Bezbjednost i zaštita informacionih sistema

Bezbjednost baza podataka

Prof. dr Nikola Žarić

e-mail: zaric@ucg.ac.me

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 zahtijevaju različite informacije, a one se u današnje doba smiještaju u bazama podataka (Active Directory, Win.Registry)
- Bezbjednost tih podataka u mnogome zavisi od primijenjenog SUBP
- Zbog toga za tim sistemima raste zanimanje kriminalne zajednice, a samim time i potreba da se oni učine bezbjednijim i sigurnijim.

Sigurnost baza podataka

- 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 smješteni 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 zlonamjernim korisnicima omogućuje istraživanje i pronalaženje sigurnosnih propusta (programerskih rupa).
-

Sistem za upravljanje bazama podataka

- SUBP (Data Base Management System) je program koji omogućava efikasno formiranje, korišćenje i mijenjanje 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 izmjene u njoj (upis, brisanje, modifikacija sadržaja BP).
- Posjeduje mehanizme za upravljanje transakcijama, rad u mreži, zaštitu od uništenja, efikasno korišćenje i zaštitu od neovlašćenog pristupa

Sistem za upravljanje bazama podataka

- 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”.

Komponente SUBP

1. Baza podataka u užem smislu:
    - Fizičko smiještanje podataka na nosioce memorije (najčešće diskove)
    - Rječnik baze podataka (katalog)
    - Struktura baze podataka
    - Pravila očuvanja integriteta
    - Prava korišćenja...
2. Sistem za upravljanje skladištenjem podataka:
    - Upravljanje baferima
    - Upravljanje datotekama

Komponente SUBP

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:
    - Autonomnost,
    - konzistentnost,
    - Izolacija,
    - Trajnost.

Ranjivost baza podataka

- Ranjivosti baza podataka mogu proizaći iz neispravne konfiguracije SUBP-a, programskih propusta ili bezbjednosnih nedostataka unutar aplikacija povezanih sa njima.
- Iako SUBP-ovi često ne podržavaju bezbjednosne 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 provjerama u rječniku i određivanje roka valjanosti naloga

Ranjivost baza podataka

2. Neprikladna podjela odgovornosti - na području upravljanja bazama nije priznata uloga administratora za bezbjednost baze podataka
3. Neprikladne metode nadzora - nadzoru SUBP-a često su pretpostavljeni zahtjevi visokih performansi i štednje disk prostora.
4. Neiskorištene mogućnosti zaštite baza podataka – bezbjedonosni 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 bezbjednosne provjere ugrađene u aplikacije.

Zaštita neovlašćenog korišćenja

1. Operativnog sistema: USERNAME, PASSWORD
2. 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).

Zaštita baze podataka od uništenja

- Za zaštitu baza podataka od uništenja koriste se sljedeći mehanizmi:
    1. BACKUP (kopiranje BP)
    2. RESTORE (restauracija BP)
    3. JOURNAL (evidentiranje promjena BP)
    4. FORWARD RECOVERY (ažuriranje kopije baze podataka sa promjenama 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 promjene izvršene nad bazom podataka.

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 izmjena kod podataka, odvajaju se funkcionalni blokovi, insistira se na enkripciji, itd.
- Razlika je u tome što kod baza podataka svi ovi mehanizmi djeluju 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.

Programski propusti kod SUBP

- 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 promjene parametara koji se šalju aplikaciji (Web) s namjerom mijenjanja SQL naredbe.
- Programski propusti uključuju i razne greške prekoračenja bafera koje mogu zlonamjernim korisnicima omogućiti izvođenje napada zasnovanih na uskraćivanju resursa (DoS - Denial of Service) napada ili izvršavanje programskog koda sa kobnim posljedicama.

Programski propusti kod SUBP

- SQL injection predstavlja trenutak kada se pristupa podacima u BP i kada korisnik namjerno unosi sadržaj koji ne odgovara očekivanom kako bi izazvao nepravilan rad baze podataka.
- Ova vrsta napada se može izvršiti na sljedeće načine:
    1. Modifikacijom SQL upita (promjena određenih stavki u upitu kako bi provjera identiteta uvijek 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 slijedi poslije umetanja poziva funkcije, gdje se prepisivanjem podatka u baferu omogućava da napadač pokrene svoj kod umjesto procesa koji treba da se izvrši

Programski propusti kod SUBP

- Zaštita od napada SQL injection se sprovodi:
    1. Upotrebom vezanih promjenjivih,
    2. Provjerom parametara koji se unose,
    3. Upotrebom sigurnih, provjerenih funkcija,
    4. Kontrola poruka o greškama.

