tvrtke. On po svojoj veličini spada u LAN mreže, ali s druge strane koristi vrlo sličnu infrastrukturu kao Internet.

Extranet (hrv. Ekstranet) je tip mreže koji biranim vanjskim korisnicima (partnerima, clientima itd.) daje pristup limitiranim informacijama tvrtke. Ova vrsta mreže također spada po svojoj veličini u LAN mreže, ali je s druge strane, budući da obično koristi resurse Interneta također na granici LAN – a i Interneta.[1]

U takvim poslovnim okruženjima koji sadrže kompleksne sigurnosne sustave nalazimo temelj svih poslovnih institucija: baze podataka.

[1] Milan Korać; Dario Car, „Uvod u računalne mreže“, (2014.).

2. BAZE PODATAKA

„Centralno mjesto informacijskog sustava je baza podataka. U bazi podataka su pohranjeni podaci o dijelu stvarnog svijeta za koji je razvijen informacijski sustav. Baza podataka je skup međusobno povezanih podataka pohranjenih s ciljem da na optimalni način posluže u raznim primjenama. Podaci se spremaju neovisno o programima koji ih koriste, zajedničkim pristupom dodaju se novi podaci te mijenjaju i premještaju postojeći.

Podaci se pohranjuju u bazu podataka koristeći odgovarajući model podataka. Model podataka je skup osnovnih koncepata koji definiraju postupak opisa podataka, manipulaciju podacima, mogućnost postavljanja upita i integritet podataka. Model podataka definira logičku strukturu baze podataka. Model podataka predstavlja osnovni koncept za razvoj sustava za upravljanje bazom podataka (eng. *Database Management System, skraćeno DBMS*) pomoću kojeg se implementira odgovarajuća baza podataka.„[2]

U ovome radu fokus će biti na sustavu koji se smatra najboljom solucijom u poslovnom okruženju, Oracle, te PostgreSQL i izazovi vezani uz baze podataka unutar zatvorenog mrežnog sustava.

2.1 PostgreSQL

PostgreSQL je sustav za upravljanje objektno relacijskim bazama podataka. Objektno relacijska baza podataka je baza u kojoj su podaci u odvojenim tablicama, što daje brzinu i fleksibilnost pri obrađivanju podataka. Tablice su povezane definiranim relacijama što omogućuje kombiniranje podataka iz nekoliko tablica.

[2] http://www.pfri.uniri.hr/~tudor/materijali/Informacijski%20sustavi,%20baze%20podataka.htm

PostgreSQL baza otvorenog je koda, što znači da je dozvoljeno svakome da ju koristi i prilagođava za svoju namjenu. Iako je besplatan, PostgreSQL usporediv je sa komercijalnim bazama podataka kao što su Sysbase, Oracle i DB2.

PostgreSQL je utemeljen na modelu client-server.

PostgreSQL se sastoji od dvije međusobno povezane aplikacije:

- Serverske aplikacije, zvane postgres, koja je zadužena za rad sa datotekama baze, za veze od clientskih aplikacija prema bazi i obradu istih.
- Client aplikacije koja koristi bazu podataka. Client može biti tekstualno orijentiran, imati grafičko sučelje, biti web server ili specijalizirana aplikacija za nadzor i održavanje baze podataka. PostgreSQL komunikaciju obavlja preko TCP/IP sučelja. On stvara novi proces za svako spajanje kako bi se omogućilo paralelno obrađivanje velikog broja korisnika. Nakon toga više ne komunicira s postgres-om, nego s novim procesom koji je stvoren za tu clientsku aplikaciju. [3]

2.1. ORACLE

Oracle je baza podataka namijenjena za velike ustanove i korporacije gdje se raspolaže sa ogromnim količinama podataka, gdje od pouzdanosti baze podataka ovisi opstanak kompanija i sigurnost. Oracle je relaciona baza podataka koja pored baze podataka uključuje i cijeli skup pomoćnih alata i aplikacija kao što su e-mail i web serveri.

Oracle koristi cluster, ujedinjavanje više manjih servera ili računala u jednu logičku cjelinu koja gledana izvana djeluje kao integrirano. Takva tehnologija se zove **RAC** (Real Application Clusters**)**, gdje se ne mora ulagati u kompleksnu i skupu opremu, već u slučaju potrebe za većim kapacitetom i obradom, dodaju se nova računala u cluster.

Najveća prednost takvog sustava je daljnji rad u slučaju pada jednog ili više računala,

[3] Douglas K., Douglas S. *PostgreSQL: The comprehensive guide to building, programming, and administering PostgreSQL databases*, (2005.), 7-36.

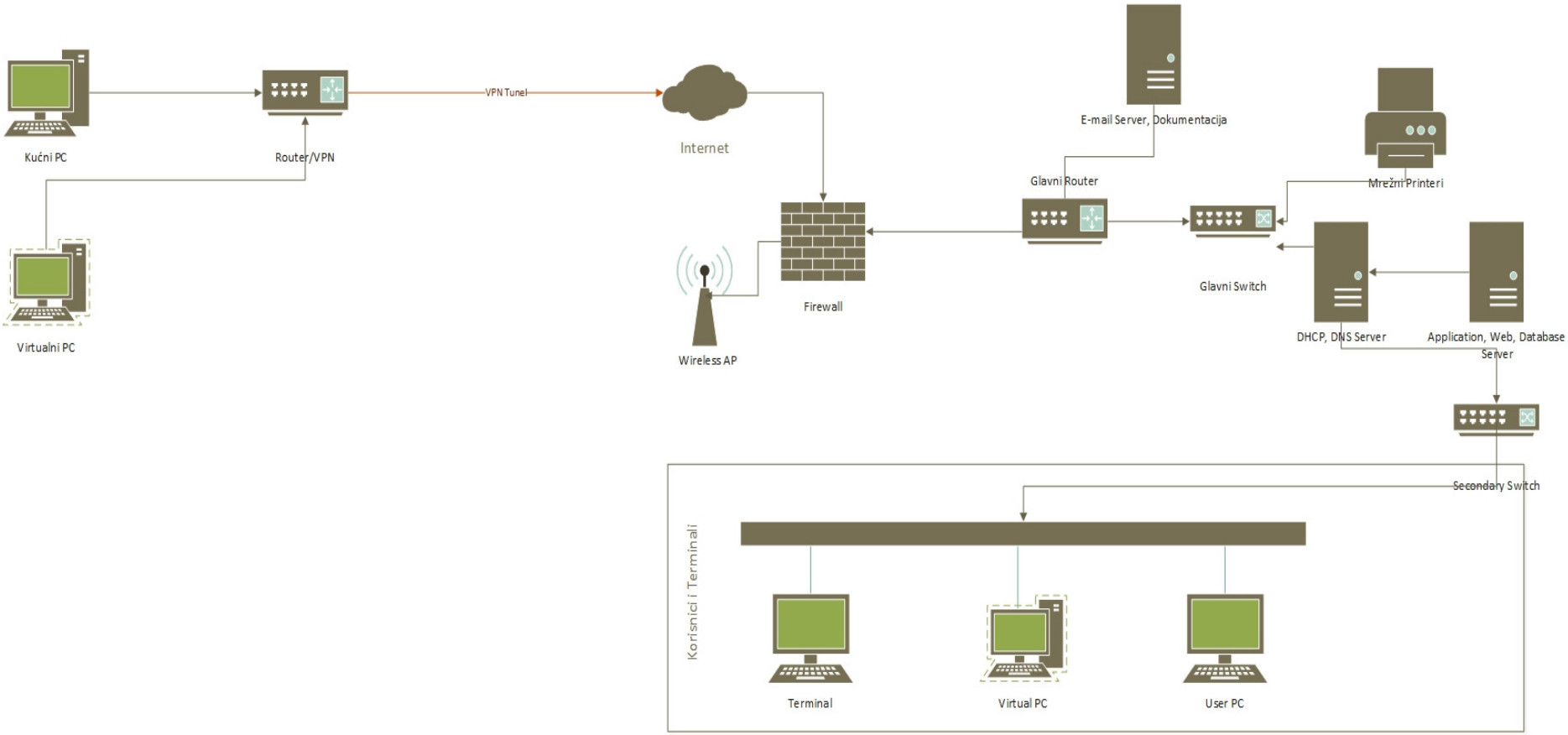
gdje se lakom zamjenom sa drugim računalom sustav obnavlja. Fokus Oracle baze podataka je velika mogućnost programiranja unutar okruženja. Oracle ima najveću manu u činjenici da je rađen za velike baze. Njegova složenost i manjak user-friendly alata, te potreba za striktnom specijalizacijom odbija korisnike i smanjuje fleksibilnost rada. Ako se uključuju limitacije software-a i cijena, vidi se kome je namijenjen Oracle: Velikim korporacijama i institucijama orijentiranim na sigurnost.

