Sigurnosni mehanizmi za zaštitu baza podataka

Majnarić, Petra

SVEUČILIŠTE U ZAGREBU
FILOZOFSKI FAKULTET
ODSJEK ZA INFORMACIJSKE I KOMUNIKACIJSKE ZNANOSTI
Ak. god. 2018./2019.

Petra Majnarić

Sigurnosni mehanizmi za zaštitu baza podataka

Završni rad

Mentor: doc. dr. sc. Vedran Juričić

Zagreb, rujan 2019.

Izjava o akademskoj čestitosti

Izjavljujem i svojim potpisom potvrđujem da je ovaj rad rezultat mog vlastitog rada koji se temelji na istraživanjima te objavljenoj i citiranoj literaturi. Izjavljujem da nijedan dio rada nije napisan na nedozvoljen način, odnosno da je prepisan iz necitiranog rada, te da nijedan dio rada ne krši bilo čija autorska prava. Također izjavljujem da nijedan dio rada nije korišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

_____

(potpis)

Sadržaj

1. Uvod

Suvremeni način života i poslovanje nezamislivi su bez uporabe informacijske tehnologije. Sve prisutna dostupnost interneta nije više samo zabava i čitanje vijesti, već potreba za sigurnim i brzim pristupom raznim uslugama i informacijama kao što su prijava ispita, plaćanje računa, kupovina, narudžba za medicinske usluge i sl. iz bilo kojeg dijela svijeta i u bilo koje doba dana. Na taj način fleksibilnije se koriste resursi, skraćuje vrijeme čekanja i izvršenja za određenom informacijom ili uslugom. Potreba za raspolaganjem i posjedovanjem određenih podataka neophodna je u svim sferama poslovanja, a količina novih podataka svaki dan raste.

Sve su veći zahtjevi i potražnja za brojnim informacijama rezultirali stvaranjem niza baza podataka kojima se obično intranetom ili internetom pristupa putem sustava za upravljanje bazom podataka (DBMS). Sustav za upravljanje bazama podataka se sastoji od integriranog skupa računalnog softvera koji omogućuje korisnicima interakciju s jednom ili više baza podatka te pruža različite funkcije kao što su unos, pohranjivanje i dohvaćanje podataka.

Većina podataka od kritične su važnosti, poput znanstvenih, zdravstvenih ili vojnih, su organizirana u neku vrste baze podataka te njihova sigurnost i zaštita predstavlja sve kompleksniji problem (Centar informacijske sigurnosti, 2012). Bez uporabe informacijske tehnologije i interneta danas je nezamisliv bilo koji poslovni proces i poslovanje u svim organizacijama, poslovnim subjektima, tijelima državne i javne uprave. Stoga je potrebno naročito obratiti pozornost računalnoj sigurnosti i računalnim sigurnosnim mehanizmima te zaštiti podataka od samog projektiranja informacijskog sustava, odabira računalne i mrežne arhitekture do programiranja.

Najčešće pojava zlouporabe i krađe podataka su neovlaštene aktivnosti ili zlouporaba od strane ovlaštenih korisnika baze podataka, administratora baze podataka, neovlaštenih korisnika ili hakera, infekcije zlonamjernog softvera koje uzrokuju incidente kao što su neovlašteni pristup ili otkrivanje osobnih podataka, brisanje ili oštećenje podataka ili programa, prekid ili uskraćivanje ovlaštenog pristupa bazi podataka te malware koji bez znanja korisnika postaje izravan kanal za pristup osjetljivim podacima. Primjena sigurnosnih mehanizama je sigurnosnom politikom postupcima smanjiti navedene aktivnosti te održati sigurnost podataka.

2. Baze podataka

Baze podataka su skup međusobno povezanih podataka i informacija koje su organizirane u vanjskoj memoriji računala. Njima se može lako pristupiti, upravljati i ažurirati te su istovremeno dostupni raznim korisnicima i aplikacijskim programima (Manger, 2014).

Podaci su najčešće organizirani u retke, stupce i tablice te su indeksirani kako bi se olakšalo pronalaženje relevantnih informacija. Podržavaju radnje (aktivnosti) kao što su umetanje, brisanje, ažuriranje, mijenjanje, kontrola i čitanje podataka koji se obavljaju pomoću posebnog softvera, takozvanog sustava za upravljanje bazom podataka (Data Base Management System – DBMS). On je zadužen za održavanje, sigurnost, upravljanje i obradu podataka pohranjenih u bazama podataka.

Sustav za upravljanje bazom podataka (DBMS) je poslužitelj (server) baze podataka te on oblikuje fizički prikaz baze podataka s traženom logičkom strukturom. Također, on u ime klijenta obavlja sve operacije s podacima i prihvaća zahtjev za podacima iz aplikacije i upućuje operativni sustav da dostavi određene podatke (Manger, 2014).

Također, on je u stanju podržati razne baze, od kojih svaka može imati svoju logičku strukturu. DBMS također olakšava dodatne administrativne operacije kao što su upravljanje promjenama, oporavak od pada, praćenje usklađenosti i učinkovitosti te još puno toga (Manger, 2014).

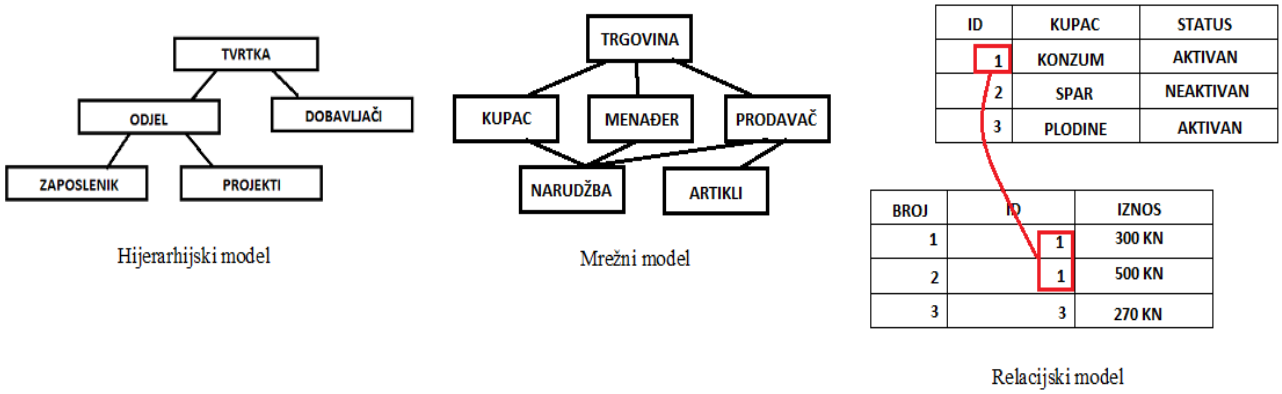
2.1. Modeli podataka

Model baze podataka definira logički dizajn i strukturu baze podataka i definira kako će se podaci pohranjivati, pristupati i ažurirati u sustavu za upravljanje bazom podataka te kako su podaci međusobno povezani i kako se obrađuju i pohranjuju unutar sustava.

Baze podataka mogu se organizirati na različite načine. Tri su najčešća i najrasprostranjenija modela baza podataka: hijerarhijski model podataka, mrežni model podataka i relacijski model podataka. Oni su se razvijali usporedno s rastom znanja korisnika i programera o uporabi sustava za upravljanje bazom podataka. Razlikuju se međusobno u troškovima primjene, brzini pristupa podacima, stupnju redundancije podataka, načinima zadovoljenja potreba korisnika za informacijama i sl. (Vujnović, 1995).