Programski propusti kod SUBP

- Napad ugnježđavanjem SQL naredbi najbolje se može ilustrovati primjerom 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 primjer: SELECT * FROM WebKorisnici WHERE KorisnickoIme='Nikola' AND Lozinka='lozinka1'
- Napadač može umjesto lozinke upisati niz slova i završiti znakovni niz jednostrukim navodnikom, dodati logički izraz koji je uvijek istinit, te tako kao odgovor dobiti sve redove tabele. SELECT * FROM WebKorisnici WHERE KorisnickoIme='Nikola' AND Lozinka=' Aa' OR 'A'='A'
- Sprječavanje ugnježđavanja SQL naredbi može biti jednostavno ako se poznaje mehanizam napada. Dva pristupa: provjera korisničkih unosa i korišćenje parametrizovanih upita.

Elementi sistema zaštite

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

1. Dodjeljivanje primjerenih 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 bezbjednosti, ne preporučuje se direktna dodjela ovlašćenja pojedinim nalozima već dodjeljivanje Uloga (Roles)

Elementi sistema zaštite

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 podrazumijeva promjenu izvorno postavljenih lozinki, onemogućenje naloga poslije određenog broja neuspešnih prijava, ograničenje pristupa podacima, onemogućenje neaktivnih naloga te upravljanje životnim ciklusom korisničkih računa.

Elementi sistema zaštite

3. Korišćenje enkripcije:
   - enkripcija za zaštitu podataka tokom prenosa data-in-motion, što se postiže upotrebom komunikacionog protokola SSL
   - drugi je način primjena 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.

Elementi sistema zaštite

4. Primjerene metode nadzora i evidencije
    - Jedan od ključnih elemenata zaštite SUBP-ova je nadzor koji treba biti usklađen s njihovom primjenom.
    - 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.
5. Kontrola pristupa tabelama
    - najzanemarivaniji element zaštite baza podataka zbog toga što je njena implementacija složena i zahtijeva saradnju sistemskog administratora i razvojnog programera baze podataka.

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 obezbjeđivanja zadovoljavajućih performansi, tako i za delegiranje administracije bezbjednosnih poslova.
    - Delegiranjem odgovornosti može se pojedinim administratorima omogućiti obavljanje radnih zadataka u okviru pojedinog odjeljenja kompanije, npr. marketinškog ili finansijskog odjeljenja.
2. Smiještanje SUBP-a u unutrašnju mrežu
    - Smiještanjem 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 smješteni na odvojenim računarima.

Modeli zaštite baza podataka

3. Sistem dozvoljenih IP adresa
   - Usluge SUBP-a treba omogućiti isključivo sigurnim IP adresama.
   - Lokalnim i spolja vidljivim BP treba dodijeliti posebne servere.
4. Periodična analiza promjena 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.

Modeli zaštite baza podataka

5. Postavljanje zamki
   - Neke od periodičnih analiza poželjno je automatizovati tako da rezultate dostavljaju elektronskom poštom
   - Primer primjene ove strategije je zapisivanje svakog dodjeljivanja 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 vrijeme.
6. Primjena zakrpa i testiranje
   - Iako sve zakrpe uklanjaju ranjivosti treba ih oprezno primjenjivati zbog mogućnosti unošenja novih pogreški u sistem.
   - Jedino oružje protiv takvih grešaka je prethodno ispitivanje.

Preporuke za zaštitu BP

- Preporuke vezane uz sigurnost BP se mogu sažeti u sljedeći spisak:
  - korisnicima je potrebno dodjeljivati samo neophodne ovlašćenja,
  - posebnu pažnju potrebno je posvetiti upravljanju korisničkim nalozima i lozinkama,
  - ispravno primijenjene metode nadzora, periodične analize i korišćenje zamki mogu uveliko pomoći prilikom otkrivanja napada
  - korišćenje enkripcije otežava pristup osjetljivim informacijama kako korisničkim šiframa, tako i svim ostalim podacima smještenim u bazi
  - Osnovni vid zaštite je ograničenje fizičkog pristupa BP
  - 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