Oracle baza sastoji se od datoteka pohranjenih na disku te memorijskih struktura i procesa koji se izvršavaju na baznom serveru. Memorijske strukture i procesi čine instancu baze. Prvi je korak prilikom pokretanja baze izgradnja instance u memoriji. Nakon toga, instanca dohvaća i čita datoteke na disku. Memorijske strukture koje čine instancu pohranjene su u SGA (System Global Area) memorijskom segmentu. SGA se alocira pri pokretanju instance. Sastoji se od nekoliko komponenata čija se veličina može dinamički mijenjati dok je instanca aktivna. Korisničke aplikacije uspostavljaju sesije s bazom.

Sesija se sastoji od korisničkog procesa (aplikacije) koji se izvršava na lokalnom računalu i serverskog procesa koji se izvršava na serveru. Korisnički proces generira SQL naredbe, a serverski ih proces izvršava. Svakoj je sesiji pridružen jedan serverski proces. Svaki takav proces zauzima dio radne memorije za vlastite potrebe. Ta se memorija naziva PGA (Program Global Area). PGA je memorija koju koristi isključivo jedan serverski proces, dok je SGA na raspolaganju svim serverskim procesima. Podatkovne se strukture mogu promatrati s dva aspekta – logičkog i fizičkog. Podaci su u logičkom smislu pohranjeni u segmentima. Postoje različiti tipovi segmenata, a najznačajniji su tablice i indeksi. Segmenti su fizički pohranjeni u podatkovnim datotekama na disku. Veze između fizičkih i logičkih struktura podataka pohranjene su u rječniku podataka. [4]

[4] John Watson . *Oracle Database 11g: Administration I,* (2008.)

Baze podataka se u zatvorenim informacijskim sustavima najčešće pohranjuju na aplikacijskim ili web serverima fizički ili u cloudu. Takav sustav se najčešće sastoji od kompleksnih struktura koje su spojene sa internetom preko routera i firewalla, koji preko switcheva i servera vode kroz ukupnu infrastrukturu do korisničke baze. U sljedećem dijelu opisati ćemo temeljne strukture mreže unutar zatvorenog informatičkog sustava i objasniti integriranost baza podataka unutar njih.



Slika 3. Zatvorena mrežna arhitektura

3. MREŽNA ARHITEKTURA I SIGURNOST

Objekt može biti u fizičkom stanju sigurnosti ili teoretskom stanju sigurnosti. U fizičkom stanju, objekt je siguran ako je zaštićen barijerom, ima sigurna unutarnja i vanjska područja, a može i zaustaviti prodiranje uljeza.

Ovo stanje sigurnosti može biti zajamčeno ako su sljedeća četiri mehanizma zaštite u upotrebi: odvraćanje, prevencija, otkrivanje i odgovor.

Odvraćanje je obično prva linija obrane protiv uljeza koji pokušavaju dobiti pristup. Djeluje tako da stvara atmosferu namijenjenu za zastrašivanje uljeza. Ponekad to može uključivati upozorenja teškim posljedicama, ako je sigurnost probijena.

Prevencija je proces koji pokušava spriječiti uljeza pri dobivanju pristupa na resurse sustava. Prepreke su firewall (vatrozid), demilitarizirana zona (DMZ), i korištenje pristupnih alata kao što su ključevi, pristupne kartice, biometrija i sl. koji dopuštaju samo ovlaštenim korisnicima korištenje i pristup objektu. [5]

Detekcija se događa kada je uljez uspio ili je u postupku stjecanja pristupa sustavu. Signali iz procesa detekcije su upozorenja da postoji uljez. Ponekad ove obavijesti mogu biti u realnom vremenu i čuvati daljinu analizu od strane sigurnosnog osoblja.

Odgovor je mehanizam koji nastoji odgovoriti na neuspjeh prva tri mehanizama. Djeluje tako da pokušava spriječiti i / ili zaustaviti buduće štete ili pristup objektu.[6]

Računalna sigurnost

[5] U računalnoj sigurnosti, DMZ i demilitarizirana zona je fizička ili logička podmreža koja kontrolira izlaze i ulaze prema nesigurnim mrežama kao što je Internet.

[6] Springer-Verlag J.M. Kizza, *Guide to Computer Network Security, Computer Communications and Networks*, (2015.), 41.

Računalna sigurnost je grana računalne znanosti, s naglaskom na stvaranje sigurnog okruženja za korištenje računala. Ima fokus na "ponašanje korisnika" i protokole kako bi se stvorilo sigurno okruženje za svakoga tko koristi računala. To kompleksno polje, dakle, uključuje četiri područja interesa: studija računalnih etika, razvoj software i hardware protokola i razvoj najbolje prakse. [7]

Sigurnost mreže

Računalne mreže su mreže distribuiranih[8] računala koje ili koriste i dijele resurse iz jednog središnjeg računala ili dijele resurse koji se samo koriste za mrežni rad. Kada se govori o sigurnosti mreža govori se o cijelom sustavu: mreži. Sigurnost mreža je vrlo široka grana informatike, koja se dotiče s računalnom sigurnošću ali seže u još mnogo vanjskih faktora. U takvim sustavima se stvara okruženje u kojem mreža i svi njeni resursi, podaci i korisnici sigurni.

Sigurnost informacija

Sigurnost informacija je još veće područje koje uključuje računala i sigurnost računalnih mreža. Ovo područje se nalazi u različitim disciplinama, uključujući i računalne znanosti, poslovno upravljanje, informacijske studije i inženjering. To uključuje stvaranje stanja u kojem su informacije i podaci sigurni. U ovom modelu, informacije ili podatci, su u pokretu kroz komunikacijske kanale ili uskladištene u bazama podataka na serveru. To, dakle, uključuje proučavanje ne samo detaljnih matematičkih kriptografskih nacrta, komunikacija, transporta, protokola i najbolje prakse već i stanja podataka i informacija u pokretu. [9]

[7] Mario Radovan, *Računalne mreže 1 – povezivanje računala i mreža, sveučilište u Rijeci, odjel za informatiku*, (2010.), 163 – 164.

[8] Mreža koja se širi van područja jednog računala.

[9] „Sigurnost sustava za upravljanje bazama podataka CCERT-PUBDOC-2006-10-171," 5-17.

