# X - Sigurnost i zaštita baza podataka

## S A D R Ž A J

# 10.1 – Sigurnost baza podataka

- Baze podataka su skupovi neredundantno sačuvanih i organizovanih podataka koje održavaju, distribuiraju i kontrolišu programi nazvani **SUBP** - sistemi za upravljanje bazama podataka (***DBMS***)
- Baze podataka čuvaju različite informacije: korisničke i sistemske
- Različiti programi zahtevaju različite informacije, a one se u današnje doba smeštaju u bazama podataka (***Active Directory***, ***Win.Registry***)
- Bezbednost tih podataka u mnogome zavisi od primenjenog SUBP
- Zbog toga za tim sistemima raste zanimanje kriminalne zajednice, a samim time i potreba da se oni učine bezbednijim i sigurnijim.
- Osim velikog broja informacija koje čuvaju, postoji još nekoliko faktora koji doprinose velikoj zainteresovanosti za bazama podataka.
- Sve većim korišćenjem Interneta, SUBP-ovi koji su tradicionalno bili smešteni u zatvorene mreže i iza zaštitnog zida, postaju sve otvoreniji prema udaljenim korisnicima, a time i sve izloženiji napadima.
- Takođe je postalo vrlo lako pribaviti programske pakete popularnih SUBP-ova, što zlonamernim korisnicima omogućuje istraživanje i pronalaženje **sigurnosnih propusta** (programerskih rupa).

# 10.2-Sistem za upravljanje bazama podataka

- SUBP (***D**ata **B**ase **M**anagement **S**ystem*) je program koji omogućava efikasno formiranje, korišćenje i menjanje baze podataka.
- Zasnovan je na nekom modelu podataka i mora da ima jezike pomoću kojih se definiše integritet baze i kojima se manipuliše bazom tj. vrši selekcija i izmene u njoj (upis, brisanje, modifikacija sadržaja BP).
- Poseduje mehanizme za upravljanje transakcijama, rad u mreži, zaštitu od uništenja, efikasno korišćenje i zaštitu od neovlašćenog pristupa

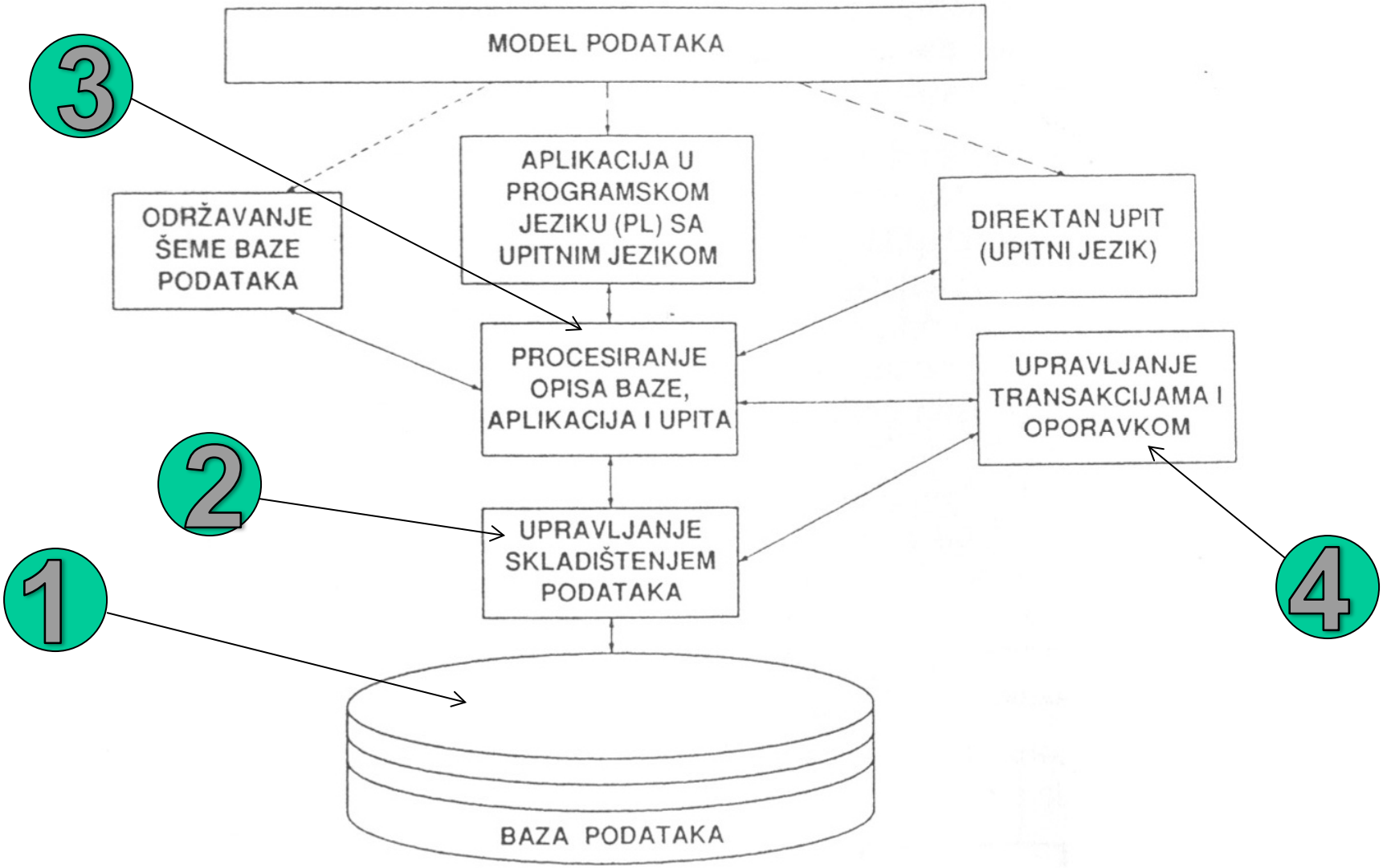
- Višestruke su prednosti sistema za upravljanje bazama podataka:

