BÀI 8 BẢO VỆ SỰ AN TOÀN CỦA HỆ CSDL VÀ BẢO MẬT THÔNG TIN TRONG CSDL

Học xong bài này, em sẽ:

- Nêu được tầm quan trọng của an toàn và bảo mật hệ CSDL.
- Nêu được một số biện pháp bảo vệ sự an toàn và bảo mật hệ CSDL.

Hệ CSDL của một tổ chức thường có nhiều người dùng truy cập, do vậy có những nguy cơ đe doạ sự an toàn của hệ CSDL. Em hãy cho một vài ví dụ về những nguy cơ đó và hậu quả có thể xảy ra.

1 Tầm quan trọng của việc bảo vệ sự an toàn của hệ CSDL và bảo mật thông tin trong CSDL

Bảo vệ sự an toàn của hệ CSDL và tầm quan trọng của an toàn hệ CSDL

Bảo vệ sự an toàn hệ CSDL là bảo vệ hệ CSDL khỏi các mối đe doạ cố ý hoặc vô tình. Nguy cơ phá vỡ sự an toàn của hệ CSDL có thể đến từ những sự cố, tai hoạ ngẫu nhiên. Ví dụ, do thao tác vô tình hoặc do lỗi bất chợt ở phần cứng làm hỏng các ổ đĩa lưu trữ dữ liệu hay sự cố cháy nổ,... Tất nhiên sự cố tình phá hoại hoạt động của hệ CSDL, sử dụng hệ CSDL một cách bất hợp pháp hay đánh cắp dữ liệu cũng là nguy cơ làm mất đi sự an toàn của hệ CSDL.

Bảo vệ sự an toàn của hệ CSDL là rất quan trọng đối với bất cứ tổ chức nào vì bất kì một hỏng hóc hay mất mát nào cũng sẽ ảnh hưởng đến hoạt động hằng ngày của tổ chức và hiệu suất làm việc của mọi người.

Bảo mật thông tin trong CSDL và tầm quan trọng của bảo mật thông tin

Một CSDL có thể có những dữ liệu cần được bảo mật. Điều này có nghĩa là cần kiểm soát được việc xem dữ liệu, mỗi cá nhân chỉ được phép xem dữ liệu mà họ được quyền xem. Bảo mật được thông tin trong CSDL là bảo vệ được tính bí mật của những thông tin có tính riêng tư của cá nhân hay tổ chức. Ví dụ, để lộ những thông tin cá nhân bí mật như hồ sơ sức khoẻ, số tài khoản cũng như mật khẩu thẻ tín dụng là vi phạm tính bảo mật thông tin. Những thông tin như bí mật thương mại, phân tích cạnh tranh, kế hoạch tiếp thị và bán hàng cũng là những ví dụ về thông tin cần bảo mật của một công ty thương mại, không phải ai trong công ty đó cũng được quyền biết.

Bảo mật thông tin trong CSDL cũng rất quan trọng. Các tổ chức không thực hiện được bảo mật thông tin sẽ phải gánh chịu nhiều hậu quả khó giải quyết hoặc tổn thất. Ví dụ, nếu thông tin bị đánh cắp là tài sản trí tuệ của một công ty thì họ có thể đánh mất

lợi thế cạnh tranh trên thị trường. Một ví dụ khác, nếu thông tin bí mật của khách hàng bị lộ, đơn vị kinh doanh chủ quản hệ CSDL lưu trữ thông tin đó có thể phải đối mặt với pháp luật, bồi thường cho khách hàng, mất uy tín trong kinh doanh.

Bảo vệ tính an toàn của hệ CSDL và bảo mật thông tin trong CSDL là vô cùng cần thiết. Đó không chỉ là bảo vệ dữ liệu bên trong CSDL, bảo vệ tính bí mật của thông tin, mà còn gồm cả bảo vệ hệ quản trị CSDL và tất cả các ứng dụng CSDL sao cho không có truy cập sử dụng dữ liệu sai mục đích và làm hư hỏng dữ liệu.

2 Một số biện pháp bảo vệ sự an toàn của hệ CSDLvà bảo mật thông tin trong CSDL

Theo em, sự an toàn của hệ CSDL và bảo mật thông tin trong CSDL có liên quan đến nhau không? Em hãy giải thích ý kiến của mình về điều đó.

a) Bảo vệ sự an toàn của hệ CSDL

Có nhiều biện pháp và cách thức khác nhau mà các tổ chức, doanh nghiệp thực hiện để hệ CSDL của họ được an toàn. Dưới đây là một số biện pháp thường được sử dụng.