Dosadašnji DBMS-ovi obično su podržavali neki od ovih modela:

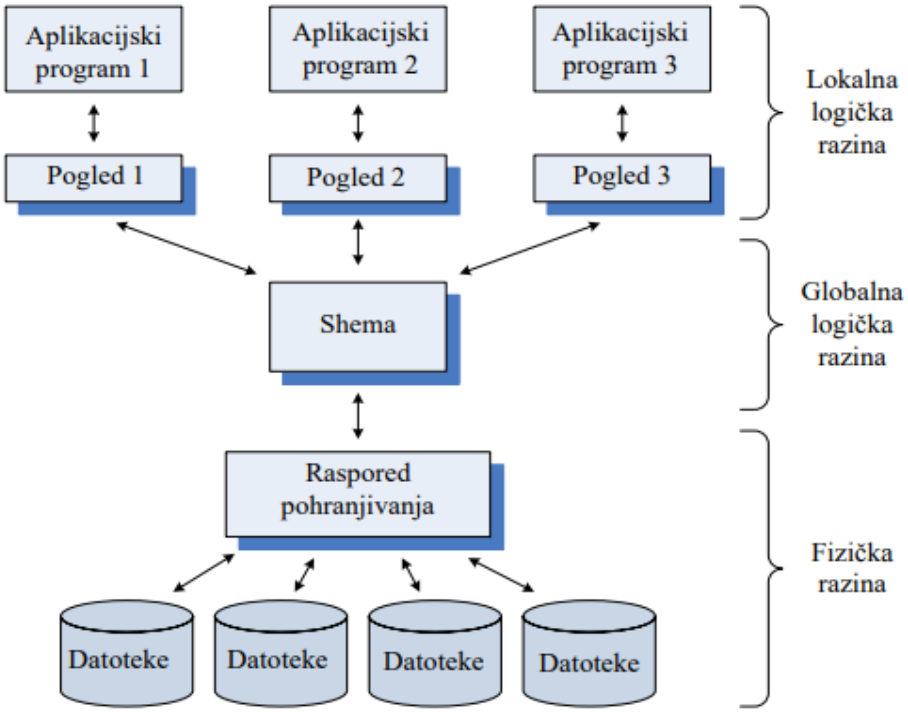
- Hijerarhijski model - baza je predočena jednim stablom (hijerarhijom) ili skupom stabala. Svako stablo sastoji se od čvorova i veza „nadređeni-podređeni“ između čvorova. Čvorovi su tipovi zapisa, a odnos „nadređeni-podređeni" izražava hijerarhijske veze među tipovima zapisa (Manger, 2010; Vujnović, 1995).
- Mrežni model – proširenje hijerarhijskog modela gdje je baza predočena mrežom koja se sastoji od čvorova i usmjerenih lukova. Na temelju teorije matematičkih skupova, model je konstruiran s nizom povezanih zapisa od kojih čvorovi predstavljaju tipove zapisa (slogova podataka), a lukovi definiraju veze među tipovima zapisa (Manger, 2010).
- Relacijski model - zasnovan je na matematičkom pojmu relacije. Bavi se s tri aspekta podataka: definicijom, integritetom i manipulacijom. On organizira podatke u tablice od kojih se svaki sastoji od stupaca i redaka. Svaki stupac navodi atribut dotičnog entiteta te zajedno, atributi u odnosu nazivaju se domenom (Vujnović, 1995). Određeni atribut ili kombinacija atributa odabrana je kao primarni ključ koji se može navesti u drugim tablicama, kada se naziva stranim ključem.



Slika 1. Primjeri modela podataka

2.2. Arhitektura baze podataka

Arhitektura baze podataka sastoji se od tri sloja, kao što je vidljivo na slici 2., i sučelja među slojevima prema ANSI/SPARC[1] Study Group (Darbar Kishansing G. i Suthar Sagar M., 2014) koja je autor standarda i naziva ANSI/SPARC arhitekturom.



Slika 2. Arhitektura baze podataka (Izvor: Manger, 2010)

- Fizička razina odnosi se na unutarnju shemu koja opisuje strukturu fizičke pohrane baze podataka, te je poznata i kao fizička shema. Ona koristi fizički model podataka te definira načina pohranjivanja podataka u blokove. Koristi za detaljno opisivanje složenih podatkovnih struktura na najnižoj razini (Vujnović, 1995).
- Globalna logička razina odnosi se na logičku strukturu cijele baze. Pomoću konceptualne sheme opisuje se dizajn baze podataka na konceptualnoj razini. Konceptualna shema opisuje strukturu cijele baze podataka, podatke koje treba pohraniti u bazu podataka te opisuje odnos između tih podataka. Na ovoj razini

[1] [1] *ANSI/SPARC – American National Standards Institute, Standards Planning And Requirements Committee*

unutarnji detalji strukture podataka su skriveni (Vujnović, 1995). Programeri i administratori baza podataka rade na ovoj razini.

- Lokalna logička razina odnosi se na logičku predodžbu o dijelu baze koji rabi pojedina aplikacija (Manger, 2014). Na ovoj razini, baza podataka sadrži nekoliko shema koje se ponekad nazivaju i podshema. Podshema se koristi za opisivanje različitog pogleda na bazu podataka poznatu kao view shema. Svaka shema pogleda prikazuje dio baze podataka koja je namijenjena određenoj grupi korisnika od koje skriva preostale podatke u bazi. Shema pogleda opisuje interakciju krajnjeg korisnika sa sustavima baza podataka (Vujnović, 1995).

3. Vrste sigurnosti

Sigurnost baze podataka odnosi se na korištenje sigurnosnih mehanizama za zaštitu podataka i baza podataka, uključujući sljedeće:

1. Razna pravna i etička pitanja koja se odnose na pravo pristupa određenim informacijama i zaštita podataka od neovlaštenog pristupa tako što im ne mogu legalno pristupiti neovlaštene organizacije ili osobe (Elmasri i Navathe, 2015). Diljem svijeta postoje brojni zakoni koji reguliraju privatnost informacija.
2. Politička pitanja na vladinoj, institucionalnoj ili korporativnoj razini o tome koje vrste informacija ne bi trebale biti dostupne javnosti (Elmasri i Navathe, 2015), ovo se na primjer odnosi na osobnu medicinsku dokumentaciju ili podatke o kreditnim karticama.
3. Pitanja vezana uz sustav kao što su razine sustava na kojima bi se trebale provoditi različite sigurnosne funkcije, na primjer da li bi se sigurnosna funkcija trebala rješavati na fizičkoj razini hardvera, razini operacijskog sustava ili razini DBMS-a (Elmasri i Navathe, 2015).
4. Potreba u nekim organizacijama da identificiraju višestruke razine sigurnosti i da na temelju tih podataka klasificiraju podatke i korisnike na temelju tih klasifikacija, (Elmasri i Navathe, 2015) ovo se odnosi na stroge tajne, tajne, povjerljive i neklasificirane. Sigurnosna politika je organizacija s obzirom na dopuštanje pristupa različitim klasifikacijama podataka koji se moraju provoditi.
5. Potreba u nekim organizacijama da definiraju višestruke razine sigurnosti i da klasificiraju podatke (tajne i povjerljive) i korisnike na temelju klasifikacija tih sigurnosnih razina. Sigurnosna politika je važna pri takvim regulacijama te ona upravlja pristupom različitim klasifikacijama podataka koji se moraju provoditi (Elmasri i Navathe, 2015)

U sustavima baze podataka, ACID (Atomicity, Consistency, Isolation, Durability) se odnosi na standardni skup svojstava koji garantiraju pouzdane i sigurne transakcije baze podataka. ACID se posebno bavi načinom na koji se baza podataka oporavlja od bilo kakvog neuspjeha koji se može dogoditi tijekom obrade transakcije. DBMS koji je usklađen s ACID-om osigurava da podaci u bazi podataka ostanu točni i dosljedni unatoč mogućim kvarovima i prekidima (Ian, n.d.).

Atomarnost znači da će sve transakcije biti uspješno izvršene ili neće niti jedna, drugim riječima, ako jedan dio transakcije ne funkcionira kako bi trebalo, drugi neće uspjeti kao rezultat - i obrnuto. Ukratko, atomičnošću dobivamo "sve ili ništa" (Ian, n.d.).

Konzistentost znači da bi bilo koja baza podataka trebala raditi onako kako je namijenjena, mora slijediti odgovarajuća pravila za provjeru valjanosti podataka. Prema tome, dosljednost znači da se u bazu podataka mogu pisati samo podaci koji slijede ta pravila. Time se uključuju i sva ograničenja i okidače koji su primijenjeni na bazu podataka (Ian, n.d.)

Izolacija se odnosi na sposobnost istodobnog obrade višestrukih transakcija na način koji ne utječe na drugi. Tijekom istodobnog izvršenja transakcija, međusobni rezultati međufaznih transakcija ne bi trebali biti dostupni jedan drugome (Ian, n.d.).

Trajnost znači da će, nakon što je transakcija izvršena, ostati u sustavu čak i ako dođe do pada sustava odmah nakon transakcije. Sve promjene iz transakcije moraju se trajno pohraniti (Ian, n.d.). Cilj trajnosti je učiniti one kvarove nevidljivima krajnjem korisniku.

Zaključak je da DBMS-ovi sukladni s ACID-om osiguravaju organizacijama zaštitu da će njihova baza podataka održati integritet podataka, čak i ako se neka vrsta neuspjeha dogodi dok su transakcije u središtu obrade.

Osnovne funkcije koje moraju biti ugrađene u svaki sustav za upravljanje bazom podataka:

- Integritet i zaštita podataka – DBMS mora čuvati integritet podataka i njihovo ponašanje prema točno definiranim pravilima, a zahtjeve korisnika koji narušavaju integritet podataka DBMS mora prepoznati i odbaciti.
- Manipulacija podacima – DBMS mora imati mogućnost obrade odnosno manipuliranja podataka prema zahtjevima korisnika. Ti zahtjevi mogu biti dodavanje novih podataka, brisanje ili promjena vrijednosti postojećih itd.
- Definicija podataka – DMBS mora biti u stanju definicije podataka izrečene u nekom jeziku za definiciju podataka pretvoriti u oblik interne pohrane podataka
- Oporavak u slučaju pogreške – dođe li do oštećenja baze ili do greški koje bi mogle uzrokovati njeno nekonzistentno stanje, sustav mora omogućiti njezin oporavak, dakle povratak u blisko konzistentno stanje dođe li do zloupotrebe , sustav ima mogućnost
- Efikasnost – sve nabrojene funkcije DBMS mora osigurati uz što bolje performanse (Ian, n.d.).