1. Skladištenje podataka sa minimumom redundanse.
2. Pouzdanost podataka i pri mogućim hardverskim i softverskim otkazima.
3. Pouzdano konkurentno korišćenje podataka od strane više korisnika.
4. Logička i fizička nezavisnost programa od podataka.
5. Jednostavno komuniciranje sa bazom podataka pomoću jezika bliskih korisniku tzv. "**upitnih jezika**".

# 10.2 – Komponente SUBP

1. **Baza podataka u užem smislu**
   - ✓Fizičko smeštanje podataka na nosioce memorije (najčešće diskove)
   - ✓Rečnik baze podataka (katalog)
   - ✓Struktura baze podataka
   - ✓Pravila očuvanja integriteta
   - ✓Prava korišćenja...
2. **Sistem za upravljanje skladištenjem podataka**
   - ✓Upravljanje baferima
   - ✓Upravljanje datotekama
3. **Elementi za pristup bazi podataka**
   - ✓Upiti i aplikacije
   - ✓Održavanje šeme baze podataka
   - ✓Jezik baze podataka
   - ✓Jezik za opis podataka (***Data Definition Language***)
   - ✓Jezik za manipulaciju podataka (***Data Manipulation Language***)
4. **Upravljanje transakcijama i oporavkom**
   - ✓Osobine transakcije: autonomnost, konzistentnost, izolacija i trajnost

# 10.2 – Komponente SUBP



# 10.3 – Ranjivost baza podataka

- Ranjivost baza podataka mogu proizaći iz **neispravne konfiguracije** SUBP-a, **programskih propusta** ili **bezbednosnih nedostataka** unutar aplikacija povezanih sa njima.
- Iako SUBP-ovi često ne podržavaju bezbednosne mogućnosti tradicionalno prisutne kod drugih sistema, ispravno postavljanje postojećih mogućnosti može mnogo podići sigurnosnu nivo
- Osnovni konfiguracioni propusti koji se javljaju kod baza podataka su:

1. **Slaba zaštita korisničkih naloga** - SUBP nemaju mogućnosti kontrole lozinki proverama u rečniku i određivanje roka valjanosti naloga
2. **Neprikladna podela odgovornosti** - na području upravljanja bazama nije priznata uloga administratora za bezbednost baze podataka
3. **Neprikladne metode nadzora** - nadzoru SUBP-a često su pretpostavljeni zahtevi visokih performansi i štednje disk prostora.
4. **Neiskorištene mogućnosti zaštite baza podataka** – bezbedonosni elementi se obično ugrađuju u aplikacije a ne u SUBP. Postoje mnogi alati koji omogućavaju pristup bazi podataka pomoću ODBC-a koji u potpunosti zaobilazi bezbednosne provere ugrađene u aplikacije.