Osiguranje računalne mreže

Stvaranje sigurnosti u računalnim mrežnim modelima znači stvaranje sigurne okoline za različite resurse. Osigurava se izvor koji je zaštićen od unutarnjeg i vanjskog neovlaštenog pristupa. Ta sredstva, fizička ili ne, su objekti. Osiguravanje sigurnosti objekta znači štititi objekt od neovlaštenog pristupa, kako unutar objekta tako i izvana. Sustavni objekti mogu biti materijalni i nematerijalni. U modelu računalnih mreža, materijalni objekti su hardverski resursi u sustavu, a nematerijalni objekti informacije i podaci.

Hardware

Zaštita hardverskih resursa uključuje zaštitu:

- Objekta krajnjeg korisnika, u koje uključujemo komponente korisničkog sučelja, kao što su svi dijelovi ulaznog sustava, uključujući tipkovnicu, miš, zaslon osjetljiv na dodir, svjetlosno pero i drugo
- Mrežne objekte kao što su firewall, hub, switch, router i gateway koji su ranjivi na vanjske napade
- Mrežni komunikacijski kanali koji sprječavaju prisluškivanje u svrhu presretanja domene ili mreže

3.1. Uređaji u mreži

Svi krajnji uređaju u mreži pridonose sigurnosti same mreže. U ovom poglavlju govorimo o sustavima i dijelovima mreže koji čine zatvoreno i sigurno mrežno okruženje.

„Krajnji uređaji mogu biti ishodište ili odredište podataka koji se šalju mrežom. Za identifikaciju ishodišnog i odredišnog uređaja svaki uređaj na mreži ima adresu. U trenutku pokretanja komunikacije ishodišni uređaj koristi adresu odredišnog uređaja kako bi odredio gdje se podaci šalju.
Potrebno je razlikovati logično i fizičko adresiranje uređaja. Logičko adresiranje određuje administrator mreže dok svi uređaji koji sudjeluju u komunikaciji imaju unaprijed postavljenu fizičku adresu.

U računalnim mrežama krajnji uređaj (*engl. host, end system*) može imati ulogu clienta, servera ili ulogu clienta i servera. Prema tome treba biti svjestan da host nije uvijek samo client na kojem je pokrenuta neka aplikacija (npr. Internetski preglednik) iako je to često slučaj, nego host može biti i Web server. Zapravo mehanizam client/server (*hrv. Klijent/Poslužitelj*) danas dominira Internetom i velika je količina internetskih aplikacija koje funkcioniraju na ovaj način (npr. Web stranice, e-mail, FTP, newsgroups…).

Općenito možemo reći da je **Client** (hrv. klijent) sustav (npr. računalo) koje udaljeno pristupa servisima na drugom uređaju i potražuje podatke. **Server** (hrv. Poslužitelj) ima instaliran software (servis) koji pruža uslugu clientu i koji mu može omogućiti pristup tim podacima. Budući da i client i server zapravo kao hardversku podlogu mogu imati računala, možemo reći da je client/server arhitektura po kojoj funkcioniraju brojne aplikacije na Internetu zapravo zasnovana na **distribuiranim aplikacijama**.[10] Nadalje, budući da je Internet dobrim dijelom građen upravo od takvih

[10] Distribuirani sustav je skup nezavisnih računala i pripadne programske opreme koji su zajedno predstavljeni korisniku kao jedan cjeloviti sustav.

sustava, posredno se može zaključiti da je i Internet baziran na distribuiranim aplikacijama.“[11]

Client

Client je ono računalo koje daje zahtjev za operaciju koja se izvodi na serveru baze podataka. Client također može biti web preglednik ili bilo koja vrsta programa. U složenim arhitekturama, client se spaja na server baze podataka kroz jedan ili više servera aplikacija.

Server

Server (poslužitelj) je računalo koje pruža podatke za druga računala. Može poslužiti podatke sustava na lokalnoj mreži (LAN) ili mreže širokog područja (WAN) preko interneta.

Postoje razne vrste servera, uključujući web server, mail server i data server. Svaka vrsta ima svoj software specifičan za svrhu servera. Na primjer, web-server može pokrenuti Apache Database Server ili PostgreSQL Server gdje je cilj osigurati pristup na baze podataka unutar sustava. Mail server može pokrenuti program kao što je Exim ili iMail, koji pruža SMTP usluge za slanje i primanje e-pošte. Data server može koristiti Samba ili Windows servise za razmjenu datoteka preko mreže.

Gotovo svako osobno računalo ima mogućnost pružati uslugu mrežnog servera. Doduše računala koja su raspoloživa na software/hardware bazi imaju mogućnosti i konfiguracije koje su namijenjene isključivo mrežnim operacijama. Na primjer, dedicated (posvećeni) serveri imaju velike količine brze RAM memorije, brži procesor i više visoko kapacitetnih hard diskova. Dodatno, posvećeni serveri su često spojeni na dodatna redundantna napajanja, više mrežnih priključaka, mreža i drugih servera. Veze sa takvim mogućnostima i konfiguracijama su potrebne jer velike količine korisnika i

[11] Milan Korać; Dario Car, „Uvod u računalne mreže“, (2014.).

programa ovisi o njihovim performansama koje moraju biti učinkovite, točne i pouzdane.[12]

Dok je bilo koje računalo može biti konfigurirano kao server, većina velikih poduzeća koriste ugradbeni hardware dizajniran posebno za funkcionalnost servera. Ti sustavi često zauzimaju minimalan prostor i imaju korisne značajke kao što su LED svjetla statusa i hot-swap (vanjska zamjena kroz ladice) tvrdih diskova. Više ugradbenih servera se mogu staviti u zajedničku policu i često dijele iste monitore i ulazne uređaje. Većini servera se može pristupiti i na daljinu pomoću software-a za daljinski pristup, tako da ulazni uređaji često nisu niti potrebni.

Dok serveri mogu izvoditi na različitim vrstama računala, važno je da je hardware može izdržati zahtjeve servera. Bez obzira na vrstu servera, brz mrežni priključak je najbitnija točka, unutar i van mreže, jer su svi podaci teku kroz njih.

Da bi se radilo u jedinstvenom mrežnom okruženju gdje postoje mnoga računala i hardware/software sustavi a često ovise o jednom ili nekoliko server računala, server često ima posebne karakteristike i mogućnosti, uključujući:

- Sposobnost za ažuriranje hardvera i softvera bez ponovnog pokretanja ili ponovno podizanje sustava.
- Napredne backup mogućnosti za česti backup kritičnih podataka.
- Napredne mrežne performanse.
- Automatski (nevidljiv za korisnika) prijenos podataka između uređaja .
- Visoku sigurnost za resurse, podatke i zaštitu memorije.

[12] Bažant, A., (et al.). *Osnovne arhitekture mreža*, (2004.).

Aplikacijski serveri

Aplikacijski server omogućuje pristup podacima za clienta. On služi kao sučelje između clienta i jednog ili više servera baza podataka i u njemu se nalazi i sama aplikacija.

Aplikacijski server omogućuje tako zvane, tanke cliente, koji su clienti opremljeni sa minimalnim softverskim konfiguracijama, za pristup aplikacijama bez potrebe za tekuće održavanje client računala. Aplikacijski server može obavljati neke preinake podataka za clienta, čime se smanjuje opterećenje na client radnoj stanici.

Aplikacijski server preuzima identitet clienta kada se obavlja operacija na serveru baze podataka. Privilegije aplikacijskog servera treba ograničiti kako bi se spriječilo obavljanje nepotrebnih i neželjenih operacija tijekom rada clienta.

Serveri baza podataka

Server baze podataka osigurava podatke koje je zatražio aplikacijski server za račun clienta. Baza podataka obavlja sve obrade upita.

