**Bài 15: Bảo mật và an toàn hệ cơ sở dữ liệu**

**Giải thích:**

1. **Tầm quan trọng của việc bảo vệ hệ CSDL**:
   * **CSDL (Cơ sở dữ liệu)** là nơi lưu trữ thông tin quan trọng của tổ chức hoặc cá nhân. Việc bảo vệ CSDL giúp đảm bảo rằng các thông tin này không bị mất mát, thay đổi hoặc truy cập trái phép.
   * Nếu không bảo vệ CSDL, các thông tin nhạy cảm có thể bị rò rỉ, gây thiệt hại về tài chính, danh tiếng, hoặc thậm chí ảnh hưởng đến an ninh quốc gia. (Ví dụ: sự mất mát thông tin hàng triệu người dẫn đến sự sụp đổ của Yahoo)
2. **Một số biện pháp bảo vệ hệ CSDL**:

### ****Phần cứng****

* **UPS (Uninterruptible Power Supply)**: Sử dụng hệ thống nguồn điện liên tục để đảm bảo cơ sở dữ liệu không bị tắt đột ngột do mất điện, tránh mất mát dữ liệu.
* **Bảo mật vật lý**: Hạn chế quyền truy cập vật lý đến các máy chủ (server) chứa cơ sở dữ liệu bằng cách đặt chúng trong các phòng máy có khóa bảo mật và giám sát bằng camera.
* **RAID (Redundant Array of Independent Disks)**: Sử dụng RAID để đảm bảo an toàn cho dữ liệu thông qua việc lưu trữ dữ liệu trên nhiều ổ đĩa cứng khác nhau, tăng khả năng khôi phục khi một ổ cứng gặp sự cố.
* **Thiết bị làm mát**: Đảm bảo các thiết bị làm mát hoạt động ổn định để giữ nhiệt độ của phần cứng trong giới hạn an toàn, tránh các sự cố do quá nhiệt.

### ****Phần mềm****

* **Mã hóa dữ liệu**: Áp dụng mã hóa dữ liệu trong quá trình lưu trữ và truyền tải để bảo vệ thông tin nhạy cảm khỏi bị truy cập trái phép.
* **Tường lửa (Firewall)**: Thiết lập tường lửa để bảo vệ cơ sở dữ liệu khỏi các cuộc tấn công từ bên ngoài và lọc các truy cập không hợp lệ.
* **Hệ thống phát hiện và ngăn chặn xâm nhập (IDS/IPS)**: Sử dụng các hệ thống IDS/IPS để phát hiện và ngăn chặn các cuộc tấn công vào cơ sở dữ liệu.
* **Quản lý quyền truy cập (Access Control)**: Sử dụng các cơ chế quản lý quyền truy cập, chỉ cho phép người dùng hoặc ứng dụng có thẩm quyền mới có thể truy cập vào cơ sở dữ liệu.
* **Sao lưu định kỳ**: Thực hiện sao lưu dữ liệu định kỳ và lưu trữ bản sao lưu ở nơi an toàn, giúp khôi phục dữ liệu nhanh chóng trong trường hợp bị mất hoặc hỏng hóc.
* **Cập nhật và vá lỗi thường xuyên**: Thường xuyên cập nhật và áp dụng các bản vá lỗi phần mềm để bảo vệ cơ sở dữ liệu khỏi các lỗ hổng bảo mật mới được phát hiện.
* **Giám sát và ghi nhật ký (Logging and Monitoring)**: Thiết lập hệ thống giám sát và ghi nhật ký để theo dõi các hoạt động và truy cập vào cơ sở dữ liệu, từ đó phát hiện và xử lý kịp thời các hoạt động đáng ngờ.

Những biện pháp trên giúp bảo vệ hệ CSDL một cách hiệu quả, đảm bảo rằng thông tin quan trọng được an toàn và bảo mật.