Заштита база података

- Базе података су скупови нередундантно сачуваних и организованих података које одржавају, дистрибуирају и контролишу програми названи **СУБП - системи за управљање базама података (ДБМС)**
- Базе података чувају различите информације: корисничке и системске
- Различити програми захтевају различите информације, а оне се у данашње доба смештају у базама података (Активе Директору, Вин.Регистру)
- Безбедност тих података у многоме зависи од примењеног СУБП
- Због тога за тим системима расте занимање криминалне заједнице, а самим тиме и потреба да се они учине безбеднијим и сигурнијим.

- Осим великог броја информација које чувају, постоји још неколико фактора који доприносе великој заинтересованости за базама података.
- Све већим коришћењем Интернета, СУБП-ови који су традиционално били смештени у затворене мреже и иза заштитног зида, постају све отворенији према удаљеним корисницима, а тиме и све изложенији нападима.
- Такође је постало врло лако прибавити програмске пакете популарних СУБП-ова, што злонамерним корисницима омогућује истраживање и проналажење сигурносних пропуста (програмерских рупа).

- Рањивост база података могу произаћи из неисправне конфигурације СУБП-а, програмских пропуста или безбедносних недостатака унутар апликација повезаних са њима.
- Иако СУБП-ови често не подржавају безбедносне могућности традиционално присутне код других система, исправно постављање постојећих могућности може много подићи сигурносну ниво
- Основни конфигурациони пропусти који се јављају код база података су:
- 1.Слаба заштита корисничких налога - СУБП немају могућности контроле лозинки проверама у речнику и одређивање рока ваљаности налога

- 2.Неприкладна подела одговорности - на подручју управљања базама није призната улога администратора за безбедност базе података
- 3.Неприкладне методе надзора - надзору СУБП-а често су претпостављени захтеви високих перформанси и штедње диск простора.
- 4.Неискоришћене могућности заштите база података – безбедоносни елементи се обично уграђују у апликације а не у СУБП. Постоје многи алати који омогућавају приступ бази података који у потпуности заобилази безбедносне провере уграђене у апликације.

- Заштита од неовлашћеног коришћења:
- 1. оперативног система: УСЕРНАМЕ, ПАССВОРД
- 2. самог СУБП-а: путем наредби # СQЛ ГРАНТ , # СQЛ КРЕАТЕ ВЕБ # СQЛ РЕВОКЕ
- 3. механизама за заштиту: подшема или поглед.
- 4. увођење привилегија које се дефинишу за сваког корисника и сваки елемент интензионалног описа БП, а односе се на дозволу: – само читања, – читања и уписивања, – читања и модификовања, – читања и брисања садржаја БП. Привилегије се уносе у ауторизациону табелу, која садржи тројке (корисник, елемент интензионалног описа, привилегија).

- За заштиту база података од уништења користе се следећи механизми: 1. БАКАП (копирање БП) 2. РЕСТОРЕ (рестаурација БП) 3. ЏОУРНАЛ (евидентирање промена БП) 4. ФОРВАРД РИКАВЕРИ (ажурирање копије базе података са променама из ЏОУРНАЛ-а) 5. РОЛЛ БАК (враћање незавршених трансакција на почетак)
- Кључни механизам је вођење џоурнал датотеке (ЏОУРНАЛ ФАЈЛ или ТРАНСАКТИОН ЛОГ). Ту се евидентирају све промене извршене над базом података.

- Употреба ЏУРНАЛ-а се даље своди на: ажурирање копије БП променама, при рестаурацији враћању оних промена, које су у БП извршиле незавршене трансакције.
- враћање промена је задатак управљача трансакцијама (део РСУБП).
- циљ враћања је одржавање индекса и табела у усаглашеном стању

- ако се нека трансакција не заврши, управљач трансакцијама детектује то стање и аутоматски поништава извршене измене БП, користећи ЏУРНАЛ

- Уграђивање безбедносних елемената директно у СУБП-ове и њихова исправна примена једини су прави начин за уклањање рањивости БП. 1. Додељивање примерених овлашћења и дозвола приступа
- Корисницима се додељују минимална потребна овлашћења према тзв. 'Леаст привилеге' начелу.
- Треба водити рачуна о уграђивању описаних ограничења директно у СУБП, а не у клијентску апликацију која приступа бази података.
- У циљу повечања рачунарске безбедности, не препоручује се директна додела овлашћења појединим налозима веч додељивање Улога (Ролес)

- 2. Ефикасни кориснички налози и лозинке
- Корисничке налоге, нужне за приступ бази података, потребно је дефинисати у складу са традиционалним методама управљања корисничким налозима.
- То подразумева промену изворно постављених лозинки, онемогућење налога после одређеног броја неуспешних пријава, ограничење приступа подацима, онемогућење неактивних налога те управљање животним циклусом корисничких рачуна.