Server baze podataka može provjeravati operacije koje se izvode od aplikacijskog servera u ime klijenata i poslova koje obavlja server aplikacija na svoje ime (Monitoring). Na primjer, operacija clienta može zatražiti informacije za prikaz na clientu, a operacija aplikacijskog servera može zatražiti vezu na server baza podataka.

3.2. Mrežni i Distribuirani sustavi

Osnovna razlika između arhitekture mrežne i softverske arhitekture u cjelini je da komunikacija između dijelova je ograničena na prolazne poruke, ili ekvivalent poruke koja prolazi ako se učinkovitiji mehanizam može odabrati na vrijeme izvođenja koji se temelji na lokaciji komponenata.

Razlika između distribuiranih sustava i mrežnih sustava je opisana kao: distribuirani sustav je onaj koji gleda korisnike kao običan centralizirani sustav, ali radi na više, nezavisnih procesora. Za razliku od toga, sustavi za mreže su oni sposobni za rad preko mreže, ali ne nužno na način koji je transparentan za korisnika. U nekim slučajevima je poželjno da korisnik zna razliku između akcije koja zahtijeva mrežni zahtjev i ona koja je moguća na njihovom lokalnom sustavu, osobito kada uporaba mreža podrazumijeva dodatnu upotrebu resursa.

3.2.1. Client-Server

Client-server (client-poslužitelj) arhitektura je okruženje gdje server poslužuje visoko zahtjevne i složene usluge za clienta kao potrošača. Takvi procesi mogu uključiti korištenje aplikacija, spremanje i dijeljenje podataka, mrežnih i lokalnih printera, baza podataka i/ili direktnog korištenja sirove snage servera.

Client-server arhitektura djeluje samo kada client traži i šalje resurse i procese prema serveru preko mrežne veze, koja je procesuirana i vraćena clientu. Server mora imati mogućnost procesiranja više clienta istovremeno, ali s druge strane jedan client može biti povezan sa više servera istovremeno, gdje svaki pruža određene usluge. U svojem najjednostavnijem obliku Internet također spada u client-server strukturu gdje Web server opslužuje velike količine korisnika sa podacima na web stranicama.

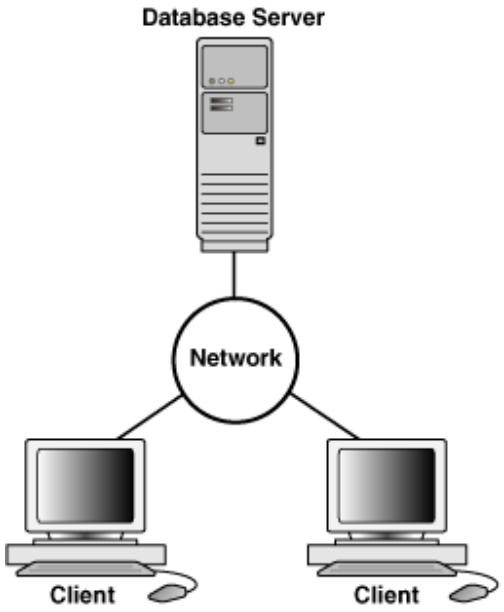
3.2.2. Pregled client / server arhitekture

U Oracle ili SQL Database okruženju, baza podataka aplikacija i baza podataka su odvojeni u arhitekturi client / server:

Client pokreće aplikaciju baze podataka, na primjer, SQL * Plus ili Visual Basic program za unos podataka, koji pristupa informacijama baze podataka i interakciju s korisnikom.

Server pokreće Oracle ili SQL Database software i upravlja funkcijama potrebnim za istodoban, zajednički pristup podacima na Oracle ili SQL bazi podataka.

Iako clientska aplikacija i baza podataka se može izvoditi na istom računalu, veća učinkovitost se postiže kada se client i server pokreću od strane različitih računala spojenih preko mreže.[13]



Slika 4. Jednostavna arhitektura baze podataka

[13] http://docs.oracle.com/cd/A57673_01/DOC/server/doc/SCN73/ch20.htm#o client/server

3.2.3. Prednosti client / server arhitektura

Oracle ili PostgreSQL client / server arhitektura pruža sljedeće prednosti: Aplikacije clienta nisu korištene za obavljanje obrade podataka. Umjesto toga, one traže unos od korisnika, zatraže podatke s servera, a zatim analiziraju i prezentiraju te podatke pomoću prikaza mogućnosti njihova računala ili terminala (na primjer, pomoću grafike ili tablice).

Aplikacije client ne ovise o fizičkoj lokaciji podataka. Čak i ako se podaci premjeste ili distribuiraju na drugim serverima baza podataka, aplikacija će i dalje funkcionirati s malo ili bez preinaka.

Oracle ili SQL baza iskorištava multitasking i zajedničke memorijske sadržaje svojih temeljnih operativnih sustava. Kao rezultat toga, ona pruža najviši mogući stupanj podudarnosti, integriteta podataka i izvedbe svojim clientskim aplikacijama.

Clientske radne stanice ili terminali mogu biti optimizirani za prikaz podataka (na primjer, pružajući grafiku i podršku za miša), a server može biti optimiziran za obradu i pohranu podataka (na primjer, velike količine memorije i prostor na disku).

U mrežnom okruženju, možete koristiti jeftine clientske radne stanice za pristup udaljenim podacima na serveru.

Baza podataka može rasti kada se i sam sustav širi. Možete dodati više servera za distribuciju opterećenja za baze podataka u mreži (horizontalno po veličini), ili možete premjestiti bazu podataka na miniračunalo ili mainframe da bi iskoristili performanse većeg sustava (vertikalno po veličini). U svakom slučaju, podaci i aplikacije održavaju se s malo ili bez preinaka, jer Oracle i SQL Database su prenosivi između sustava.

U mrežnom okruženju, zajednički podaci pohranjuju se na serverima, a ne na svim računalima, gdje je lakše i učinkovitije upravljati s istodobnim pristupom.

U mrežnom okruženju, clientske aplikacije podnose zahtjeve baza podataka prema serveru koristeći SQL izjave. Nakon što ih je server primio, svaki SQL proces obrađuje

server, koji vraća rezultate za clienta. Mrežni promet je sveden na minimum, jer se samo zahtjevi i rezultati dostavljaju putem mreže.[14]

Ostali fizički dijelovi LAN-a također su vrlo bitni za sigurnost same mreže:

3.3. Mrežni hardware

Router **(Usmjernik)**

„Routeri povezuju i omogućavaju komunikaciju između računalnih mreža. Router može biti računalo ili poseban uređaj specijaliziran za usmjeravanje podataka kroz mrežu.
Router, kao posebni uređaj, je računalo koje ima gotovo sve komponente (CPU, memoriju, sistemsku sabirnicu, ulazno-izlazna sučelja…) i operacijski sustav pomoću kojeg se konfigurira za usmjeravanje paketa.
Može se koristiti za segmentiranje velikih LAN mreža, ali njegova glavna upotreba je u WAN mrežama. Routeri su osnova velikih LAN i WAN mreža i Interneta.“[15]

Firewall

U informatici, firewall (vatrozid) kao zaštita između pouzdanog sustava ili mreže i izvan veze, kao što je Internet.

Firewall postoji u stanju hardware-a ili software-a i često se koriste oba. U mnogim organizacijama i tvrtkama nalazimo hardware firewall. Jedan ili dva firewall-a mogu se koristiti za stvaranje zone koja sprječava nepouzdane podatke da ikad dostignu LAN. Software Firewall postoji na lokalnim računalima i operativnim sustavima i mogu se prilagoditi po želji. Windows i OS X uključuju built-in firewall, ali napredniji firewall programi ili oprema nude se od strana vanjskih kompanija.