# 10.3 Zaštita neovlašćenog korišćenja

1. **operativnog sistema**: **USERNAME**, **PASSWORD**
2. **samog SUBP-a**: putem naredbi # **SQL GRANT** , # **SQL CREATE VIEW** i # **SQL REVOKE**
3. **mehanizama za zaštitu**: podšema ili pogled.
4. **uvođenje privilegija** koje se definišu za svakog korisnika i svaki element intenzionalnog opisa BP, a odnose se na dozvolu:
   - samo čitanja,
   - čitanja i upisivanja,
   - čitanja i modifikovanja,
   - čitanja i brisanja sadržaja BP.

   Privilegije se unose u autorizacionu tabelu, koja sadrži trojke (korisnik, element intenzionalnog opisa, privilegija).

# 10.3 Zaštita baze podataka od uništenja

- Za zaštitu baza podataka od uništenja koriste se sledeći mehanizmi:
  1. **BACKUP** (kopiranje BP)
  2. **RESTORE** (restauracija BP)
  3. **JOURNAL** (evidentiranje promena BP)
  4. **FORWARD RECOVERY** (ažuriranje kopije baze podataka sa promenama iz JOURNAL-a)
  5. **ROLL BACK** (vraćanje nezavršenih transakcija na početak)
- Ključni mehanizam je vođenje ***journal*** datoteke ( JOURNAL FILE ili TRANSACTION LOG ).
- Tu se evidentiraju sve promene izvršene nad bazom podataka.
- Upotreba JOURNAL-a se dalje svodi na:

✓ ažuriranje kopije BP promenama, pri restauraciji

✓ vraćanju onih promena, koje su u BP izvršile nezavršene transakcije.

✓ vraćanje promena je zadatak upravljača transakcijama (deo RSUBP).

✓ cilj vraćanja je održavanje indeksa i tabela u usaglašenom stanju

✓ ako se neka transakcija ne završi, upravljač transakcijama detektuje to stanje i automatski poništava izvršene izmene BP, koristeći JOURNAL

# 10.4 Programski propusti kod SUBP

- U mnogo čemu je osiguranje BP slično osiguranju računarskih mreža
- U oba slučaja korisniku se daju samo neophodna ovlašćenja, smanjuje se ranjiva "površina" onemogućavanjem nepotrebnih funkcionalnosti, strogo se vrši autorizacija pristupa i pravljenih izmena kod podataka, odvajaju se funkcionalni blokovi, insistira se na enkripciji, itd.
- Razlika je u tome što kod baza podataka svi ovi mehanizmi deluju unutar samog SUBP-a, a za to je potrebna programska podrška.
- Činjenica da se SUBP nalazi iza firewalla ne čini ga apsolutno sigurnim od napada.
- Postoji nekoliko vrsta napada koje je moguće izvesti kroz firewall, a ugnježđavanje SQL naredbi (*SQL injection*) je najčešći.
- Nije direktni napad na SUBP već je pokušaj promene parametara koji se šalju aplikaciji (Web) s namerom menjanja SQL naredbe.
- Programski propusti uključuju i razne greške prekoračenja bafera koje mogu zlonamernim korisnicima omogućiti izvođenje napada zasnovanih na uskraćivanju resursa (*DoS - Denial of Service*) napada ili izvršavanje programskog koda sa kobnim posledicama.

# 10.4 Programski propusti kod SUBP

- **SQL injection** predstavlja trenutak kada se pristupa podacima u BP i kada korisnik namerno unosi sadržaj koji ne odgovara očekivanom kako bi izazvao nepravilan rad baze podataka.
- Ova vrsta napada se može izvršiti na sledeće načine:
  1. **Modifikacijom SQL upita** (promena određenih stavki u upitu kako bi provera identiteta uvek vraćala rezultat *true*)
  2. **Umetanje koda** (postojećem upitu se pridodaje dodatni SQL upit)
  3. **Umetanje funkcijskih poziva** (dodavanje određenih funkcija u sam upit, koji onda izvršavaju funkcijske pozive operativnog sistema)
  4. **Prekoračenje bafera -** predstavlja napad koji sledi posle umetanja poziva funkcije, gde se prepisivanjem podatka u baferu omogućava da napadač pokrene svoj kod umesto procesa koji treba da se izvrši
- Zaštita od napada **SQL injection** se sprovodi putem:
  1. **Upotrebom vezanih promenjivih**
  2. **Proverom parametara koji se unose**
  3. **Upotrebom sigurnih, proverenih funkcija**
  4. **Kontrola poruka o greškama**

