Uvod

Problem predstavlja i iznimno veliki broj slabih točaka koje se svakodnevno otkrivaju u različitim komercijalnim i open-source bazama podataka (MySQL, MSSQL, Oracle i sl.), a kojima sistem administratori često ne pridaju dovoljno pažnje. U ovom seminarskom radu pokušati ću što bolje pojasniti što je to zapravo sigurnost baze podataka.

Najprije ću definirati što je to zapravo sigurnost baze podataka i koje opasnosti postoje, nakon toga o načinima njezine zaštite, ulozi administratora u njezinoj sigurnosti, ponešto o napada u SQL injection, te na kraju upotrebom kriptografije za njenu sigurnost.

1.Sigurnost baza podataka

U današnje vrijeme većina informacija čuva se u bazama podataka. Sigurnost baze podataka je veoma važna, privatni podaci su tajni podaci o korisnicima (npr. kreditne kartice), koji smiju biti dostupni samo njima ili nekom tko ima odobrenje od samog korisnika. Uzimajući u obzir prirodu informacija koje se nalaze u bazi podataka, one su konstantno predmet napada, pa je njihova sigurnost ključna za poslovni uspjeh neke organizacije. Kontrola pristupa, kontrola toka informacija, sigurnost operacijskog sustava, sigurnost računalnih mreža, detekcija upada, sve su to različiti mehanizmi i tehnike zaštite baze podataka. Također, način ispitivanja razlikuje ovisno o programskom paketu, odnosno bazi podataka koja se ispituje jer različita programska rješenja sadrže svoje jedinstvene ranjivosti. Obzirom da su poslovne baze podataka rijetko otvorene prema Internetu, ovakvi testovi češće se provode na internoj računalnoj mreži s ciljem zaštite sustava od internih napadača. S druge strane, moderno poslovanje sve se više okreće prema Internetu kroz različite online aplikacije i servise kao što su Internet bankarstvo, online trgovine i sl., tako da sigurnost baza podataka i u ovom području ima sve veću ulogu. Tradicionalno, baze podataka često su zaštićene putem firewallova (vatrozidova) i routera na mrežnoj razini, a dodatnu sigurnost čine uređaji za mrežnu sigurnost.

Dakle, osnova zaštite je fizičko ograničenje pristupa do samog računala, nadalje, ograničava se udaljeni pristup do računala kroz mrežu. No ja ću ovdje prvenstveno pisati o softverskom načinu zaštite, koji je ugrađen u DMBS. Svaki korisnik baze ima svoje korisničko ime i lozinku. Da bi korisnik mogao raditi s bazom, mora se najprije predstaviti DMBS upisujući svoje ime, te dokazati svoj identitet upisujući lozinku, u suprotnom DBMS mu ne dopušta rad. Zaštita se zasniva na tajnosti lozinke. Bazama podataka može se pristupiti s udaljenih računala, a sama prednost pristupanju bazi podataka je i mana jer se putem Interneta lagano dolazi do povrede sigurnosti. Prilikom procjene ranjivosti pokušava pronaći slabe točke koji bi mogle biti iskorištene za provalu u bazu podataka, procjenu pokreću administratori tih baza kako bi uočili slabe točke u sigurnosti i pokušali povećati sigurnost.