[14] Tamer Özsu, Patrice Valduriez*, Principles of distributed database systems*., (1999.), 111-121.

[15] Milan Korać; Dario Car, „Uvod u računalne mreže“, (2014.), 6-8.

Firewall se može konfigurirati na nekoliko različitih načina. Osnovni firewall može dopustiti promet iz svih IP adresa osim onih označena na crnoj listi. Više siguran firewall se konfigurira da se samo dijeli promet od sustava ili IP adrese navedene u popisu dopuštenih. Većina firewall-a koristi kombinaciju pravila za filtriranje prometa, kao što su blokiranje poznatih prijetnji, a propušta dolazni promet iz pouzdanih izvora. Firewall također može ograničiti odlazni promet kako bi se spriječio spam ili napadaji na sustav.[16]

Neki firewall-ovi čak i "uče" s vremenom i dinamički razvijaju vlastita pravila filtriranja. U tom slučaju se sustav sam prilagođava novim prijetnjama i regulira promet unutar sustava.

Switch

Switch ili preklopnik se koristi za umrežavanje više računala zajedno. Za manje tržište koristi se od 4 do 8 portova. Portovi služe za direktno povezivanje sa računalom preko UTP kabela. Switch u velikom sustavu može imati više od 50 portova.

Switch može ograničiti promet svakoga porta, tako da regulira svim računalima jednaku količinu bandwidtha. Iz tog razloga, možete misliti na switch kao „pametno čvorište“. Međutim, switchevi nemaju mogućnosti firewall-a i sposobnost zapisivanja koje imaju routeri. Routeri se često mogu konfigurirati (obično putem web sučelja), dok prekidači rade samo onako kako je hardware bio dizajniran. Iako određeni switchevi od kompanija kao CISCO pruže mogućnost kompletne konfiguracije brzina i spajanja na mrežu.[17]

[16] *Ibidem*, 6.

[17] *Ibidem*, 7.

3.4. Mrežni software

Zaštita software resursa uključuje zaštitu operativnih sustava, servera, protokola, preglednika, aplikacijskih software-a i intelektualnih objekata pohranjenih na mreži na diskovima i bazama podataka. To također uključuje zaštitu software-a klijenata, kao što su ulaganja portfelja, financijski podatci, evidencije nekretnina, slike i slične osobne podatke najčešće pohranjeni na kućna i poslovna računala.

3.5.1 Virtualizacija

Pod pojmom „virtualizacija“ podrazumijeva se predstavljanje pojedinih funkcionalnosti i resursa. Odnosno, za korisnika nema razlike između stvarnog i virtualnog ostvarenja djelovanja, ali stvarne vrijednosti i aktivnosti u virtualnom okruženju razlikuju se od onih prikazanih.

Stvarni operacijski sustav komunicira izravno sa hardware-om računala, dok virtualni operacijski sustav ima za korisnika sva obilježja stvarnog sustava, ali se pokreće u drugom stvarnom sustavu. Komunikacija se ne obavlja sa hardware-om nego sa drugim sustavom. Taj drugi sustav oponaša hardware u komunikaciji s virtualnim sustavom. Rad hardware-a se simulira programski pa je riječ o virtualnom hardware-u. Virtualizacija može značiti da korisnik preko virtualnog sučelja više sustava koristi kao jedan, a može i značiti da se na jednom računalu simulira rad nekoliko sustava.

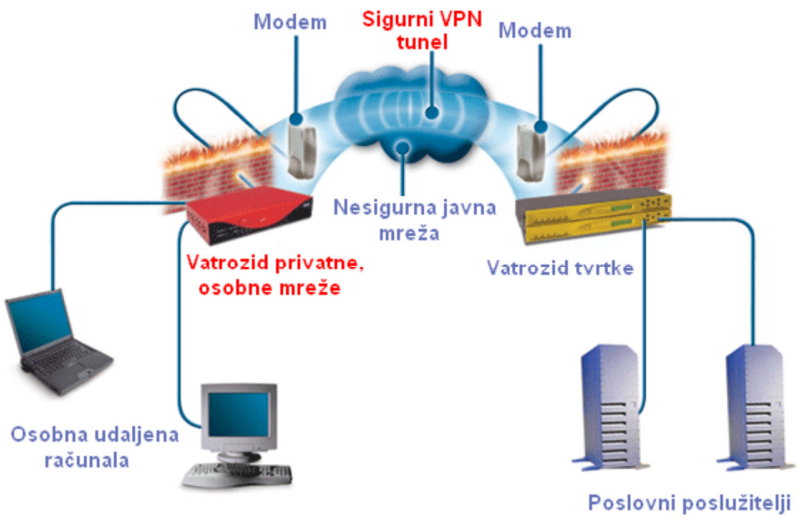
Virtualizacija omogućuje učinkovitije korištenje računalnih, memorijskih i mrežnih resursa. Zbog svojstva apstrakcije omogućuje i zaštitu osjetljivih dijelova sustava tako što im ograničava pristup virtualnim sučeljem. [18]

VPN Virtualna privatna mreža (eng. VPN – Virtual Private Network) drugačija je virtualizacijska tehnologija od virtualizacije operacijskih sustava. U ovom slučaju virtualizacija se obavlja u sustavu mreže, a virtualiziraju se svojstva mrežne komunikacije. VPN omogućuje uspostavljanje zaštićene komunikacije između računala u nesigurnoj javnoj mreži. Na taj način između različitih mreža simulira komunikacija sa

[18] Amit Singh*, An Introduction to Virtualization*, (2009.)

svojstvima one koja bi se odvijala u lokalnoj mreži. Ostala računala iz javne mreže nemaju pristup podacima koji se šalju preko VPN veze.

Tvrtke često koriste VPN da bi komunicirali na više lokacija. Na primjer, ako se server i baza podataka nalazi na jednoj lokaciji, a uredi ili poslovnice na drugoj, pomoći VPN veze se može omogućiti direktni prijenos i rad sa bazom podataka i programima, gdje se postiže direktni centralizirani rad i sustav koji se može lakše zaštititi. U manjem opsegu, pojedini korisnik može imati VPN račun s njihovom tvrtkom, što im omogućuje da se spojite na svoj ured i od kuće ili drugo mjesta. To je osobito korisno za poslovne putnike koji trebaju pristupiti uredske podatke iz svojih prijenosnih računala. Da bi se učinilo podatke sigurnim, tvrtka može postaviti VPN sa šifriranom vezom.[19]



Slika 5. VPN okruženje

[19] Scott Granneman, „Virtualization for security“, (2009.)

3.5.2. RDC

Remote desktop tehnologija omogućuje da vidite radnu površinu drugog računala na svojem računalu. Korisnik može otvoriti mape, premještati datoteke, pa čak i pokretati programe na udaljenom računalu, izravno iz vlastitog desktopa. Windows i Macintosh računala podržavaju povezivanje preko takvih servisa, iako je drugačija implementacija u sustavima.

Windows uključuje Remote Desktop kao dio operativnog sustava. Remote Desktop koristi Microsoft Terminal Services i Remote Desktop Protocol (RDP) za spajanje na udaljeno računalo. Daljinske veze otvaraju se putem Windows 'Remote Desktop (RDC), koji se također naziva i Terminal Services Client (TSC). Ovaj program omogućuje korisnicima podešavanje i upravljanje daljinske veze s drugim računalima. Za spajanje na drugi stroj, daljinski sustav mora biti konfiguriran tako da prihvati ulazne RDC veze.