# 10.4 Programski propusti kod SUBP

- Napad ugnježđavanjem SQL naredbi najbolje se može ilustrovati primerom autorizacije na Web stranici.
- Korisnik unosi svoje korisničko ime i lozinku pomoću kojih se stvara SQL upit za pretraživanje tabele s korisničkim imenima i lozinkama.
- Ako se u tabeli pronađu unešeno ime i lozinka, izvrši se autorizacija.
- Problem kod ovakvog pristupa je što se SQL upit stvara ulančavanjem bez izuzimanja jednostrukih navodnika. Na primer:

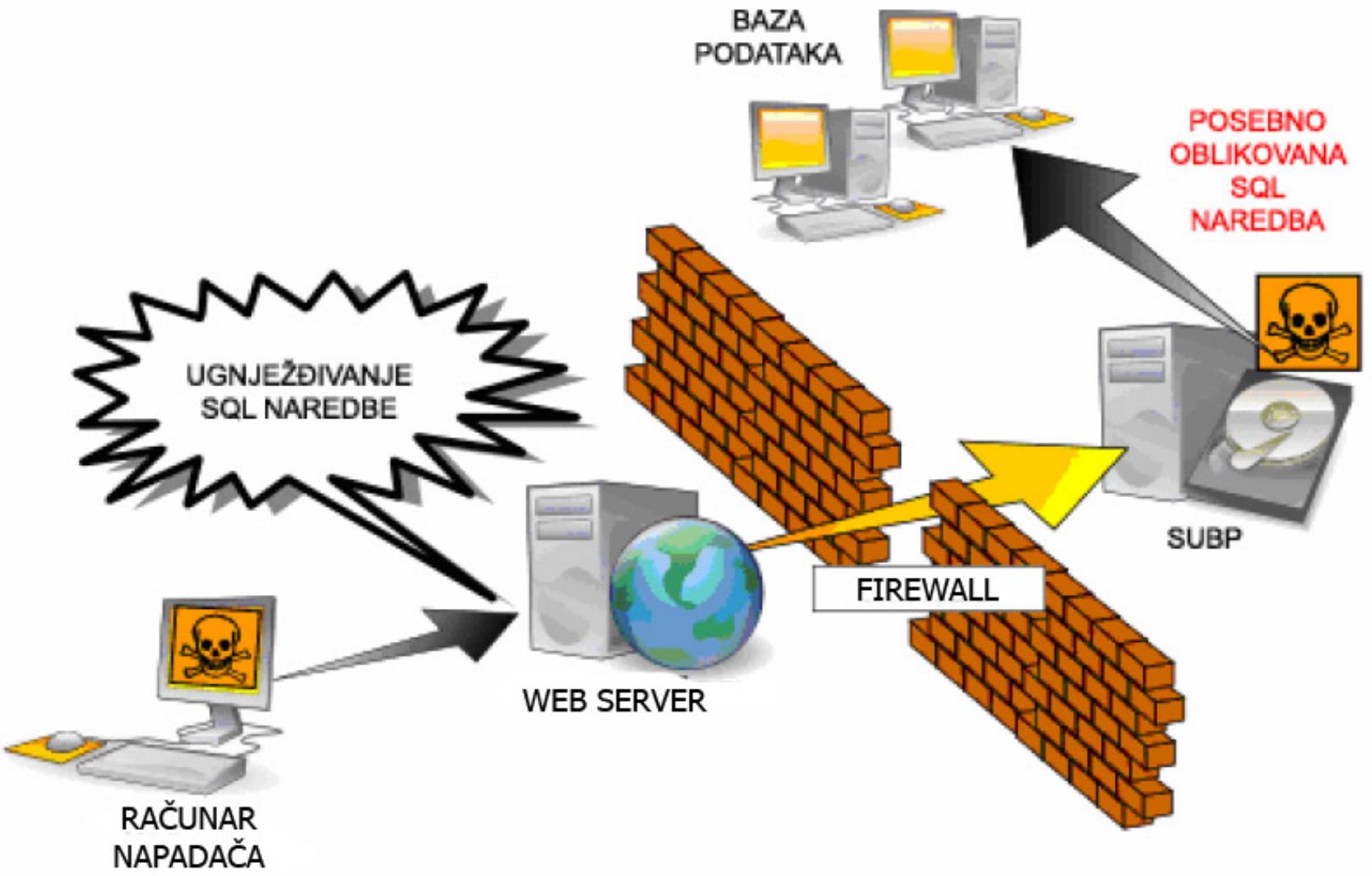
**SELECT * FROM WebKorisnici WHERE KorisnickoIme='Ivan' AND Lozinka='lozinka2'**

- Napadač može umesto lozinke upisati niz slova i završiti znakovni niz jednostrukim navodnikom, **dodati logički izraz koji je uvek istinit**, te tako kao odgovor dobiti sve redove tabele.