4. Sigurnost u Republici Hrvatskoj

Područja informacijske sigurnosti za koja se propisuju mjere i standardi informacijske sigurnosti su:

- sigurnosna provjera
- fizička sigurnost
- sigurnost podatka
- sigurnost informacijskog sustava
- sigurnost poslovne suradnje (Narodne novine, 2007).

Sigurnosna politika je dio sustava upravljanja sigurnošću informacijskih sustava modeliranjem sigurnosnog okruženja te se odnosi na stanje povjerljivosti, cjelovitosti i raspoloživosti podataka i primjenom propisanih mjera i standarda informacijske sigurnosti.. Tehnološke tajne mogu biti predmet interesa raznih pojedinaca, organizacija ali i pojedinih država.

„Razvojem tehnologije sve se više podataka važnih za nacionalnu sigurnost pohranjuje u informacijskim sustavima tijela državne uprave ili se razmjenjuju informacijsko-komunikacijskim kanalima. SOA[2] je zadužena za otkrivanje i sprječavanje neovlaštenog ulaska u zaštićene informacijske i komunikacijske sustave državnih tijela te odavanje klasificiranih podataka.“ (Sigurnosno–obavještajna agencija, n.d.)

Zadaća institucija je da u skladu sa Zakonom o informacijskoj sigurnosti RH provode mjere zaštita i prevencija od računalnih ugroza, sigurnosti javnih informacijskih sustava u Republici Hrvatskoj, osobito incidenata na internetu.

Institucije i tijela koje na nacionalnoj razini vode brigu o informacijskoj sigurnosti:

- Nacionalni CERT
- Zavod za sigurnost informacijskih sustava (ZSIS)
- Carnet CERT (C-CERT)
- Ured Vijeća za nacionalnu sigurnost (UVNS)
- Sigurnosno obavještajna agencija (SOA)
- Vojno sigurnosno obavještajna agencija (VSOA).

„Ovo područje ima izražen međuresorni karakter te u provedbi mjera, postupaka i standarda informacijske sigurnosti SOA surađuje s tijelima javne vlasti, državnim institucijama te drugim

[2] *SOA - Sigurnosno obavještajna agencija*

institucijama i ustanovama. Posebno je ta suradnja intenzivna s Vladom RH, UVNS-om, ZSIS-om, MUP-om, VSOA-om, Ministarstvom pravosuđa, DORH-om i MVEP-om.“ (Sigurnosno–obavještajna agencija, n.d.)

Zavod za sigurnost informacijskih sustava je središnje državno tijelo za obavljanje poslova u tehničkim područjima informacijske sigurnosti državnih tijela Republike Hrvatske. Oni obuhvaćaju standarde sigurnosti informacijskih sustava, sigurnosne akreditacije informacijskih sustava, upravljanje kriptomaterijalima koji se koriste u razmjeni klasificiranih podataka te koordinaciju prevencije i odgovora na računalne ugroze sigurnosti informacijske sigurnosti.

Započeli su sa svojim radom 2006. godine te su im zadaće utvrđene Zakonom o sigurnosno-obavještajnom sustavu Republike Hrvatske, Zakonom o informacijskoj sigurnosti te Uredbom Vlade Republike Hrvatske o mjerama informacijske sigurnosti. Uloga Zavoda za sigurnost informacijskih sustava je reguliranje standarda tehničkih područja sigurnosti informacijskih sustava pravilnicima, provoditi sigurnosne akreditacije informacijskih sustava u kojima se koriste klasificirani podaci te odgovor sigurnosne računalne prijetnje (Zavod za sigurnost informacijskih sustava, n.n).

Nacionalni CERT je nacionalno tijelo za prevenciju i zaštitu od računalnih ugroza sigurnost javnih informacijskih sustava u Republici Hrvatskoj te je osnovan 30. listopada 2007. godine u skladu sa Zakonom o informacijskoj sigurnosti Republike Hrvatske. Jedna od glavnim zadaća Nacionalnog CERT-a je provođenje postupaka i mjera kojima se nastoji očuvati sigurnost informacijskih sustava te sprečavanje i obrada računalnih incidenata na javnim informacijskim sustavima nastalih u Republici Hrvatskoj. Obradu incidenata podrazumijeva forenzička analiza, analiza zlonamjernog softvera, mrežnog prometa i logova. Nacionalni CERT je zadužen za prevenciju i zaštitu incidenata za sektore ključnih usluga kao što su bankarstvo, infrastrukture financijskog tržišta, digitalna infrastruktura, poslovne usluge za državna tijela (Središnji državni portal, 2019).

Ured Vijeća za nacionalnu sigurnost središnje je državno tijelo za informacijsku sigurnost koje je zaduženo za donošenje i nadziranje primjene mjera i standarda informacijske sigurnosti. UVNS radi sigurnosne provjere, održava sigurnost podataka i informacijskih sustava te utvrđuje mjere nakon provedenih nadzora nad agencijama sigurnosno-obavještajnog sustava te odobrava međunarodnu suradnju na području nacionalne sigurnosti. VNS čine Predsjednica RH, predsjednik Vlade RH, ministri obrane, unutarnjih poslova, vanjskih poslova i pravosuđa, savjetnik Predsjednice RH za nacionalnu sigurnost, načelnik Glavnog stožera GS OS RH,

predstojnik UVNS-a, ravnatelji SOA-e i VSOA-e te u radu sudjeluje predsjednik Hrvatskog sabora, a po potrebi i druge osobe (Ured vijeća za nacionalnu sigurnost, n.n).

5. Sigurnosni rizici u bazama podataka

Kako bismo mogli brzo i učinkovito upravljati velikom količinom podataka, potreban je dobro organiziran i zaštićen sustav. Sigurnost baze podataka počinje od fizičke sigurnosti sustava nakon čega se baza podataka mora se zaštititi od neovlaštenog pristupa od strane ovlaštenih korisnika kao i od neovlaštenih korisnika. Postoje mnoge unutarnje i vanjske prijetnje sustavima baza podataka, kao što je neispravna konfiguracija sustava za upravljanje bazom podataka, programskih propusta ili sigurnosnih nedostataka unutar aplikacija povezanih s njima. Neke od prijetnji i rizika koji mogu proizaći iz navedenog su:

Prekomjerne povlastice. Kada su zaposlenicima dodijeljene pretpostavljanje povlastice baze podataka koje prekoračuju zahtjeve njihovih radnih funkcija, te se povlastice mogu zloupotrijebiti (Maurer, 2015) tako da se koriste za pristup povjerljivim informacijama. Rješenje ovog problema je kontrola pristupa na razini upita. Kontrola pristupa na razini upita (engl. *query*) ograničava povlastice na operacije i podatke koji su minimalno potrebni. Većina izvornih platformi za sigurnost baza podataka nudi neke od ovih mogućnosti (okidači, RLS - *Row Level Security*, ACL - *Access Control List* itd.), ali ih ručni dizajn tih alata čini nepraktičnim u svim osim u najmanjim postavkama.

SQL injektiranje. Dva glavna tipa napada na baza podataka su SQL injekcije koje ciljaju tradicionalne sustave baza podataka i NoSQL injekcije koje ciljaju na platforme "velikih podataka" (Maurer, 2015). SQL injekcijski napadi uključuju korisnika koji koristi prednosti ranjivosti u web-aplikacijama i pohranjenim procedurama za slanje neovlaštenih upita baze podataka, često s povišenim ovlastima.

Upotrebom SQL injekcije, napadači su mogli dobiti neograničen pristup cijeloj bazi podataka. Bilo koja procedura koja konstruira SQL izraze trebala bi biti pregledana za injekcijske ranjivosti jer će SQL poslužitelj izvršiti sve sintaktički valjane upite koje primi (Shribastava et al., 2012).

Uskraćivanje usluge. Uskraćivanje usluge (DoS) može se pozvati kroz mnoge tehnike. Uobičajene DoS tehnike uključuju preljeve međuspremnika, korupciju podataka, mrežne „poplave“ i potrošnju resursa. DoS preventiva bi se trebala pojaviti na više slojeva, uključujući mrežu, programe i baze podataka (Shribastava et al., 2012).

Napadačima je namjera kod ovakvih napada da se sruši baza podataka te da se onemogući rad i korištenje. Obično se to događa kada naredba "zbunjuje" bazu podataka, analizator upita ili podfunkciju dovoljno da se ona sruši. S obzirom da su baze podataka sastavljane od međusobno

ovisnih procesa, tako gubitak jedne usluge može uzrokovati obustavom resursa cijele baza podataka (Shribastava et al., 2012).