Cijeli sustav omogućuje administratoru da se spaja na desktope pod njegovom mrežom i upravlja njihovim računalima u slučaju podrške ili uvida u informacije, pa sve do potrebama za sigurnošću i prebacivanju podataka. Čest način korištenja RDC sustava je mogućnost ulaska na server putem otvorenog porta na routeru i zadanoj vanjskoj IP adresi koju ISP (Internet service provider) može staviti kao fiksnu i onda služi kao točka spajanja. Na taj način, pomoću svojeg username i passworda korisnik može raditi na virtualnom desktopu i spajati se na baze podataka od doma ili sa radnog mjesta.

Razlika između VPN i RDC sustava je u tome što je VPN stalna veza i naše računalo se „prebacuje“ na mrežu od servera i funkcionira na njihovom sustavu, dok RDC otvara svoj prozor i instancu gdje se mi spajamo na virtualni desktop koji dodjeljuje server. VPN u ovom slučaju koristi intenzivnije mogućnosti routera i prebacivanja podataka preko Interneta, što može „zagušiti“ mrežu i onemogućiti rad drugima koji ne rade na bazama, dok RDC ima nedostatak što preopterećuje resurse servera.

4. SIGURNOST BAZA PODATAKA

DBMS[20] može se koristiti za izgradnju različite vrste baza podataka. Svaka baza podataka pohranjuje posebnu zbirku podataka te se koristi za specifičnu namjenu. Tijekom godina, kako su se tehnologije i inovativne uporabe baza podataka razvijale, drugačiji postupci su korišteni za klasificiranje baze. Na primjer, baza podataka može se razvrstati po broju podržanih korisnika, gdje se nalaze podaci, vrsta podataka koji pohranjuje, namjerna uporaba podataka, te stupanj do kojeg su podaci strukturirani.

Broj korisnika određuje da li je baza podataka je klasificirana za jednog korisnika (single-user) ili višekorisnička. Single-user baze podataka podržava samo jednog korisnika za vrijeme korištenja. Drugim riječima, ako korisnik A koristi bazu podataka, korisnik B i C moraju čekati da korisnik A završi sa radom. Single-user baze podataka koje se izvodi na osobnom računalu nazivaju se desktop baze podataka. Nasuprot tome, višekorisnička baza podataka podržava više korisnika u isto vrijeme. Kada višekorisnička baza podataka podržava relativno mali broj korisnika (često manje od 50) ili određenog odjela unutar organizacije, to se naziva radne grupe baza podataka. Kada je baza podataka se koristi od strane cijele organizacije i podržava mnoge korisnike (više od 50, obično stotine) u mnogim odjelima, baza podataka je poznat kao poduzeće baze podataka.

Elementi zaštite sustava za upravljanje bazama podataka

Ugrađivanje sigurnosnih elemenata izravno u SUBP-ove i njihova ispravna primjena jedini su pravi način za uklanjanje ranjivosti. Ti elementi obuhvaćaju dodjeljivanje primjerenih ovlasti i dozvola pristupa, primjenu efektivnih korisničkih računa

[20] Database management system

i zaporki, primjerene metode nadzora i logiranja, korištenje enkripcije i nadzor nad pristupom tablicama.[21]

Dodjeljivanje primjerenih ovlasti i dozvola pristupa

Korisnicima se dodjeljuju minimalne potrebne ovlasti prema tzv. 'least privilege' načelu. Ovo načelo temelji se na dozvoli pristupa samo onim podacima baze i funkcionalnostima DBMS-a koji su korisnicima neophodno potrebni, obzirom na njihov status i opis posla. Pri tome treba voditi računa o ugrađivanju opisanih ograničenja izravno u SUBP, a ne u clientsku aplikaciju koja pristupa nekoj od pohranjenih baza podataka.

U svrhu podizanja računalne sigurnosti, ne preporuča se izravno dodjeljivanje ovlasti pojedinim korisničkim računima. Puno je bolji način da se oblikuju tzv. "uloge" (eng. roles) i da se njima dodijele pojedine ovlasti. Nakon toga se svakom korisniku dodaju "uloge" koje mu pripadaju. Na taj način jedan korisnik može zauzeti više uloga, a olakšano je dodjeljivanje i oduzimanje ovlasti vezanih uz radne zadatke.

Administratorima se savjetuje dokumentiranje zahtjeva za stvaranje, kao i samo stvaranje korisničkih računa, te pridjeljivanje i oduzimanje pojedinih uloga korisnicima. Također, prilikom promjene radnog mjesta ili radnog zadatka potrebno je preispitati ovlasti korisnika. Korisničke račune bivših zaposlenika potrebno je odmah ukinuti i provesti odgovarajuće postupke nad objektima baze podataka koji su pripadali takvim korisnicima.

4.1. Oracle

Oracle je najrašireniji DBMS i pokriva najveći dio tržišta za baze podataka. Razlozi za to su duga tradicija i podržanost od strane većine operacijskih sustava.

[21] S. Brian Suddeth, „Database – The Final Firewall“, (2002.).

Ranjivosti

Server preko kojega se pristupa bazi podataka zove se Listener. Zbog njegovog smještaja van baze podataka dolazi do problema sa sigurnošću, te udaljeno administriranje i postavljanje zaporka ne mogu se pratiti i često su nepoznate. Listener server nema uobičajene mogućnosti upravljanja zaporkama. Pomoću jednostavnih skripti mogu se probiti jednostavne zaporke jer ne postoji sustav onemogućavanja računa, odvojen nazor ili istjecanje zaporki.

Listener server može neovlaštenim userima dozvoliti pristup vrlo osjetljivim informacijama. U slučaju slanja paketa sa neispravnim „size of packet“ Listener daje paket koji sadrži prijašnju naredbu i uvid u pakete. Postoje problemi i greške u prepisivanju spremnika. U takvim slučajevima zlonamjerni korisnici mogu izvoditi programski kod koji manipulira SEH[22] mehanizmom. Unutar Oracle baza postoje i značajne ranjivosti povezane sa „SYS.LINK$“ tablicama. U tim tablicama se zapisuju korisnička imena i zaporke u vrijeme stvaranja te su na taj način izložene napadima. Podaci se spremaju bez enkripcije i može im pristupiti svaki korisnik.
Zbog takvih situacija i propusta vrlo je bitno zaštiti baze firewall-om i vanjskim zaštitnim programima.
Također postoje sigurnosti elementi s kojima možemo ojačati sustav iznutra.

Sigurnosni elementi

Korištenjem "PRODUCT USER PROFILES" alata moguće je onemogućiti korištenje određenih naredbi i funkcionalnosti od strane pojedinih korisnika. Tako se može globalno onemogućiti "HOST" mogućnost koja dozvoljava pristup operacijskom sustavu.[23]

Oracle omogućuje enkripciju korisničkih zaporki tijekom mrežne komunikacije. Ako se ova mogućnost uključi na clientskom i poslužiteljskom računalu, Oracle koristi

[22] Structured Exception Handling.

[23] „Application Security Inc.: Database Security, A Key Component of Application Security“, (2006.) http://hosteddocs.ittoolbox.com/Database_Security.pdf.

prilagođeni DES (eng. Data Encription Standard) algoritam za enkripciju zaporki prije slanja. Za enkripciju cjelokupnog mrežnog prometa prema SSL protokolu potrebno je instalirati Oracle Advance Security paket. Inačice namijenjene Windows operacijskim sustavima podržavaju enkripciju na razini datoteka korištenjem EFS (eng. Encripting File System) datotečnog sustava. Enkripcija na razini programskog sučelja je omogućena "DBMS_OBFUSCATION_TOOLKIT" alatom.