**SELECT * FROM WebKorisnici WHERE KorisnickoIme='Ivan' AND Lozinka=' Aa' OR 'A'='A‘**

- Sprečavanje ugnježđavanja SQL naredbi može biti jednostavno ako se poznaje mehanizam napada. Dva su moguća pristupa: provera korisničkih unosa i korišćenje parametriziranih upita.

# 10.4 – Napad na bazu podataka



# 10.5 – Elementi sistema zaštite

- Ugrađivanje bezbednosnih elemenata direktno u SUBP-ove i njihova ispravna primena jedini su pravi način za uklanjanje ranjivosti BP.

## 1. Dodeljivanje primerenih ovlašćenja i dozvola pristupa

- ✓ Korisnicima se dodeljuju minimalna potrebna ovlašćenja prema tzv. *'Least privilege'* načelu.
- ✓ Treba voditi računa o ugrađivanju opisanih ograničenja direktno u SUBP, a ne u klijentsku aplikaciju koja pristupa bazi podataka.
- ✓ U cilju povečanja računarske bezbednosti, ne preporučuje se direktna dodela ovlašćenja pojedinim nalozima već dodeljivanje **Uloga** (R*oles*)

## 2. Efikasni korisnički nalozi i lozinke

- ✓ Korisničke naloge, nužne za pristup bazi podataka, potrebno je definisati u skladu sa tradicionalnim metodama upravljanja korisničkim nalozima.
- ✓ To podrazumeva promenu izvorno postavljenih lozinki, onemogućenje naloga posle određenog broja neuspešnih prijava, ograničenje pristupa podacima, onemogućenje neaktivnih naloga te upravljanje životnim ciklusom korisničkih računa.

# 10.5 – Elementi sistema zaštite

## 3. Primerene metode nadzora i evidencije

- ✓ Jedan od ključnih elemenata zaštite SUBP-ova je nadzor koji treba biti usklađen s njihovom primenom.
- ✓ Pogrešan je pristup nadzoru baziran na načelu "sve ili ništa".
- ✓ Pažljivo postavljen sistem nadzora omogućava uštede vremena i ne utiče značajno na performanse nadziranog SUBP-a.

## 4. Korišćenje enkripcije

- ✓ enkripcija za zaštitu podataka tokom prenosa *data-in-motion,* što se postiže upotrebom komunikacionog protokola SSL
- ✓ drugi je način primena enkripcije na podatke u mirovanju *data-at-rest*
- ✓ postoji i enkripcija datoteka (*file-based*) -ne štiti od napada kroz SUBP
- ✓ Enkripcija na nivou programskog interfejsa (API)
- ✓ Najslabiju podršku imaju za tzv. 'Transparent' enkripciju.

## 5. Kontrola pristupa tabelama

- ✓ najzanemarivaniji element zaštite baza podataka zbog toga što je njena implementacija složena i zahteva saradnju sistemskog administratora i razvojnog programera baze podataka.

# 10.6 Modeli zaštite baza podataka

- Osim ugrađenih sigurnosnih elemenata, u onemogućavanju napada na baze podataka važnu ulogu imaju i modeli njihove zaštite:

**1. Delegiranje odgovornosti**

- ✓ Administratore baze podataka potrebno je zadužiti kako za poslove upravljanja SUBP-a i obezbeđivanja zadovoljavajućih performansi, tako i za delegiranje administracije bezbednosnih poslova.
- ✓ Delegiranjem odgovornosti može se pojedinim administratorima omogućiti obavljanje radnih zadataka u okviru pojedinog odeljenja kompanije, npr. marketinškog ili finansijskog odeljenja.

**2. Smeštanje SUBP-a u unutrašnju mrežu**

- ✓ Smeštanjem SUBP u unutrašnju mrežu ograničava se pristup samoj BP
- ✓ Ako je baza nedostupna, onda je i sigurna od napada.
- ✓ Web server i BP trebaju biti smešteni na odvojenim računarima

**3. Sistem dozvoljenih IP adresa**

- ✓ Usluge SUBP-a treba omogućiti isključivo sigurnim IP adresama.
- ✓ Lokalnim i spolja vidljivim BP treba dodeliti posebne servere.