Malware. *Malware* je softver koji je kreiran s namjerom da nanese štetu računalu, serveru, klijentu ili mreži. Napredni ciljani napadi koriste više taktika i alata, no većinom napadi obično slijede poznati uzorak:

- Napadači započinju operaciju pretraživanjem i prikupljanjem informacija o organizaciji koju žele napasti
- *Malware* se isporučuje tim osobama kao način za pristup mreži tvrtke
- Napadači zatim pregledavaju podatke o poduzeću kako bi pronašli željene informacije
- Prije odlaska napadač može stvoriti put za povratak koji im omogućuje povratak u slučaju budućih napada (Anonymus, 2013)

6. Sigurnosni mehanizmi

Kako bismo u potpunosti ili barem djelomično uklonili ranjivosti sustava za upravljanje bazom podataka, potrebna je ispravna primjena i ugradnja mehanizama za sigurnost baze podataka što uključuje razne vrste kontrola, poput tehničkih, administrativnih i fizičkih.

6.1. Kontrola pristupa

Osnovna metoda zaštite osjetljivih informacija koje se čuvaju u bazi podataka je ograničenje pristupa podacima koje se sastoje od skupa pravila pristupa (engl. access rules) koja definiraju privilegije potrebne za izvođenje određenih operacija nad objektima u bazi podataka (Vujnović, 1995). Privilegije su prava određenog korisnika za pristup, kreiranje, brisanje i manipuliranje raznih objekata unutar baze podataka kao i administriranje bazom podataka.

Kontrola pristupa može se ostvariti na dva načina:

1. autentifikacijom odnosno ovjeravanjem putem korisničkog imena ili lozinke
2. davanjem posebnih privilegija i prava specifičnim objektima i skupovima podataka.

Unutar baze podataka to su obično tablice, pregledi, redci i stupci, a prava koja im se dodjeljuju su čitanje, pisanje ili oboje. Općenito kontrola pristupa definirana je na tri načina:

1. obvezna kontrola pristupa (eng. *Mandatory Access Control*, MAC)
2. diskretna kontrola pristupa (eng. *Discretionary Access Control*, DAC)
3. kontrola pristupa zasnovana na ulogama (eng. *Role Based Access Control* RBAC) (Centar informacijske sigurnosti, 2012.)

6.2. Zaštita od neovlaštenog pristupa

Najčešće brigu oko zaštite od neovlaštenog pristupa u bazama podataka preuzima administrator baze te je on odgovaran za njezinu sigurnost. On dodaje korisnike te dodaje ovlasti tim korisnicima. Ukoliko korisnik pokušava obaviti neku radnju za koju nema pristup tj. nije ovlašten, DBMS neće izvršiti traženu operaciju te će na ekranu ispisati poruku o greški. Da bi administrator mogao to odraditi, on mora imati najveća moguća ovlaštenja (Centar informacijske sigurnosti, 2012).

6.3. Autentifikacija i autorizacija korisnika

Proces autentifikacije, odnosno provjere korisničkog identiteta, iznimno je važan element sigurnosti baze podataka te predstavlja prvu crtu obrane (Manger, 2003). Prije nego se izvrši pristup DBMS-u, vrši se provjera informacija te se nakon provjere identiteta, omogućuje pristup resursima podacima bazi podataka. U autentifikacije metode i tehnologije se ubrajaju lozinke, PIN-ovi, tokeni, SSL digitalne potvrde...

Provjera autentičnosti također omogućuje odgovornost povezivanjem pristupa i radnji s određenim identitetima. Nakon provjere autentičnosti, procesi autorizacije mogu dopustiti ili ograničiti razine pristupa i akcije dopuštene tom entitetu. Autorizacija omogućuje korisniku ovjeren i dopušten pristup bazi podataka putem dodijeljenog sustava dozvola za pojedine objekte. Ona prvenstveno uključuje dva procesa:

1. Dopuštanje samo određenim korisnicima pristupa, obrade ili mijenjanja podataka
2. Primjena različitih ograničenja na pristup ili radnje korisnika. Ograničenja postavljena na (ili uklonjena iz) korisnika mogu se primijeniti na objekte, kao što su sheme, tablice ili redovi; ili resursima, kao što su vrijeme (CPU, povezivanje, ili mirovanje) (Manger, 2003).

6.4. Sigurnosne kopije

U informacijskoj tehnologiji, sigurnosna kopija, ili sigurnosna kopija podataka, ili proces izrade sigurnosnih kopija, odnosi se na kopiranje u arhivsku datoteku računalnih podataka koji su već u sekundarnoj pohrani, , kako bi se mogla koristiti za vraćanje originala nakon događaja gubitka podataka (Mifflin Harcourt, 2018).

Nekada zbog kvara i ispada sustava ili ljudskom pogreškom mogu se oštetiti ili u potpunosti izgubiti podaci spremljeni u bazi. U tom slučaju, sigurnosna kopija baze podataka je jedan od načina zaštite i vraćanja baze podataka. Da bi se omogućila zaštita podataka i baze podataka, potrebno ih je često snimati i pohranjivati te pravilno izrađivati sigurnosne kopije podataka kako bi se rizici i štete koje mogu nastati gubitkom podataka minimalizirale.

Dva najčešća modela izrade sigurnosnih kopija su:

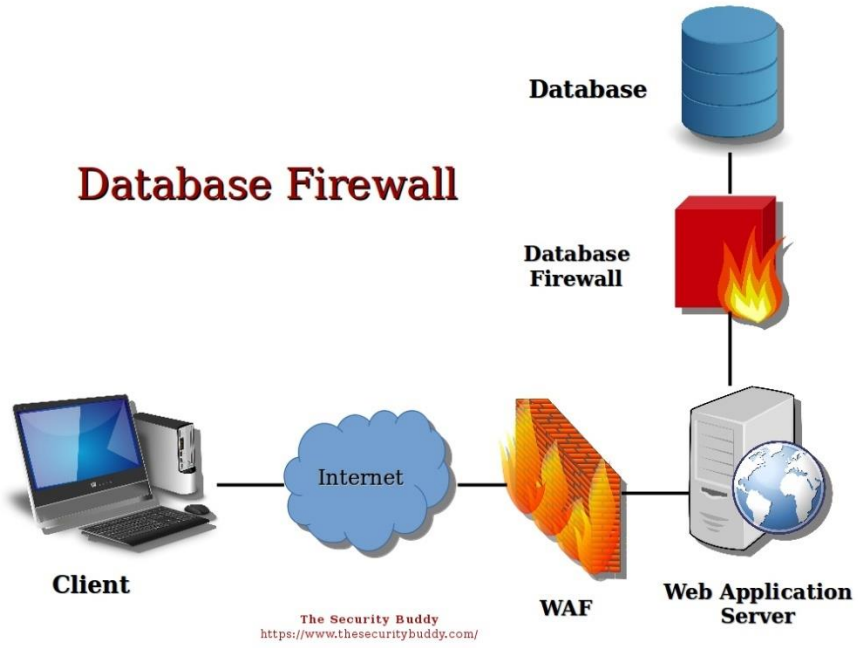
- Potpuna sigurnosna kopija – omogućuje izradu sigurnosne kopije cijele baze podataka
- Diferencijalna sigurnosna kopija – omogućuje izradu sigurnosne kopije samo od posljednje promjene sigurnosne kopije baze podataka (McGehee, 2012).

6.5. Vatrozid

Zaštitne barijere u obliku vatrozida koje mogu biti softverske ili hardverske čija je uloga nadzora, pristupa i transakcije nad bazama podataka sa svrhom identificiranja neovlaštenih radnji i pristupa te aktivirali određene zaštite kao što je onemogućavanje pristupa (Khat, 2011).

Vatrozid baze podataka

Zaštitne barijere u obliku vatrozida koje mogu biti softverske ili hardverske čija je uloga nadzora, pristupa i transakcije nad bazama podataka sa svrhom identificiranja neovlaštenih radnji i pristupa te aktivirali određene zaštite kao što je onemogućavanje pristupa.