U svrhu podizanja računalne sigurnosti, korisnicima se savjetuje pronalaženje i promjena svih izvorno postavljenih korisničkih zaporki kao što su: "SYS", "SYSTEM" ili "APPS". Oracle omogućuje kontrolu složenosti korisničkih zaporki, njihovog roka trajanja i ponovnog korištenja.
Također, Oracle posjeduje nekoliko metoda autorizacije korisnika:

1. Kerberos security – implementira Kerberos protokol za sigurno uzajamno dokazivanje identiteta korisnika tijekom komunikacije koja se temelji na enkripciji simetričnim ključem i zahtjeva sigurnu treću stranu (eng. Trusted Third Party, TTP),
2. VPD (eng. Virtual Private Databases) – tehnologija koja omogućava ograničenje pristupa pojedinim zapisima u tablici,
3. Role-based security – omogućuje grupiranje ovlasti u uloge koje je potom moguće pridijeliti pojedinim korisnicima,
4. Grant-execute security – omogućuje ograničavanje mogućnosti procedura ovisno o ovlastima korisnika koji ih pokreće,
5. Authentication servers – poslužitelji za sigurnu identifikaciju vanjskih korisnika,
6. Port access security – Listener poslužitelj može se postaviti tako da ograniči pristup pojedinim portovima.

Nadzor nad Oracle bazom podataka obavlja se stvaranjem "AUDIT TRAIL VIEWS" zapisa pomoću "CATAUDIT.SQL" skripte. Podatke prikupljene nadzorom moguće je pohranjivati za svaku sjednicu ili za svaki uočen pokušaj pristupa. Za vremenski ograničen nadzor koristi se "DBMS_JOB" mogućnost, koja uz "TRIGGERS" mogućnost može poslužiti i za postavljanje zamki uljezima. Korisnicima se pokazalo

korisnim nadziranje već spomenute "SYS.LINK$" tablice te tablice "SYS.AUD$" u koju se spremaju podaci prikupljeni nadzorom.[24]

4.2. PostgreSQL

4.2.1 Sigurosni mehanizmi

PostgreSQL ima izgrađen RBAC[25] sustav za upravljanje pristupom koji upravlja samom bazom ali i proizvodima same baze.

1. Useri

PostgreSQL user je uloga koju ima CONNECT privilegiju za sve povezane.

2. Grupe

Grupa je uloga koju ima i druge uloge kao dio sustava. Članovi grupa imaju samostalne i određene privilegije i mogućnosti.

3. Uloge

Uloga je konstrukt baza podataka koji sadrži popis određenih sigurnosnih povlastica i primjenjuje ih na temelju povlastica i na temelju konstrukata (koji se sastoje od):

Instance, baze podataka, sheme, tablica, slijeda, pregleda i procedura

Uloge su dostupne na razini dodijeljenih prava, što ih čini prenosivima na svim bazama podataka u instancama baze, a može imati atribute koji su dodijeljeni na bilo koji pod-objekt unutar baza podataka.

Uloge mogu imate određene parametre na strani servera koje se moraju provoditi pri prijavi, a mogu se koristiti za promjenu sve, od vrste planova upita koji se mogu izvršiti, do memorijskih parametara dostupnih korisniku.

[24] Scott Mead, „OpenSCG PostgreSQL Operational Procedures“, http://www.openscg.com/wp-content/uploads/2013/04/SecurityHardeningPostgreSQL.pdf
[25] role-based access control.

Autentikacija

PostgreSQL pruža više načina autentikacije uz svoj vlastiti unutarnji sustav logina lozinkama.

1. Autentikacija lozinkom

Standardna metoda za provjeru autentičnosti na PostgreSQL bazu podataka je interni sustav za provjeru autentičnosti na temelju lozinke. Ovaj sustav pohranjuje samo opis lozinke u bazi podataka i potvrđuje da je opis jednak ključu unutar sustava.

U ovom sustavu, userima i lozinkama upravlja administrator baze podataka u bazi Postgres.

2. LDAP[26] Autentikacija

LDAP autentikacija je dostupna u PostgreSQL, dok LDAP autorizacija nije. Naime, LDAP se može koristiti za upravljanje lozinke i politike lozinka, kao i uskraćivanje pristupa prijave. LDAP se ne može koristiti za kontrolu pristupa određenim bazama podataka na razini predmeta, međutim to se postiže pomoću ugrađenog PostgreSQL RBAC sustava. Da bi LDAP korisnici imali pristup Postgres-u korisnik mora imati ulogu instaliranu na isti login atributa (obično uid = ili CN =) koji LDAP koristi. U ovom scenariju, RDBMS[27] bi pozivao na LDAP sustav za provjeru autentičnosti.

3. Kerberos provjera autentičnosti

Kerberos provjera autentičnosti je dostupna u PostgreSQL, a kao i sa LDAP, autorizacija nije. To znači da imena uloga koji se koriste u Kerberos infrastrukture moraju također postojati u bazi podataka Postgres. a RDBMS će pozvati na ticketing[28] sustava za utvrđivanje autentičnosti.

[26] Lightweight Directory Access Protocol – protokol za spajanje preko vanjskih IP adresa servera.

[27] Relational database management system – sustav za upravljanje baza koji koristi relacioni model.

[28] Mali privremeni ključ unutar autentikacijskog file-a.

Za strogo zatvorene mreže i mali broja uloga, koriste se interne provjere autentičnosti. Kada se koriste vanjski sustavi, puno je bolje koristiti vanjske sustave autentikacije zbog uzdržavanja baze i aktivnosti korisnika. Za manje stroge sustave, koristiti se vanjska provjera autentičnosti. Kada je potrebna analiza podataka strogo zatvorenih sustava, zahtijeva se veliki broj korisničkih prijava

Operativni sustav

PostgreSQL ima sigurnosne zahtjeve kada se izvodi na operativnom sustavu. Ne mogu se pokrenuti kao korisnici već moraju imati račune koji posjeduju sve pokrenute procese baze podataka. Ovaj račun mora imati potpuni pristup direktoriju i podacima na disku, ali direktorij mora biti zaključan da dopušta samo pristup Postgres korisnika na serveru . Drugim riječima, podaci i direktorij vidjeti će samo super-user računala i user Postgres. Nema mogućnosti pristupa na temelju grupe za datotečni sustav. Ako dozvole nisu postavljene na ovaj način, baza podataka će odbiti pristup.

Treba dopustiti samo potrebnom osoblju da imaju prava logina. Pružanje usluga 'Postgres' sustava samo onima koji trebaju pristup za kontrolu Postgres procesa na sustavu, a tek nakon što su ovjereni sa svojim računom.

Ograničiti broj portova za pristup bazi podataka: Port baze, portovi za upravljanje, a ostale portove treba zatvoriti za uporabu.

4.3. Izbor baze podataka

Uvijek postoji neka vrsta sukoba koji alati su najbolji za baze podataka. Svaki administrator ima svoje preferencije, a svaki programer ima svoj jedinstven način rješavanja koda.