# 10.6 Modeli zaštite baza podataka

**4. Periodična analiza promena i sumnjivih situacija**

- ✓ Korišćenjem Unix komande "grep" ili Windows komande "find" moguće je pronaći lozinke zapisane u skriptama, tekstualnim datotekama, porukama elektronske pošte te čak u log datotekama.
- ✓ Periodično je potrebno pregledati naloge ne bi li se pronašli korisnici sa nepotrebno visokim ovlašćenjima ili ulogama.

**5. Postavljanje zamki**

- ✓ Neke od periodičnih analiza poželjno je automatizovati tako da rezultate dostavljaju elektronskom poštom
- ✓ Primer primene ove strategije je zapisivanje svakog dodeljivanja uloge administratora korisnicima kojima ta uloga inače ne pripada.
- ✓ U slučaju kada jedan od korisnika baze podataka treba dobiti otkaz, može se pokazati korisnim nadgledati njegov nalog određeno vreme

**6. Primena zakrpa i testiranje**

- ✓ Iako sve zakrpe uklanjaju ranjivosti treba ih oprezno primenjivati zbog mogućnosti unošenja novih pogreški u sistem.
- ✓ Jedino oružje protiv takvih grešaka je prethodno ispitivanje.

# 10.7 - Preporuke za zaštitu BP

- Svi SUBP-ovi sadrže ranjivosti i nije moguće odrediti niti najsigurnijeg niti najranjivijeg među njima.
- Najsigurniji je onaj sistem koji se najbolje poznaje.
- Dobro poznavanje arhitekture i funkcionalnosti sistema od strane administratora, omogućava njegov siguran rad.
- Broj funkcionalnosti koje SUBP poseduje može takođe biti pokazatelj njegove bezbednosti, odnosno nesigurnosti.
- Veći broj funkcionalnosti znači i veće mogućnosti za pojavljivanje ranjivosti, odnosno veću "površinu" izloženu napadima.
- Preporuke vezane uz sigurnost BP se mogu sažeti u sledeći spisak:
  - ✓ korisnicima je potrebno dodjeljivati samo neophodne ovlašćenja,
  - ✓ posebnu pažnju potrebno je posvetiti upravljanju korisničkim nalozima i lozinkama,
  - ✓ ispravno primenjene metode nadzora, periodične analize i korišćenje zamki mogu uveliko pomoći prilikom otkrivanja napada
  - ✓ korišćenje enkripcije otežava pristup osetljivim informacijama kako korisničkim šiframa, tako i svim ostalim podacima smeštenim u bazi

# 10.7 – Preporuke za zaštitu BP

- ✓ postavljanje servera sa bazom podataka u unutrašnju mrežu čini ga daleko sigurnijim, a sistem dozvoljenih IP adresa dodatno smanjuje verovatnoću udaljenih napada.
- ✓ Za bezbednost SUBP-a je vrlo važna stalna i redovna primena zakrpi.
- ✓ Osnovni vid zaštite je ograničenje fizičkog pristupa BP
- ✓ Postoji i softverski vid zaštite koji se ugrađuje u SUBP. Njime se ograničava rad sa BP i ljudima koji imaju mogućnost fizičkog pristupa.
- ✓ Sasvim isključiti mrežne mogućnosti SUBP-a
- ✓ Dopustiti da samo lokalni programi pristupaju SUBP (*localhost*)
- ✓ Dopustiti da samo računari unutar LAN-a pristupaju SUBP
- ✓ Dopustiti nekima, ali uz identifikaciju (korisnik/lozinka)
- ✓ Koristiti šifriranu komunikaciju (ssl/ssh, dvostruki ključevi,. . . )
- ✓ Kroz poglede (*views*) korisniku dati ograničeni pristup bazi podataka
- ✓ Ovlašćenjima se određuje što korisnik može raditi sa podacima: READ/SELECT, UPDATE, INSERT, DELETE
- ✓ SUBP mora pamtiti popis ovlašćenja za svakog korisnika i svaku relaciju iz pripadajućeg pogleda (*view*).