Slika 3. Vatrozid baze podataka (Izvor: Mitra, 2017)

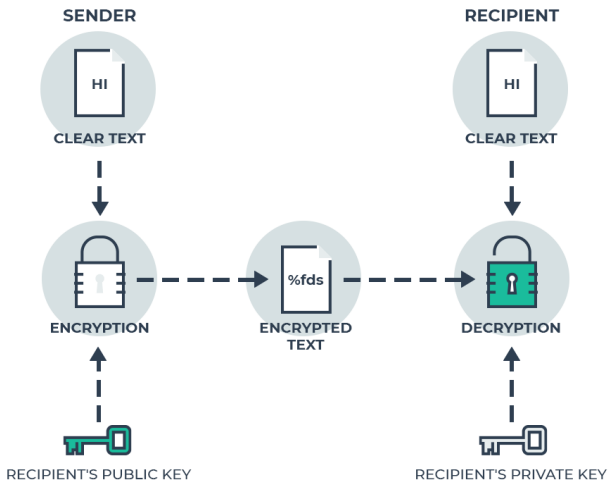
Softverski vatrozid štiti jedno računalo, osim kad je to računalo namijenjeno za zaštitu čitave mreže. On se postavlja ili u liniji s poslužiteljem baze podataka (neposredno prije poslužitelja baze podataka) ili u blizini mrežnog pristupnika (kada štiti više baza podataka na više poslužitelja) (Khat, 2011).

Hardverski vatrozid omogućuje zaštitu čitave mreže ili određenog broja računala. Za ispravan rad vatrozida potrebno je precizno odrediti niz pravila koja određuju kakav promet je dopušten a kakav je zabranjen. Vatrozidi temeljeni na hardveru podržavaju nadzor mreže bez dodatnog opterećenja poslužitelja baze podataka (Khat, 2011).

Vatrozid baze podataka funkcionira tako što uključuje skup unaprijed definiranih, prilagodljivih pravila revizije sigurnosti i oni mogu identificirati napade baze podataka na temelju uzoraka prošlih incidenata ili prijetnji nazvanih "potpisi". Dakle, SQL ulazni izrazi i upiti se uspoređuju s tim potpisima, koji se često ažuriraju kako bi identificirali poznate napade na bazu podataka (Khat, 2011).

6.6. Enkripcija

Enkripcija je proces prikrivanja ili transformacije informacije pomoću šifre tako da ona postaje nečitljiva svim drugim korisnicima, osim onima koji imaju ključ informacija (Basharat et al., 2012).



Slika 4. Algoritam enkripcije (Izvor: Pixel Privacy, n.n)

Enkripcija pruža dodatni sigurnosni sloj pomoću kojega štiti podatke od neovlaštenog pristupa. Trebala bi se primjereno primjenjivati u sva tri sloja informacijskih sustava, odnosno u aplikacijske, sistemske i mrežne slojeve.

Slika 4. prikazuje algoritam enkripcije, u kojem je važna veličina ključa i zaštita ključeva kako bi se osigurala što veća zaštita. Što se bolje koristi algoritam enkripcije, to će sigurnost biti bolja (Basharat et al., 2012).

The Data Encryption Standard (DES) je sustav koji je razvila američka vlada za opću upotrebu. DES može pružiti end-to-end enkripciju na kanalu između pošiljatelja A i prijemnika B.

DES algoritam je pažljiva i složena kombinacija dviju temeljnih tipova enkripcije: supstitucije i permutacije. Nakon preispitivanja adekvatnosti DES-a, NIST je uveo *Advanced Encryption Standard (AES)*. AES omogućuje više mogućih ključeva u usporedbi s DES i tako treba puno više vremena da ga se "probije" (Elmasri i Navathe, 2015).

6.7. VPD

VPN je privatna mreža koja koristi javnu mrežu (obično Internet) za povezivanje udaljenih mjesta ili korisnika. Koristi kompletnu enkripciju podataka, od jednog komunikacijskog kraja do drugoga. VPN-ovi se općenito pridružuju provjeri autentičnosti krajnje točke i sigurnosti podataka, sprečavajući neovlaštene korisnike da koriste web-lokacije ili presreću informacije, iako su u tranzitu preko sustava koji su javni.

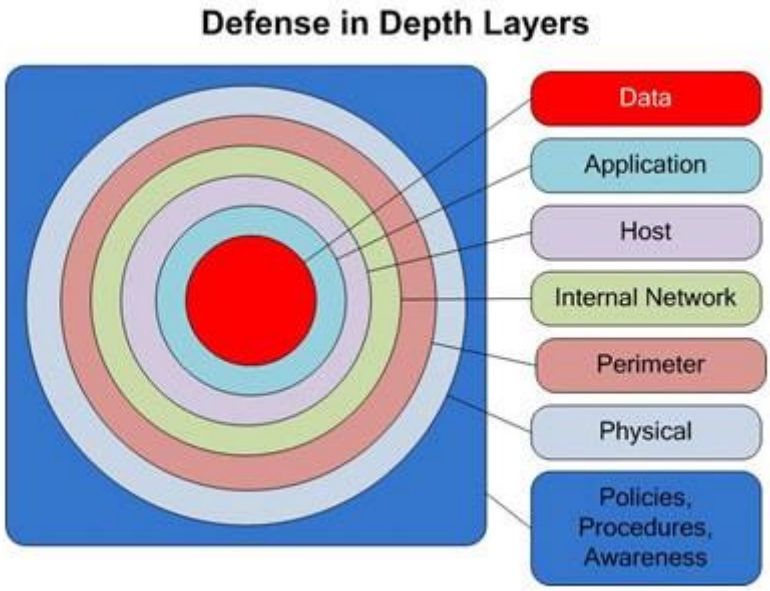
Za razliku od VPN-a, VPD radi provjeru poslužitelja te preciznu kontrolu pristupa za sigurnosne aplikacije. Također pruža i kontrolu pristupa na temelju pravila. Ove VPD politike provode kontrolu pristupa na razini objekta ili sigurnost na razini retka. VPD pruža aplikacijsko sučelje za programiranje (API) koje omogućuje da se sigurnosne politike priključe tablicama ili prikazima baze podataka. VPD je omogućen povezivanjem sigurnosne politike s tablicom, prikazom ili sinonimom (Elmasri i Navathe, 2015).

6.8. Strategija Defence in depth

Obrana u dubini (engl. *Defence in depth*) je pristup cyber sigurnosti u kojem je slojevito prikazan niz obrambenih mehanizama pomoću kojih se štite vrijedni i povjerljivi podaci i informacije. Raslojavanje informacijskog sustava omogućuje obranu i sprečavanje izravnih napada na bazu podataka (Forcepoint, n.d.). Ukoliko jedan od mehanizama nije uspješan, drugi se odmah pokreće kako bi spriječio mogući napad. Ovakav višeslojni pristup povećava sigurnost sustava u cjelini te omogućuje obrani više vremena za zaštitu na kritičnim mjestima u tijeku napada.

U smislu sigurnosti informacija, administrator ili organizacija implementiraju slojeve obrambenih mjera kako bi smanjili rizik od neovlaštenog pristupa ili napada na informacije. U ovoj vrsti napada, napadač pokušava iskoristiti informacijski sustav ili imovinu u okolini u stvarnom vremenu s različitim metodama koje je izuzetno teško spriječiti, a arhitektura obrane u dubini može pružiti diferencijalnu zaštitu (Shamim et al., 2014).

Slojevi obrambenih položaja u *Defense in depth* su, kao što je vidljivo i prema slici, 5. sljedeće:



Slika 5. Strategija Defence in Depth (Izvor: Borga, 2017.)

- Podaci – krajnji cilj je onemogućavanje neovlaštenom pristupu podacima
- Aplikacije – softver koji manipulira podacima
- Radne stanice – računala koja pokreću aplikaciju
- Lokalna mreža – mreža u korporativnoj IT infrastrukturi
- Perimetar – mreža koja povezuje korporativnu IT infrastrukturu s drugom mrežom, poput vanjskih korisnika, partnera ili interneta
- Fizička – opipljivi resursi: poslužitelj računala, hard diskovi, napajanje..
- Politike, postupci, svijesti – sveukupna načela sigurnosnog stratega bilo koje organizacije bez koje čitava strategija propada (Elmasri i Navathe, 2015)

Neke od uobičajenih elemenata koje možemo naći u *Defence in depth* strategiji su:

Sigurnost poslužitelja

Sigurnost računala je važna izrazito važna u sigurnosnoj arhitekturi. Moraju se implementirati antivirusni, anti-malware, mehanizmi za otkrivanje i sprječavanje upada domaćina, vatrozidi temeljeni na poslužitelj kako bi izbjegli moguće napade na mrežu.

Perimetar i kontrole mrežne sigurnosti

Prva linija obrane pri osiguravanju mreže je analiza mrežnog prometa.

Kontrola mrežne sigurnosti počinje s pokrivanjem arhitekture protiv poznatih i očiglednih mrežnih napada. Perimetar mrežnog prometa mora se filtrirati kroz potpunu kontrolu vatrozida, mehanizme za otkrivanje upada, tehnologije identifikacije i blokiranja zlonamjernog softvera, filtriranje predstojećeg opasnog sadržaja (Shamim et al., 2014). Vatrozidi sprječavaju pristup neovlaštenim mrežama i iz njih te dopuštaju ili blokiraju promet na temelju skupa sigurnosnih pravila.