Oracle ima prednosti i mane u sljedećem:

- Closed-source.[29] Besplatna verzija je vrlo limitirana.
- Privremene tablice ostaju aktivne i nakon rada i mora ih korisnik zatvarati osobno.
- Podržava četiri vrste charactera/stringova: CHAR, VARCHAR2, NCHAR, NVARCHAR2
- Tablice i redovi podržavaju zaključavanje
- Ekstenzivno i fleksibilno podešavanje spremanja baza i upravljanjem prostora uključući tablespace, synonym i razni drugi paketi
- Složeni i široki spektar backup tehnologija
- Dizajniran da podržava velike i složene baze

PostgreSQL je:

- Open-source
- Podržava sve trenutačne SQL standarde i lakše se uči
- Težina i veličina aplikacija često nije učinkovita sa programima gdje ima puno čitanja podataka
- Napredne opcije za poslovne sustave i lokacijsku analitiku
- Široki spektar podrške za razne programske podjezike
- Podržava ACID[30]

[29] Software zatvorenog koda. Licenca se treba kupiti i korisnici nemaju uvid u temelje programa.

- Temelji se na principu lakog integriranja podataka i stabilnosti.

- Potpuna podrška pregleda tablica i zapisa, podrška raznih jezika na strani servera

- Potpuna podrška SQL procedura kao što su „table expressions“ i „windows functions“

- Mogućnost spajanja velikog broja tablica

- Teža replikacija i slabija podrška za replikaciju

Koju bazu koristiti?

U slučaju da je potrebna fleksibilnost transakcija i jaka kontrola, želimo velike i stabilne baze podataka, počinjemo sa manjim ali možemo nadograditi prema većem i većem sustavu ili želimo podršku za sve operativne sustave i platforme preporuča se korištenje Oracle baza.

U slučaju da je potrebno programiranje kompleksnih procedura, treba nam podrška Java sustava. Ako je potrebna baza podataka koja se sastoji od velikih kompleksnih funkcija sa visokim ponavljanjem, ili se koristi velika količina pisanja a brzina čitanja nije važna i vaše baze su fokusirane na development, PostgreSQL je tada najbolja opcija.[31]

[30] Atomicity, Consistency, Isolation, Durability. Standard za transakcije unutar baza podataka smišljen u 1970-ima od strane znanstvenika Jim Gray-a.

[31] Chitij Chauhan , *PostgreSQL Cookbook*, (2015.), 31-43.

ZAKLJUČAK

Unutar svih sustava, neovisno o kompleksnosti, temelji rada sa bazama podataka i programskim sustavima počivaju na sigurnosti i kontroli client-server arhitekture. Sigurnost kao grana informatike svakim danom je sve složenija i prestižnija pozicija unutar informatičkih sustava, počevši od zaštite protiv virusa, napada, neovlaštenih ulaza, pregledavanja informacija, pa čak i email i web firewallova, danas ne postoji poslovna jedinica bez barem neke vrste zaštite.

Unutar takvih sustava baze podataka čine veliki dio funkcija kojima se bave korisnici i velika se važnost daje administriranju i kontroliranju baza. Sigurnost baza je još jedna, zasebna grana unutar sigurnosti sustava koja se temelji na upravljanjem dozvola, lokacija, datoteka, tablica i pravima korištenja same baze podataka.

U današnje doba Oracle nudi bolju, stabilniju zaštitu i podršku od konkurencije, pogotovo u velikim sustavima, ali rast kompleksnosti enkripcija i podrške za open source programe kao PostreSQL daju raznolike mogućnosti pri odabiru baza podataka.

Da bi se postigla potrebna razina zaštite podataka potrebna je edukacija ne samo administratora sustava već i korisnike unutar mreže.

Zbog važnosti informacija kojima raspolažu kompanije, banke, korporacije ali i kućna računala, u današnje doba razvoj tehnologija zaštite će rasti ubrzanom stopom i informacije same biti će najvrjednija valuta.

LITERATURA

Knjige:

1. Mario Radovan; *Računalne mreže (1): Povezivanje računala i mreža*, Digital point tisak, Rijeka, 2010.
2. J.M. Kizza, *Guide to Computer Network Security (Computer Communications and Networks)*, Springer-Verlag, London, 2015.
3. Chitij Chauhan, *PostgreSQL Cookbook*, Packt Publishing, London, 2015.
4. Douglas K., Douglas S., *PostgreSQL: The comprehensive guide to building, programming, and administering PostgreSQL databases*, Packt Publishing, London, 2005.
5. John Watson, *OCA Oracle Database 11g Administration I Exam Guide*, McGraw-Hill Education, New York , 2008.
6. Tamer Özsu and Patrice Valduriez, *Principles of distributed database systems*, New Jersey, 1999.

Članci na webu:

1. Milan Korać; Dario Car, „Uvod u računalne mreže“, Zagreb, 2014. http://umag.hr/sadrzaj/dokumenti/NATJECAJ_informaticki_referent_Uvod_u_racunalne_mreze_Visoko_uciliste_Algebra.pdf
2. „Sigurnost sustava za upravljanje bazama podataka CCERT-PUBDOC-2006-10-171“,

   http://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2006-11-171.pdf
3. S. Brian Suddeth, „Database – The Final Firewall“, SANS Institute2, 2002. https://www.sans.org/reading-room/whitepapers/application/database-the-final-firewall-11

Web materijali:

1. Bažant, A. (et. al.), „Osnovne arhitekture mreža“, Element, Zagreb, 2004. http://www.etfos.unios.hr/~drago/predmeti/mip/MiP1.pdf
2. Amit Singh, „An Introduction to Virtualization“, 2009.

   https://webdocs.cs.ualberta.ca/~sr16/Virtualization/An%20Introduction%20to%20Virtualization.pdf
3. Scott Granneman, „Virtualization For Security“, *Theregister.co.uk*. N.p., 12 Sept. 2016. http://www.theregister.co.uk/2006/04/13/virtual_security/
4. „Oracle server Concepts Manual“

   http://docs.oracle.com/cd/A57673_01/DOC/server/doc/SCN73/ch20.htm#o client/server
5. http://www.pfri.uniri.hr/~tudor/materijali/Informacijski%20sustavi,%20baze%20podataka.htm

POPIS SLIKA

SAŽETAK

U doba širenja informacijske i komunikacijske tehnologije sigurnost je jedan od najvažnijih faktora poslovnog i privatnog svijeta. Ova tema se bavi svim faktorima za uspješno i sigurno poslovno okruženje, ističe razliku između sigurne zatvorene mreže i nesigurne mreže van sustava. Rad se temelji na opisu i razumijevanju svih faktora koji čine mrežu i pokazuje ulogu baza podataka unutar nje. Dotiče se i strukture, arhitekture i odnosa između clienta i servera, povezuje glavne vrste servera sa njihovim ulogama unutar sustava. Navodi se i važnost virtualizacije kao najjačeg alata za udaljeni rad, ali i podršku prema svim korisnicima, koja omogućuje domensku mrežu unutar kućne ili čak druge domenske mreže. U zadnjem dijelu rada i njegovom zaključku imamo pregled korištenja baza kao Oracle ili PostgreSQL i njihovu usporedbu iz prakse, gdje se objašnjavaju i uspoređuju prednosti i mane oba sustava.

Ključne riječi: Sigurnost, Oracle, PostgreSQL, mrežna arhitektura

At the time of the spread of information and communication technology security is one of the most important factors affecting the business and the private world . This thesis deals with all the factors for a successful and safe business environment, stresses the difference between a secure closed network and secure network outside the system. The paper is based on the description and understanding of all the factors that make up the network and shows the role of databases within it . It addresses the structure, architecture and the relationship between client and server, connects the main types of servers with their roles within the system. It also states the importance of virtualization as the most powerful tool for remote work and support for all users, which allows domain networking at home or even other domain networks. In the last part of the thesis we review the use of databases such as Oracle or PostgreSQL and their comparison from the field, in which are explained and compared the advantages and disadvantages of both systems.

Key words: Securty, Oracle, PostgreSQL, network architecture