# 10.8 – SUBP: Oracle

- Oracle je najviše raširen SUBP i pokriva najveći deo tržišta.
- Razlozi za to su duga tradicija i podržanost od strane većine OS.
- Listener je server preko koga klijenti pristupaju bazi podataka.
- Ovaj server smešten je izvan BP pa predstavlja problem zbog toga što mogućnosti udaljenog administriranja i postavljanja lozinke nisu dovoljno dokumentovane te su često nepoznate.
- Unutar Listener servera ne postoje uobičajene mogućnosti upravljanja lozinkama:onemogućavanje naloga,odvojen nadzor ili isticanje lozinke
- Pomoću jednostavne skripte moguće probiti čak i vrlo jake lozinke.
- Listener server u nekim situacijama može neovlašćenim korisnicima dozvoliti pristup potencijalno osetljivim informacijama.
- Ako se serveru pošalje paket s neispravnim "SIZE OF PACKET" poljem on odgovara paketom koji sadrži deo prethodne naredbe.
- Otkriveno je i nekoliko grešaka prekoraćenja bafera.
- Jedan od tih propusta može udaljenom zlonamernom korisniku omogućiti izvođenje proizvoljnog programskog koda manipulisanjem SEH (*Structured Exception Handling*) mehanizmom.

# 10.8 – SUBP: Oracle

- Postoji značajna ranjivost povezana sa "SYS.LINK$" tabelom.
- U slučaju ostvarivanja veze s nekom drugom bazom podataka, u nju se zapisuju vreme stvaranja pomenute veze te korisničko ime i lozinka
- Podaci se čuvaju bez šifriranja pa im može pristupiti svaki korisnik sa SELECT ANY TABLE ovlašćenjama.
- Pojedinim korisnicima možemo onemogućiti korišćenje određenih naredbi korišćenjem alata "PRODUCT USER PROFILES" alata
- Tako se može globalno onemogućiti "HOST" opcija koja dozvoljava pristup operativnom sistemu.
- Omogućena je enkripcija korisn. lozinki tokom mrežne komunikacije.
- Ako se ova mogućnost uključi na klijentskoj i serverskoj strani, Oracle koristi prilagođeni DES algoritam za enkripciju lozinki pre slanja.
- Za enkripciju celokupnog mrežnog saobraćaja prema SSL protokolu potrebno je instalirati *Oracle Advance Security* paket.
- Verzije namenjene Windows-u podržavaju enkripciju na nivou datoteka korišćenjem EFS (*Encripting File System*).
- Omogućena je enkripcija i na nivou programskog interfejsa

# 10.8 – SUBP: Oracle

- U svrhu podizanja sigurnosti naloga, korisnicima se savetuje pronalaženje i promena svih izvorno postavljenih korisničkih lozinki kao što su: "SYS", "SYSTEM" ili "APPS".
- Oracle omogućuje kontrolu složenosti korisničkih lozinki, njihovog roka trajanja i ponovnog korišćenja.
- Takođe, poseduje nekoliko metoda autorizacije korisnika:

1. ***Kerberos security*** - implementira Kerberos protokol za pouzdano uzajamno dokazivanje identiteta korisnika tokom komunikacije;
2. **VPD** (*Virtual Private Databases*) – tehnologija koja omogućava ograničenje pristupa pojedinim zapisima u tabeli;
3. ***Role-based security*** – omogućuje grupisanje ovlašćenja u uloge koje je nakon toga moguće dodeliti pojedinim korisnicima;
4. ***Grant-execute security*** – omogućuje ograničavanje mogućnosti procedura u zavisnosti od ovlašćenja korisnika koji ih pokreće;
5. ***Authentication servers*** – serveri za sigurnu identifikaciju korisnika;
6. ***Port access security*** – Listener server može se postaviti tako da ograniči pristup pojedinim portovima.

# 10.8 – SUBP: Microsoft SQL

- Microsoft SQL Server (MsSQL) je SUBP koji je, u poređenju sa Oracle, relativno nov proizvod s brzo rastućom popularnošću.
- Kada se MsSQL izvodi u načinu rada mešovite autentifikacije (*mixed-mode authentication*),pristupne lozinke se snimaju na raznim lokacijama
- Neke od njih se štite snažnom enkripcijom i uključuju visok stepen ograničenja a neke slabom enkripcijom i uz nizak stepen ograničenja.
- Pregledom sistemskih tabela i snimanjem procedura ili korišćenjem SQL Profiler alata, može se otkriti gde i kako se ove lozinke čuvaju.
- Ovde su prvenstveno ugrožene lozinke "SQL Agent" paketa, ***D**ata **T**ransformation **S**ervices* alata te lozinke korišćene prilikom replikacije.
- Zlonamerni prijavljeni korisnik može neovlašćeno steći više korisničkih ovlašćenja ubacivanjem trojanskog konja u SQL server.
- Korisnik ne može pristupiti tabelama za koje nema ovlašćenja, ali se takvim tabelama može pristupiti pomoću vlasničkih procedura i pogleda
- Kako svi korisnici mogu stvarati privremene procedure i tabele, vrlo je jednostavno izvesti napad uskraćivanjem resursa (DoS) na MsSQL: napravi se privremena tabela i pokrene se beskonačna petlja koja je puni.

