

به نام خدا

شهاب الدین لاهوتی
آزمایشگاه پایگاه داده ها
استاد یاریان

امنیت در پایگاه های داده

امنیت پایگاه داده چیست؟

امنیت پایگاه داده فرآیند حفاظت از داده های سازمان در برابر دسترسی و استفاده غیر مجاز، افشاگری، تخریب و یا تغییر می باشد. مدیریت امنیت داده زیر مجموعه ای از مدیریت تکنولوژی اطلاعات می باشد که خود نیز شامل زمینه های مختلفی می باشد. امنیت پایگاه های داده و به طبع امنیت داده های سازمان در واقع اصلی ترین چالش مدیران عامل و مسئولان IT سازمان ها می باشد.

چهار مفهوم امنیت داده ها

1. محرمانگی (Confidentially)
2. تمامیت (Integrity)
3. اعتبار و سندیت (Authenticity)
4. دسترسی پذیری (Availability)

محرمانگی (Confidentially)

محرمانگی اطلاعات یعنی حفاظت از اطلاعات در مقابل دسترسی و استفاده غیر مجاز. داده های محرمانه تنها توسط افراد مجاز قابل دسترسی می باشند.

تمامیت (Integrity)

در بحث امنیت اطلاعات، تمامیت به این معناست که داده ها نمی توانند توسط افراد غیر مجاز ساخته، تغییر و یا حذف گردند. تمامیت، همچنین یکپارچگی داده ها که در بخشهای مختلف پایگاه داده ذخیره شده اند را تحت الشعاع قرار می دهد.

اعتبار و سندیت (Authenticity)

اعتبار و سندیت دلالت بر موثق بودن داده ها و نیز اصلی بودن آنها دارد. به طریقی که اطمینان حاصل شود داده ها کپی یا جعلی نیستند.

دسترسی پذیری (Availability)

دسترسی پذیری به این معنی می باشد که داده ها، پایگاه های داده و سیستمهای حفاظت امنیت، در زمان مناسب نیاز به اطلاعات در دسترس باشند.

روش های ایجاد امنیت در پایگاه داده

رمزنگاری اطلاعات مابین سرور وب و سرور پایگاه داده

استفاده از SSH

عدم استفاده از Hub

استفاده از فایروال