امنیت در پایگاه داده
پوریا واحد دهکردی

امنیت پایگاه داده به مجموعه‌ای از ابزارها، کنترل‌ها و اقداماتی اشاره دارد که برای برقراری و حفظ محرمانگی، یکپارچگی و در دسترس بودن پایگاه داده طراحی شده‌اند[1]. این امنیت باید موارد زیر را در بر بگیرد:
- **داده‌های موجود در پایگاه داده**
- **سیستم مدیریت پایگاه داده (DBMS)**
- **هر برنامه‌ای که به پایگاه داده دسترسی دارد**
- **سرور فیزیکی یا مجازی پایگاه داده و سخت‌افزار زیرین**
- **زیرساخت‌های محاسباتی یا شبکه‌ای که برای دسترسی به پایگاه داده استفاده می‌شوند**

برخی از تهدیدات رایج عبارتند از:
- **تهدیدات داخلی**: خطرات امنیتی که از منابع داخلی با دسترسی مجاز به پایگاه داده ناشی می‌شوند.

- **خطای انسانی**: رمزهای عبور ضعیف، به اشتراک گذاری رمز عبور، پاک کردن یا فساد داده‌ها به صورت تصادفی.
- **استفاده از آسیب‌پذیری‌های نرم‌افزاری**: مهاجمان به دنبال شناسایی و هدف قرار دادن آسیب‌پذیری‌ها در نرم‌افزارها هستند و نرم‌افزار مدیریت پایگاه داده هدف ارزشمندی برای آن‌ها است.
- **حملات اینجکشن SQL/NoSQL**: تهدید خاص پایگاه داده که شامل استفاده از رشته‌های حمله تصادفی غیر-SQL و SQL در پرس‌وجوهای پایگاه داده است.

برای محافظت از پایگاه داده در برابر این تهدیدات، اقدامات امنیتی متعددی وجود دارد که شامل رمزنگاری داده‌ها، مدیریت دسترسی‌ها، پشتیبان‌گیری و بازیابی داده‌ها، و نظارت و آزمایش امنیتی مداوم است. همچنین، رعایت بهترین شیوه‌های برنامه‌نویسی و به‌روزرسانی منظم نرم‌افزارها برای جلوگیری از آسیب‌پذیری‌های

امنیتی ضروری است.