Analiza ponašanja

Važna je kontrola sumnjivih, nelogičnih i sličnih aktivnosti datoteka i mreže. Ako se aktivira analiza ponašanja, to znači da rješenja zaštite kao što je vatrozid ili antivirusni program nisu uspjela. Analiza kontrole u tom slučaju šalje upozorenja ili izvršava automatske kontrole koje sprječavaju daljnju štetu nad podacima. (Forcepoint, n.d.).

6.9. Strategija Defence in breadth

Defense in breadth podrazumijeva implementaciju višestrukih sigurnosnih kontrola na svakom OSI sloju. Također je riječ o automatizaciji sigurnosnih kontrola i procesa (Igbe, 2017). Obrana u širini osigurava sigurnost na razini aplikacije. Većina *Defence in breath* primjenjuje se na mrežni sloj koji je također poznat kao treći OSI sloj.

Međutim, sve se više napada događa s korištenjem ranjivosti na aplikacijskom sloju (sedmi OSI sloj) kao što su SQL injekcija, *cross site scripting* (XSS), slabo upravljanje sesijama i mnogi drugi. To je mjesto gdje vatrozid za web aplikacije (WAF) pruža zaštitu na aplikacijskom sloju. WAF je mjera sigurnosti primijenjena između web-klijenta i web-poslužitelja koji provodi duboku provjeru svakog zahtjeva i odgovora za sve uobičajene oblike web prometa. Identificiranjem i izoliranjem ili blokiranje abnormalnog zlonamjernog prometa, WAF učinkovito sprječava dopiranje prijetnji do poslužitelja (Nadarajan, n.d.).

Isto tako, *Defence in breadth* pomoću različitih aktivnosti nastoji identificirati, upravljati i smanjiti rizik od ranjivosti koje se mogu dogoditi u svim fazama životnog ciklusa sustava, mreže ili pod-komponenti (sustav, mreža ili dizajn proizvoda; proizvodnja; pakiranje, integracija sustava, distribucija, operacije) (Igbe, 2017).

Automatizacija sigurnosti

Glavni naglasak obrane u širini je automatizacija sigurnosnih procesa. Sustav bi se trebao sam oporaviti, to jest, u slučaju napada, sustav bi trebao biti sposoban otkriti anomalije i obraniti se. To podrazumijeva da se sustav obrane u širokom sustavu stalno nadzire i uspoređuje sa željenim

stanjem te se tako ispravljaju sve anomalije. Ponekad, sve što je potrebno za zaustavljanje napada je skeniranje portova kako bi se otkrila anomalija.

Defence in breadth se koristi u modernoj sigurnosnoj infrastrukturi i zahtijeva sposobnost obavljanja sigurnosne analitike za brzo otkrivanje prijetnji i zaustavljanje prijetnji, kako unutarnjih tako i vanjskih napada. Ako ne postoji inteligencija ili sposobnost obrade svih događaja u stvarnom vremenu, napad može uspjeti (Igbe, 2017).

7. Primjeri sigurnosnih mehanizma

Mnogi proizvođači programskih rješenja sustava za upravljanje bazom podataka imaju različita predefinirana rješenja za zaštitu i sigurnost takvih aplikacija. Ovisno o djelatnosti i vrijednosti poslovnog subjekta, odlučuje se za određeni sustav za upravljanje bazom podataka, te su obrađeni i uspoređeni samo neki od dostupnih sustava za upravljanje bazom podataka.

7.1. Oracle baza podataka

Oracle baza podataka (Oracle DB) je sustav za upravljanje relacijskom bazom podataka (RDBMS) iz Oracle Corporation. Izvorno je razvijena 1977. godine od strane Lawrencea Ellisona i drugih razvojnih inženjera, te ubrzo postaje jedan od najpouzdanijih i najšire korištenih DBMS relacijskih baza podataka (Huey, 2017).

Oracle Database podržava konfiguriranje sigurnosti na sljedećim područjima:

1. Sigurnost aplikacije

Prvi korak u kreiranju aplikacije baze podataka je osigurati da je ispravno zaštićena. Politika sigurnosti aplikacije je popis sigurnosnih zahtjeva i pravila aplikacije koji reguliraju korisnički pristup objektima baze podataka (Data Sunrise, n.d.).

2. Korisnički računi

Kod kreiranja korisničkih računa, može ih se zaštiti na različite načine.

Kod kreiranja korisničkih računa, prvo je potrebno specificirati odnosno dodijeliti jedinstveno korisničko ime te zahtijevati unos dovoljno jake i sigurne lozinku, dodijeliti zadani prostor i kvotu tablica za korisnika te na kraju definirati uloge tj. povlastice za korisnika. Također mogu se izraditi profili za zaporke da bi se bolje zaštitila pravila za zaporke za neku web-lokaciju (Huey, 2017).

3. Upravljanje osjetljivim podacima

Neovlašteno korištenje osjetljivih ili povjerljivih podataka može dovesti do negativnih posljedica. Prema tome, osobne podatke, zaštićene zdravstvene informacije, vlasničke informacije i intelektualno vlasništvo treba tretirati s posebnom pažnjom (Data Sunrise, n.d.).

Postoje različita rješenja za pretraživanje podataka na različitim platformama. Oracle Database ima ugrađeni program *Transparent Sensitive Data Protection.*

4. Metode provjere autentičnosti.

Oracle Database nudi nekoliko načina za konfiguriranje provjere autentičnosti za korisnike i administratore baza podataka. Na primjer, mogu se autentificirati korisnici na razini baze podataka, iz operacijskog sustava i na mreži.

Oracle Database dodatno podržava protokole i servise drugih proizvođača:

- Kerberos - protokol provjere autentičnosti dizajniran je prvenstveno za model klijent-poslužitelj i omogućuje međusobnu autentifikaciju.
- Sigurnosni sloj utikača (SSL) - standardni industrijski protokol za osiguranje mrežnih veza.
- Usluga udaljenog biranja za provjeru autentičnosti (RADIUS)
- Za pristup udaljenoj bazi podataka, dopušten je samo siguran pristup ključu (sigurna ljuska (SSH) ili VPN) (Data Sunrise, n.d.).

5. Povlastice i uloge

Mogu se koristiti povlastice i uloge za ograničavanje korisničkog pristupa podacima. Uloge stvaraju administratori kako bi grupirali povlastice ili druge uloge. Oni su način olakšavanja dodjeljivanja višestrukih povlastica ili uloga korisnicima.

Neki on najvažnijih elemenata su:

- Povlastice sustava. Ove povlastice omogućuju primatelju da obavlja standardne administratorske zadatke u bazi podataka. Mogu se ograničiti na samo pouzdane korisnike.
- Uloge korisnika. Uloga grupira nekoliko povlastica i uloga, tako da se mogu dodijeliti i opozvati korisnicima istovremeno. Uloge se moraju omogućiti za korisnika prije nego je korisnik može koristiti.
- Objektne povlastice. Svaki tip objekta ima povlastice povezane s njim. Neki od primjera su selektiranje redaka tablice nekog drugog korisnika, ažuriranje tablica, izvršavanje pohrane drugog korisnika (Data Sunrise, n.d.).

6. Informacije o korisničkoj sesiji.

Kontekst aplikacije je par vrijednosti koji sadrže informacije o sesiji. Mogu se preuzeti informacije o sesiji korisnika, kao što je korisničko ime ili terminal, i ograničiti pristup bazama podataka i aplikacijama za tog korisnika na temelju tih informacija (Data Sunrise, n.d.),

7. Enkripcija.

Mogu se sakriti podaci na mreži kako bi se spriječili neovlašteni pristup tim podacima.

8. Revizija baze podataka.

Mogu se pregledavati aktivnosti baze podataka općenito, kao što je revizija svih SQL izraza, SQL povlastica, objekata sheme i mrežne aktivnosti. Ili se mogu nadzirati

na granularan način, kao što je kada se koristi IP adresa izvan korporativne mreže (Elmasri i Navathe, 2015).

Dodatni resursi za sigurnost baze podataka

Osim već opisanih sigurnosnih resursa, Oracle Database nudi sljedeće proizvode za sigurnost baze podataka:

Oracle Label Security - on osigurava tablice baze podataka na razini reda, omogućujući filtriranje korisničkog pristupa podacima retka na temelju povlastica.

Oracle Database Vault - Oracle Database Vault omogućuje preciznu kontrolu pristupa osjetljivim podacima, uključujući zaštitu podataka od povlaštenih korisnika.

Oracle revizijski trezor - prikuplja podatke revizije baze podataka iz izvora kao što su Oracle Database tablice revizije, revizorske datoteke operacijskog sustava baze podataka i logovi ponovnog postavljanja baze podataka. Pomoću Oracle Audit Vault mogu se kreirati upozorenja o sumnjivim aktivnostima i izvješća o povijesti povlaštenih korisničkih promjena, izmjena shema, pa čak i pristupa na razini podataka.

Oracle Enterprise User Security. Oracle Enterprise User Security omogućuje upravljanje sigurnošću korisnika na razini poslovnog subjekta (Data Sunrise, n.d.).