Xác thực người truy cập: Hai loại xác thực thường được thực hiện đồng thời là xác thực bằng *thẻ vào cửa* và xác thực bằng *kiểm tra quyền truy cập tài khoản*. Hệ thống bảo vệ (người bảo vệ và camera an ninh) được các tổ chức thiết lập nhằm ngăn chặn người xâm nhập trái phép các thành phần vật lí của hệ thống như: khu vực, toà nhà, phòng chứa máy chủ. Đồng thời với điều đó, các hình thức *thẻ vào cửa* (thẻ nhân viên và mã truy cập vào cửa,...) là một biện pháp không thể bỏ qua. Để *kiểm tra quyền truy cập tài khoản*, xác thực qua mật khẩu là biện pháp phổ biến. Nhiều hệ thống sử dụng thêm các hình thức xác thực khác nữa như: chữ kí điện tử, nhận dạng vân tay, nhận dạng giọng nói, nhận dạng khuôn mặt,... Cơ chế xác thực mạnh sẽ bảo vệ quyền truy cập hiệu quả hơn.

Sử dụng tường lửa: Sử dụng một kĩ thuật được cài vào hệ thống mạng để thiết lập một rào cản giữa một mạng nội bộ đáng tin cậy và mạng bên ngoài không tin cậy.

Sao lưu dự phòng và duy trì biên bản hệ thống: Tạo các bản sao lưu của CSDL và các tệp biên bản (nhật kí) theo định kì, đồng thời đảm bảo rằng các bản sao ở một vị trí an toàn. Trong trường hợp xảy ra lỗi khiến CSDL không thể sử dụng được, bản sao lưu và các chi tiết được ghi lại trong tệp nhật kí được sử dụng để khôi phục CSDL về trạng thái nhất quán mới nhất có thể.

b) Bảo mật thông tin trong CSDL

Nhiều trường hợp cố tình truy cập trái phép, tấn công vào hệ CSDL là để nhằm lấy cắp dữ liệu, đặc biệt là dữ liệu bí mật. Bởi vậy, tất cả các biện pháp nhằm bảo vệ sự an toàn của hệ thống CSDL cũng có vai trò thiết yếu để tăng cường bảo mật thông tin trong CSDL.

Mã hoá dữ liệu là biện pháp bảo mật dữ liệu trong CSDL, là lớp bảo vệ trong trường hợp các biện pháp kiểm soát truy cập đã bị vượt qua. Mã hoá dữ liệu là quá trình chuyển đổi dữ liệu sang một định dạng khác gọi là bản mã. Chỉ những người dùng được uỷ quyền có khoá giải mã mới có thể truy cập được thông tin đó (*Hình 1*). Mục tiêu của mã hoá dữ liệu là để bảo vệ tính bí mật của dữ liệu kĩ thuật số trong quá trình lưu trữ hoặc trong quá trình truyền trên mạng.

Hình 1. Mã hoá dữ liệu và giải mã

Nén dữ liệu cũng góp phần tăng cường tính bảo mật dữ liệu ngoài mục đích giảm dung lượng lưu trữ. Khi có dữ liệu dạng nén, cần biết quy tắc nén, giải nén mới có dữ liệu gốc được. Việc áp dụng các biện pháp an toàn và bảo mật hệ CSDL có ý nghĩa rất quan trọng nhằm bảo vệ hệ CSDL.

Em hãy nêu một trường hợp cụ thể về hệ CSDL không được an toàn hoặc lộ bí mật thông tin. Với trường hợp đó, cần áp dụng biện pháp nào để tăng cường khả năng bảo vệ sự an toàn của của hệ CSDL và bảo mật thông tin trong CSDL.

Em hãy tìm hiểu các giải pháp đảm bảo an toàn cho hệ CSDL của trường em và đề xuất bổ sung giải pháp cụ thể để nâng cao tính an toàn cho hệ thống đó.

Câu 1. Vì sao cần đảm bảo sự an toàn của hệ CSDL và bảo mật thông tin trong CSDL?

Câu 2. Hãy nêu một vài biện pháp thông dụng bảo vệ sự an toàn cho hệ CSDL và giải thích mục đích của việc mã hoá dữ liệu.

Tóm tắt bài học

- Cần thiết phải bảo vệ hệ CSDL và bảo mật thông tin trong CSDL khỏi những mối đe doạ: phá hoại hoạt động của hệ thống, thay đổi dữ liệu, lấy cắp dữ liệu, làm lộ bí mật thông tin.
- Một số biện pháp bảo vệ sự an toàn của hệ CSDL được dùng rất phổ biến là: xác thực người truy cập kiểm soát các truy cập, sử dụng tường lửa, sao lưu dự phòng và duy trì biên bản hệ thống.
- Mã hoá và nén dữ liệu là những biện pháp thường dùng để bảo mật thông tin trong CSDL, ngoài ra các biện pháp bảo vệ sự an toàn của hệ CSDL cũng giúp ngăn chặn nguy cơ xâm nhập lấy cắp thông tin bí mật.