- Примерене методе надзора и евиденције
- Један од кључних елемената заштите СУБП-ова је надзор који треба бити усклађен с њиховом применом.
- Погрешан је приступ надзору базиран на начелу "све или ништа".
- Пажљиво постављен систем надзора омогућава уштеде времена и не утиче значајно на перформансе надзираног СУБП-а.
- 4. Коришћење енкрипције
- енкрипција за заштиту података током преноса дата-ин-мотион, што се постиже употребом комуникационог протокола ССЛ
- други је начин примена енкрипције на податке у мировању дата-ат-рест

- постоји и енкрипција датотека (фајл-бејсд) -не штити од напада кроз СУБП
- Енкрипција на нивоу програмског интерфејса (АПИ)
- Најслабију подршку имају за тзв. 'Транспарент' енкрипцију.
- 5. Контрола приступа табелама је најзанемаривanији елемент заштите база података због тога што је њена имплементација сложена и захтева сарадњу системског администратора и развојног програмера базе података

- Осим уграђених сигурносних елемената, у онемогућавању напада на базе података важну улогу имају и модели њихове заштите: 1. Делегирање одговорности
- Администраторе базе података потребно је задужити како за послове управљања СУБП-а и обезбеђивања задовољавајућих перформанси, тако и за делегирање администрације безбедносних послова.
- Делегирањем одговорности може се појединим администраторима омогућити обављање радних задатака у оквиру појединог одељења компаније, нпр. маркетиншког или финансијског одељења.
- 2. Смештање СУБП-а у унутрашњу мрежу
- Смештањем СУБП у унутрашњу мрежу ограничава се приступ самој БП
- Ако је база недоступна, онда је и сигурна од напада.
- Веб сервер и БП требају бити смештени на одвојеним рачунарима 3. Систем дозвољених ИП адреса
- Услуге СУБП-а треба омогућити искључиво сигурним ИП адресама. Локалним и споља видљивим БП треба доделити посебне сервере.
- Модели заштите база података 4. Периодична анализа промена и сумњивих ситуација

- Коришћењем Уницх команде "греп" или Виндовс команде "финд" могуће је пронаћи лозинке записане у скриптама, текстуалним датотекама, порукама електронске поште те чак у лог датотекама.
- Периодично је потребно прегледати налоге не би ли се пронашли корисници са непотребно високим овлашћењима или улогама.
- 5. Постављање замки
- Неке од периодичних анализа пожељно је аутоматизовати тако да резултате достављају електронском поштом

- Пример примене ове стратегије је записивање сваког додељивања улоге администратора корисницима којима та улога иначе не припада.
- У случају када један од корисника базе података треба добити отказ, може се показати корисним надгледати његов налог одређено време
- 6. Примена закрпа и тестирање
- Иако све закрпе уклањају рањивости треба их опрезно примењивати због могућности уношења нових погрешки у систем.
- Једино оружје против таквих грешака је претходно испитивање.

- Препоруке за заштиту БП
- Сви СУБП-ови садрже рањивости и није могуће одредити нити најсигурнијег нити најрањивијег међу њима.
- Најсигурнији је онај систем који се најбоље познаје.
- Добро познавање архитектуре и функционалности система од стране администратора, омогућава његов сигуран рад.
- Број функционалности које СУБП поседује може такође бити показатељ његове безбедности, односно несигурности.
- Већи број функционалности значи и веће могућности за појављивање рањивости, односно већу "површину" изложену нападима.

- Препоруке везане уз сигурност БП се могу сажети у следећи списак:
- корисницима је потребно додељивати само неопходне овлашћења,
- посебну пажњу потребно је посветити управљању корисничким налозима и лозинкама,
- исправно примењене методе надзора, периодичне анализе и коришћење замки могу увелико помоћи приликом откривања напада
- коришћење енкрипције отежава приступ осетљивим информацијама како корисничким шифрама, тако и свим осталим подацима смештеним у бази

- Препоруке за заштиту БП
- Постављање сервера са базом података у унутрашњу мрежу чини га далеко сигурнијим, а систем дозвољених ИП адреса додатно смањује вероватноћу удаљених напада.
- За безбедност СУБП-а је врло важна стална и редовна примена закрпи.
- Основни вид заштите је ограничење физичког приступа БП
- Постоји и софтверски вид заштите који се уграђује у СУБП. Њиме се ограничава рад са БП и људима који имају могућност физичког приступа.
- Сасвим искључити мрежне могућности СУБП-а

- Допустити да само локални програми приступају СУБП (локалхост)
- Допустити да само рачунари унутар ЛАН-а приступају СУБП
- Допустити некима, али уз идентификацију (корисник/лозинка)
- Користити шифрирану комуникацију (ссл/ссх, двоструки кључеви,. . .)
- Кроз погледе кориснику дати ограничени приступ бази података
- Овлашћењима се одређује што корисник може радити са подацима: РИД/СЕЛЕКТ, АПДЕЈТ, ИНСЕРТ, ДЕЛЕТЕ
- СУБП мора памтити попис овлашћења за сваког корисника и сваку релацију из припадајућег погледа.