7.2. MySQL

„MySQL je besplatan, *open source* sustav za upravljanje bazom podataka. MySQL je jedan od najčešćih izbora kod razvoja mnogih softverskih rješenja iz razloga što se radi o kvalitetnom proizvodu, a uz to je besplatan. MySQL se distribuira kao sastavni dio serverskih Linux distribucija, ali ga se može instalirati i na druge operativne sustave kao što su Windowsi, OS X, Solaris, FreeBSD.“ (Anonymus, 2015)

1. Korisnici i povlastice

Sustav povlastica je najosnovnija sigurnosna značajka koju MySQL može ponuditi. Kao i kod Oracle Database, on omogućuje definiranje tko može pristupiti bazi podataka.

Implementacija ide korak dalje od jednostavne sheme korisničkih lozinki i omogućuje povezivanje svakog korisnika s mrežnim mjestom kako bi se spriječio pristup od neželjenih ili nepouzdanih lokacija. Na primjer, MySQL može upotrijebiti znanje o tim dodatnim ograničenjima kako bi

spriječio pokušaje provjere autentičnosti za veze koje dolaze s nepoznatih lokacija, tj. one koje ne pripadaju nijednom korisniku (Dobrzanski, 2013).

2. Enkripcija veze

MySQL implementira SSL kako bi omogućio enkripciju veze. Sve krajnje točke - poslužitelji i klijenti - zahtijevaju vlastiti skup privatnih ključeva i certifikata kako bi mogli koristiti enkripciju.

3. Potvrda utemeljena na certifikatu

Ona omogućuje provjeru autentičnosti u dva faktora gdje više nije dovoljno samo znati korisničko ime i zaporku, ali se također mora dati valjani certifikat za dopuštanje povezivanja. Najosnovniji zahtjev koji se može postaviti jest da certifikati poslužitelja i klijenata moraju biti potpisani od istog tijela za izdavanje certifikata, što znači da ih ne može izdati ili krivotvoriti treća strana (Dobrzanski, 2013).

4. Zabrane poslužitelja

Jedna od ranih sigurnosno-orijentiranih značajki MySQL-a je mogućnost zabrane udaljenih sustava temeljenih na njihovoj povijesti neuspješnih autentikacija. Kontrolirano od strane varijable *max_connect_errors*, MySQL instanca može blokirati određenu adresu od daljnjeg povezivanja na nju nakon nekoliko uzastopnih pokušaja povezivanja bez uspostave uspješne veze. Takav zabranjeni klijent prima Host *'host_name'* je blokirana poruku o pogrešci te se nakon toga prekida veza.

5. Logovi baze podataka

Oni omogućuju praćenje svih aktivnosti te se iz njih mogu locirati zlonamjerne aktivnosti kao i analizu u slučaju otkrivanja nepravilnosti. MySQL nudi dvije vrste logova koji su od korisnosti za tu svrhu - opći zapisnik i zapisnik o pogreškama.

7.3. MsSQL

„MsSQL (Microsoft SQL Server) je sustav za upravljanje relacijskim bazama podataka koji je razvio Microsoft. Kao poslužitelj baze podataka, to je softverski proizvod s primarnom funkcijom pohranjivanja i dohvaćanja podataka prema zahtjevima drugih softverskih aplikacija koje se mogu izvoditi na istom računalu ili na drugom računalu preko mreže.“ (Rouse, n.d.)

Sigurnosne značajke MsSQL-a:

1. Autentifikacija

MsSQL podržava dva načina provjere autentičnosti, način provjere autentičnosti sustava Windows i miješani način rada.

- Provjera valjanosti operativnog sustava (OS) Windows je zadana i često se naziva integrirana sigurnost jer je ovaj sigurnosni model sustava SQL Server čvrsto integriran s OS Windowsom. Određeni korisnički računi za Windows i grupe pouzdani su za prijavu na SQL Server
- Mješoviti način podržava provjeru autentičnosti i za Windows i za SQL Server (Anonymus, 2017).

2. Server i uloge

Sve verzije sustava MsSQL koriste sigurnost temeljenu na dodjeljivanju uloga. Uloge fiksnog poslužitelja imaju fiksni skup dozvola i opseg poslužitelja, dok uloge fiksnih baza podataka imaju unaprijed definiran skup dozvola koje su dizajnirane tako da omogućuju jednostavno upravljanje skupinama dozvola (Anonymus, 2017).

3. Autorizacija i dozvole

Kada se kreiraju objekti baze podataka, moraju im se dodijeliti dozvole kako bi oni bili dostupni korisnicima.

Dodjeljivanje dozvola ulogama pojednostavljuje sigurnosnu administraciju. Skupovi dozvola koji su dodijeljeni ulogama nasljeđuju svi članovi određenih grupa uloga (Anonymus, 2017).

4. Enkripcija podataka

MsSQL omogućuje funkcije pomoću kojih se može kriptirati i dekriptirati podaci koristeći certifikate, asimetrične i simetrične ključeve.

7.4. IBM Db2

IBM Db2 je obitelj proizvoda za upravljanje podacima, uključujući poslužitelje baza podataka, koje je razvio IBM. Oni podržavaju relacijski model, ali posljednjih godina neki su proizvodi prošireni kako bi podržali objektno-relacijske značajke i ne-relacijske strukture kao što su JSON i XML (Chamberlin, 1998).

1. Autentičnost

Provjera autentičnosti korisnika vrši se sigurnosnim uređajem izvan sustava DB2 baze podataka putem modula sigurnosnog dodatka za provjeru autentičnosti. Prilikom instalacije sustava DB2 baze podataka uključen je modul sigurnosnog dodatka za autentifikaciju koji se temelji na provjeri autentičnosti operacijskog sustava. Kako bi osigurali još veću fleksibilnost u prilagođavanju specifičnim potrebama provjere autentičnosti, mogu se izgraditi vlastiti modul sigurnosnog dodatka za provjeru autentičnosti (IBM Knowdledge Centar, n.d.).

2. Autorizacija

Nakon provjere autentičnosti korisnika, administrator baze podataka određuje je li tom korisniku dopušten pristup DB2 podacima ili resursima. Autorizacija je proces kojim administrator baze podataka DB2 dobiva informacije o ovjerenom korisniku, naznačujući operacije baze podataka koje korisnik može izvesti i koje objekte podataka korisnik može pristupiti.

Različiti izvori dozvola koji su dostupni za autorizacijski ID su sljedeći:

- Primarne dozvole: one koje su odobrene prema autorizacijskom ID-u
- Sekundarne dozvole: one koje se dodjeljuju grupama i ulogama u kojima je autorizacijski ID
- Javne dozvole: one koje su dodijeljene PUBLIC-u
- Dopuštenja ovisna o kontekstu: ona koja su dodijeljena ulozi povjerljivog konteksta (IBM Knowdledge Centar, n.d.).

3. Pouzdani konteksti i veze

Pouzdani kontekst je objekt baze podataka koji opisuje odnos povjerenja između baze podataka i vanjskog entiteta, kao što je poslužitelj aplikacija srednje razine. Pouzdani konteksti pružaju način izgradnje brzih i sigurnijih troslojnih aplikacija.

Kada korisnik uspostavi vezu s bazom podataka, sustav DB2 baze podataka provjerava da li se atributi veze podudaraju s definicijom objekta pouzdanog konteksta u bazi podataka. Kada dođe do podudaranja, kaže se da je veza s bazom podataka pouzdana (Chen et al., 2008).

4. Revizija

Revizija pruža mogućnost ulaska u trag protoku informacija i izvršenih radnji unutar baze podataka, uključujući i pokušaje spajanja podataka, ažuriranja, brisanja, umetanja i sl. Korisno je i radi otkrivanja i sprečavanja neovlaštenih aktivnosti unutar baze podataka (Elmasri i Navathe, 2015).

U sustav revizije su uključena u IBM Db2.u:

- Mogu se koristiti novi objekti baze podataka pod nazivom revizijska pravila za kontrolu konfiguracije revizije unutar baze podataka
- Pojedine baze podataka mogu imati vlastite revizijske konfiguracije
- Dnevnici revizije postoje za svaku bazu podataka
- Revidiranje SQL izraza je lakše i proizvodi manje izlaza (Chen et al., 2008).

8. Zaključak

Organiziranjem i pohranjivanjem podataka u odgovarajuće sustave za upravljanje podataka osiguravamo njihovu dostupnost, trajnost i integritet. Programiranjem omogućavamo manipulaciju, izmjenu i dohvat podataka.