# 10.8 – SUBP: Microsoft SQL

- Najpoznatije ranjivosti unutar MsSQL baze podataka vezane su za prekoračenje bafera koja su 25. januara 2003. omogućila **Slammer crvu** izazivanje DoS napada na desetinama hiljada računara i značajno usporenje celokupnog Internet saobraćaja.
- Ovaj crv je jako mali (staje u jedan UDP paket) te nema programskog koda koga treba zapisati na disk, već ostaje u memoriji računara.
- Slammer generiše proizvoljne IP adrese te se šalje na njih.
- Neki ruteri su se srušili pod opterećenjem, što je izazvalo niz poruka za ažuriranje tabela rutiranja.
- Microsoft SQL Server server podržava SSL protokol
- Enkripcija datoteka je takođe moguća korišćenjem EFS sistema dok je enkripcija na nivou programskog interfejsa omogućena Crypto API interfejsom koje koristi proširene sačuvane procedure.
- SQL Server server može biti instaliran na više Windows fajl sistema (NTFS, FAT, FAT32 ali je preporuka da to bude NTFS) .
- Broj aktivnih mrežnih programskih biblioteka (*netlib*) treba ograničiti na minimum potreban za funkcionisanje SUBP-a.

# 10.8 – SUBP: MySQL

- MySQL je najviše korišćen SUBP iz grupe programa otvorenog koda.
- Njegova popularnost zasniva se na mogućnosti besplatnog korišćenja, podrške za veliki broj platformi, relativnoj jednostavnosti, lakom održavanju i zadovoljavajućim performansama.
- MySQL određuje nivo ovlašćenja pojedinog korisnika zavisno od hosta s koga se spaja na MySQL SUBP.
- Ako se radi o hostu s LAN-a pretpostavljaju se maksimalna ovlašćenja i zbog toga lokalni napadi mogu biti puno opasniji od udaljenih.
- MySQL sadrži brojne skripte koje u radu koriste privremene datoteke.
- U nekim slučajevima te se privremene datoteke stvaraju na nesigurnim mestima i s predvidljivim imenima pa mogu biti zamenjene simboličkim vezama prema kritičnim sistemskim datotekama.
- MySQL skripta prilikom prepisivanja sistemske datoteke koristi ovlašćenja MySQL procesa koji ju je pokrenuo.
- Značajna ranjivost postoji kod alata Win MySQLAdmin koji u datoteci **my.ini** u tekstualnom nešifrovanom (*plaintext*) formatu čuva administratorsku 'root' lozinku.

# 10.8 – SUBP: MySQL

- MySQL komunikacija izvorno nije šifrovana pa zlonamerni korisnik koji prisluškuje klijent/server vezu može doznati klijent. ime i lozinku
- Kako bi se to izbeglo potrebno je postaviti REQUIRE SSL opciju u GRANT naredbi koja se koristi prilikom povezivanja korisnika.
- Time se osigurava enkripcija saobraćaja, izbegava delovanje značajnog broja napadačkih programskih skripti i osigurava zaštićenost lozinki.
- Kod MySQL SUBP-a postoji korisnički nalog s imenom "root".
- Nekoliko dostupnih alata, skripti i tehnika napada zasnivaju se upravo na postojanju takvog korisničkog naloga.
- Zato se savetuje preimenovanje „root“ korisničkog naloga.
- Niko osim root korisnika ne bi smeo imati pristup mysql.user tabeli jer to omogućuje neovlašćeno sticanje povišenih korisničkih prava.
- Opcija *general query log* se smatra alatom za pronalaženje i uklanjanje grešaka, ali može poslužiti i kao deo rutinskih sigurnosnih provera.
- Ova mogućnost beleži sva uspešna povezivanja i sve upite
- Savetuje se i onemogućavanje *Load Data Local Infile* naredbe.
- Treba onemogućiti *skip-networking* i *skip-symbolic-links* mogućnosti

# Hvala na pažnji !!!

Pitanja

? ? ?