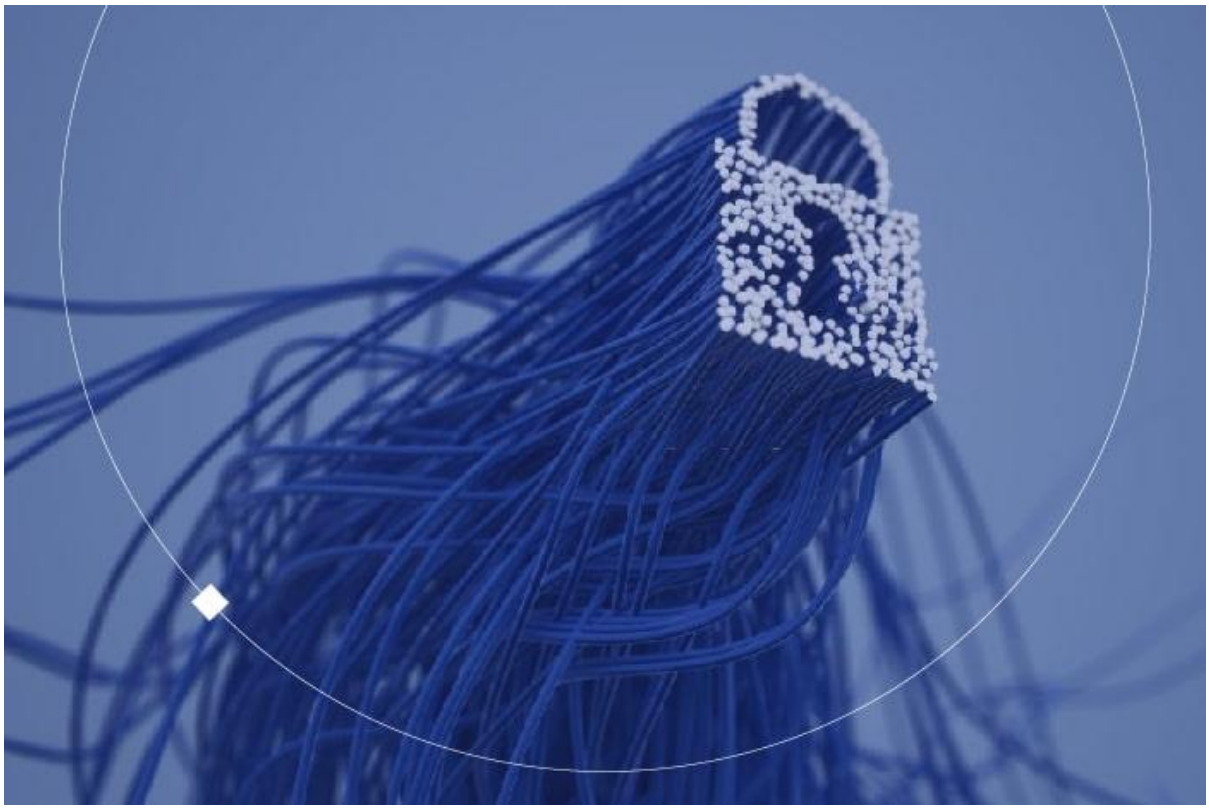
حفظ امنیت نسخه‌های پشتیبان پایگاه داده (Database)



امنیت اطلاعات، همواره یکی از اصلی‌ترین دغدغه‌های مدیر پایگاه داده است؛ اطلاعات حساس و ضروری معمولاً در دیتابیس ذخیره می‌شوند و نسخه‌های پشتیبان نیز در موارد خاص، می‌توانند بسیار حیاتی و مهم باشند. نگهداری و حفظ امنیت نسخه‌های پشتیبان به سه عامل مهم بستگی دارد:

۱. دسترسی به نسخ پشتیبان

اولین نکته‌ای که باید در نظر گرفته شود این است که کاربران نباید امکان تغییر یا حذف فایل‌های بکاپ را داشته باشند؛ پس لازم است که با تعیین سطح دسترسی بر روی محل ذخیره‌سازی نسخ پشتیبان، این امکان از کاربران سلب شود. همچنین می توان محل ذخیره نسخ پشتیبان را به صورت مستقیم به سرورِ پایگاه داده متصل کرد، تا در صورت هک شدنِ شبکه، دسترسی به این مسیر توسط هکرها امکان‌پذیر نباشد.

۲. بازیابی نسخ پشتیبان

بازیابی نسخه‌های پشتیبان نیز مقولهٔ حساسی‌ست و اگر موارد امنیتی دربارهٔ آن رعایت نشود، ممکن است به علت اشتباهات کاربران یا راهبران سیستم، بازیابی اطلاعات به صورت اشتباه انجام شود و مشکل ایجاد کند. به همین دلیل است که باید برای بازیابی اطلاعات از الگوریتم‌های رمزنگاری استفاده شود. وقتی از این الگوریتم‌ها استفاده شود، هنگام بازیابی نسخهٔ پشتیبان به کلید رمزنگاری نیاز خواهد بود.

۳. نگهداری نسخ پشتیبان در محل امن

چالش دیگری که در ارتباط با نسخه‌های پشتیبان وجود دارد، محل نگهداری فیزیکی آنهاست. بهترین کار در این مورد این است که از نسخ پشتیبان را در بستری امن خارج از پایگاه دادهٔ اصلی و حتی خارج از دیتا سنتر نگهداری شوند که در صورت بروز مشکلات و اتفاقات، دسترسی به آنها امکان‌پذیر باشد.