Želja za što bržim izvođenjem operacija, visoke performanse i veće tolerancije na greške dovode do novih tehnoloških dostignuća na razini hardvera i softvera. Životni vijek svakog informacijskog sustava je ograničen, stoga smo prisiljeni prijeći na nove platforme i nove sustave. Stoga je nužno donositi sigurnosne politike, provoditi i razvijati sigurnosnu kulturu kroz stalnu edukaciju zaposlenika i osvješćivanje korisnika, što se osobito odnosi na sljedeće: potrebi za redovitim promjenama lozinki, dodjeljivanju ovlasti za pristup podacima, redovito ažuriranje zakrpi za operativni sustav i aplikacije, ažuriranje i skeniranje antivirusnim programom, nadzor i revizije sistemskih i korisničkih log datoteka, izrađivanje sigurnosnih kopija itd.

Provođenje mjera sigurnosti i zaštite sustava za upravljanje bazom podataka predstavlja kontinuirani proces s ciljem sprečavanja štete na podacima, odnosno, na svođenje štete na najmanju moguću mjeru u slučaju incidenta.

9. Literatura

1. Mifflin Harcourt, H. Backup // The American Heritage Dictionary of the English Language, 2018.
2. Basharat, I.; Azam, F.; Muzaffar, A. W. Database Security and Encryption: A Survey Study. // International Journal of Computer Applications 47, 12(2012), str. 28-34.
3. Best Practices for Oracle Database Security, // Data Sunrise. URL: https://www.datasunrise.com/blog/professional-info/oracle_database_security_best_practices/ [27.06.2019.]
4. Borga, A. Defense In Depth For Web Applications, 2017. URL: https://medium.com/insa-tc/defense-in-depth-for-web-applications-38178696f833 [28.06.2019.]
5. Chen, W. J.; Rytir, I.; Read, P.; Odeh, R. DB2 Security and Compliance Solutions for Linux, UNIX, and Windows : IBM International Technical Support Organization, 2008.
6. Darbar Kishansing G.; Suthar Sagar M. Study Of The ANSI/SPARC Architecture // International Journal of Modern Trends in Engineering and Research, 2014.
7. DB2 security model overview. // IBM Knowdledge Centar. URL: https://www.ibm.com/support/knowledgecenter/en/SSEPGG_10.5.0/com.ibm.db2.luw.admin.sec.doc/doc/c0021804.html [27.06.2019.]
8. Dobrzanski, M. MySQL security: Overview of MySQL security features, 2013. URL: https://www.psce.com/en/blog/2013/02/06/mysql-security-overview-of-mysql-security-features/ [27.06.2019.]
9. Elmasri, R.; Navathe, S. B. Fundamentals of Database Systems : Database Security. 7th ed. Pearson, 2015.
10. Huey, P. Introducing Oracle Database Security, 2017. URL: https://docs.oracle.com/cd/E11882_01/network.112/e36292/intro.htm#DBSEG001 [27.06.2019.]
11. How Malware and Targeted Attacks Infiltrate Your Data Center : Imperva, 2013. URL: https://www.ten-inc.com/presentations/Imperva_How_Malware_and_Targeted_Attacks_Infiltrate_Your_Data_Center.pdf [27.06.2019.]
12. Ian. What does ACID mean in Database Systems? Database.Guide, 2016. URL: https://database.guide/what-is-acid-in-databases/ [27.06.2019.]
13. Chamberlin, D. A Complete Guide to DB2 Universal Database, 1998.

14. Igbe, D. Defense in Breadth or Defense in Depth?, 2017. URL: https://www.cloudtechnologyexperts.com/defense-in-breadth-or-defense-in-depth/ [27.06.2019.]
15. Informacijska sigurnost. URL: https://www.soa.hr/hr/podrucja-rada/informacijska-sigurnost/ [27.06.2019.]
16. Khat, R. What are Database Firewalls, why are they required & how do they protect databases?, 2011. URL: https://www.excitingip.com/1933/what-are-database-firewalls-why-are-they-required-how-do-they-protect-databases/ [27.06.2019.]
17. Manger, R. Baze podataka: Uvod u baze podataka. Zagreb : Element, 2014.
18. Manger, R. Osnove projektiranja baza podataka. Sveučilište u Zagrebu : Srce, 2010.
19. Manger, R. Baze podataka. Zagreb : 2003. URL: http://jadran.izor.hr/~dadic/EKO/baze-podataka.pdf [27.06.2019.]
20. Maurer, R. Top Database Security Threats and How to Mitigate Them, 2015. URL: https://www.shrm.org/resourcesandtools/hr-topics/risk-management/pages/top-database-security-threats.aspx [27.06.2019.]
21. McGehee, S. SQL Server Backup and Restore // Simple Talk Publishing, Orlando, 2012.
22. Mitra, A. What is Database Firewall?, 2017. URL: https://www.thesecuritybuddy.com/database-security/what-is-database-firewall/ [28.06.2019.]
23. MySQL, 2015. URL: https://pcchip.hr/softver/korisni/oracle/ [27.06.2019.]
24. Nacionalni CERT // Središnji državni portal, 2019. URL: https://gov.hr/moja-uprava/pravna-drzava-i-sigurnost/sigurnost-na-internetu/nacionalni-cert/1913 [30.08.2019]
25. Nadarajan, V. Defence in depth and breadth – the new approach. URL: https://www.purplebytes.co.uk/blog/2017/11/21/defence-in-depth-and-breadth-the-new-approach [27.06.2019.]
26. Narodne novine (2007) Zakon o informacijskoj sigurnosti. Zagreb : Narodne novine d.d., 79.
27. Overview of SQL Server Security, 2017. URL: https://docs.microsoft.com/en-us/dotnet/framework/data/adonet/sql/overview-of-sql-server-security [27.06.2019.]
28. Rouse, M. Microsoft SQL Server. URL: https://searchsqlserver.techtarget.com/definition/SQL-Server [27.06.2019.]
29. Schulman, A. Top 10 database attacks, 2007. URL: https://www.bcs.org/content/ConWebDoc/8852 [27.06.2019.]

30. Shamim A.; Fayyaz, B.; Balakrishnan V. Layered Defense in Depth Model for IT
31. Organizations, 2014. URL: https://pdfs.semanticscholar.org/20d7/aa23c12aaeccc823c82c785b5048dadd3058.pdf [27.06.2019.]
32. Shribastava, R.; Bhattacharyji J., Soni, R. Sql injection attacks in database using web service: detection and prevention – review. // Asian Journal Of Computer Science And Information Technology, 2/6(2012), str. 162-165.
33. Ured vijeća za nacionalnu sigurnost. URL: https://www.uvns.hr/hr [30.08.2019.]
34. Vujnović, R. SQL i relacijski model podataka. Zagreb : Znak, 1995.
35. What is Defense in Depth? // Forcepoint. URL: https://www.forcepoint.com/cyber-edu/defense-depth [27.06.2019.]
36. What Is Encryption And How Does It Work? // Pixel Privacy. URL: https://pixelprivacy.com/resources/what-is-encryption/ [28.06.2019.]
37. Zaštita baza podataka. Fakulteta elektrotehnike i računarstva, Sveučilišta u Zagrebu : Centar informacijske sigurnosti, 2012.
38. Zavod za sigurnost informacijskih sustava. URL: https://www.zsis.hr/default.aspx?id=1 [30.08.2019.]

Popis slika

Sigurnosni mehanizmi za zaštitu baza podataka

Sažetak

U radu su opisani modeli podataka, arhitektura sustava za upravljanje bazom podataka te je analizirana sigurnosna politika koja se definira kroz zakonsku regulativu informacijske sigurnosti u Republici Hrvatskoj i kroz institucije koje su zadužene za informacijsku sigurnost u Hrvatskoj. Analizirane su dvije poznate strategije planiranja sigurnosti Defence in depth strategy i Defence in breadth te obrađeni i opisani međunarodni sigurnosni standardi. Također, navedeni su i obrađeni osnovni sigurnosni mehanizmi kao što su indentifikacija, autentifikacija, autorizacija i kontrola pristupa, enkripcija, revizija, dodjeljivanje ovlasti, dodjeljivanje uloga, korištenja pogleda, izrade sigurnosnih kopija, korištenje antivirusnog programa, vatrozida i sl. Cilj rada je ukazati na mogućnosti i metode definiranja sigurnosne politike i osiguravanje visokog stupnja sigurnosti, zaštite cjelovitosti i raspoloživosti podataka.

Ključne riječi: baze podataka, sigurnost, sigurnosni mehanizmi

Security mechanisms for database protection

Summary

This paper describes the data models, the architecture of the database management system and analyzes the security policy defined through the information security legislation in the Republic of Croatia and through the institutions responsible for information security in Croatia. Two known security planning strategies, Defense in depth strategy and Defense in breadth, were analyzed and international security standards were elaborated and described. Basic security mechanisms such as authentication, authentication, authorization and access control, encryption, revision, authorization, role assignment, use of views, backup, use of antivirus, firewall, etc. are also discussed and addressed. The aim of this paper is to outline the possibilities and methods of defining a security policy and to ensure a high level of security, protection of data integrity and availability.

Key words: databases, security, security mechanisms