

SAU BÀI HỌC NÀY EM SẼ:

- Hiểu được tầm quan trọng và một số biện pháp bảo vệ hệ CSDL.



Mỗi hệ CSDL đều được xây dựng với mục đích xác định nhằm phục vụ một hệ thống quản lý như hệ thống bán vé máy bay, đặt chỗ khách sạn, quản lý bệnh án ở bệnh viện, quản lý kết quả học tập, quản lý website mạng xã hội,... Từng có nhiều thông tin về việc những khối lượng lớn dữ liệu bị đánh cắp, những tài khoản người dùng mạng xã hội bị gán những phát biểu sai trái,... Tình trạng này xảy ra một phần do các hệ CSDL liên quan chưa được bảo vệ đủ tốt. Cần phải làm gì để đảm bảo an ninh, an toàn cho các hệ CSDL?

1. BẢO MẬT HỆ CSDL

Hoạt động 1 Tổ chức phân quyền với website âm nhạc

Tất cả người dùng Internet đều có thể được tìm kiếm, được xem danh sách các bản nhạc theo tên bản nhạc, tên ca sĩ, tên nhạc sĩ mà không cần đăng nhập hệ thống. Ngoài ra, một số người dùng xác định có quyền nhập thêm dữ liệu về bản nhạc mới, nhạc sĩ mới và ca sĩ mới. Theo các em, cần phải tổ chức phân quyền truy cập CSDL như thế nào để đáp ứng các yêu cầu trên?



Việc lập danh sách và xác định quyền hạn các nhóm người dùng đối với hệ CSDL chính là công việc đầu tiên cần phải thực hiện để *Xây dựng chính sách bảo mật CSDL*.

Trong trường hợp website âm nhạc, có thể thấy có bốn nhóm người dùng với quyền hạn khác nhau:

- Nhóm 1: Nhóm người dùng, không cần khai báo, đăng nhập, được quyền chỉ tìm kiếm, xem, không có quyền cập nhật.
- Nhóm 2: Nhóm người dùng có quyền thêm vào CSDL các bản nhạc mới, tên nhạc sĩ, ca sĩ mới. Nhưng không có quyền xóa, sửa.
- Nhóm 3: Nhóm người dùng có quyền xóa, sửa dữ liệu trong các bảng của CSDL, nhưng không có quyền thay đổi cấu trúc bảng, không có quyền xóa bảng.
- Nhóm 4: Nhóm người dùng có toàn quyền đối với các bảng trong CSDL, chính là người dùng có quyền tạo lập các bảng của CSDL.

Người ta sẽ thiết lập một bảng user để quản lý những người có quyền đăng nhập website âm nhạc, bao gồm các cột: tên đăng nhập, mật khẩu và nhóm người dùng.

Mỗi khi người dùng đăng nhập website âm nhạc sẽ biết được họ thuộc nhóm người dùng nào, 2 hay 3 hay 4. Người dùng nhóm 1 không cần đăng nhập website âm nhạc.

Để tất cả người dùng Internet có thể tìm kiếm, xem danh sách các bản nhạc mà không cần đăng nhập website âm nhạc, có thể tạo một tài khoản khách (guest) và cấp cho tài khoản này quyền SELECT đối với tất cả các bảng **nhacsi**, **casi**, **bannhac**, **banthuan**. Tất cả người dùng khi vào xem website âm nhạc sẽ mặc nhiên được xem như truy xuất CSDL music với tài khoản guest.

Tiếp theo có thể tạo một tài khoản, chẳng hạn là moderator và cấp quyền SELECT, INSERT đối với tất cả các bảng cho moderator. Tất cả những người dùng nhóm này có quyền nhập thêm dữ liệu về bản nhạc mới và ca sĩ mới, sau khi đăng nhập vào website âm nhạc sẽ truy xuất CSDL music với tài khoản này.

Đối với nhóm 3, có thể tạo tài khoản, chẳng hạn là master_mod, có tất cả quyền SELECT, INSERT, UPDATE, DELETE đối với tất cả các bảng **nhacsi**, **casi**, **bannhac**, **banthuan** trong CSDL music. Tất cả những người dùng nhóm này khi đăng nhập website âm nhạc sẽ dùng tài khoản master_mod để truy xuất, cập nhật CSDL.

Cuối cùng là tài khoản admin có toàn quyền đối với tất cả các bảng trong CSDL music cho người dùng thuộc nhóm 4.

Tài khoản đăng nhập website	Nhóm 1 (không cần tài khoản)	Nhóm 2	Nhóm 3	Nhóm 4
Tài khoản truy xuất CSDL	guest	moderator	master_mod	admin

Như vậy các nhóm người dùng khác nhau đều có quyền truy xuất CSDL phù hợp, nhưng ngay cả người dùng có quyền cao nhất ở nhóm 4 cũng không thể can thiệp vào các CSDL khác được quản trị trong cùng hệ QTCSDL.

Tuy nhiên, việc đảm bảo an ninh CSDL còn phụ thuộc vào chính ý thức của người dùng. Nếu những người dùng thuộc các nhóm 2, 3, 4 không bảo vệ quyền của mình, để lộ hay để người khác chiếm được tài khoản của mình thì giải pháp bảo mật theo hình thức phân quyền nói trên sẽ hạn chế tác dụng. Nói rộng ra đối với những CSDL cần bảo mật như CSDL ngân hàng, chứng khoán,... nếu người dùng tiết lộ thông tin truy cập thì dữ liệu cũng không còn được bảo mật.

Vì vậy, khi xây dựng chính sách bảo mật CSDL, cần phải bổ sung cả những nội dung liên quan đến ý thức và trách nhiệm của người dùng đối với tài khoản của mình cũng như đối với dữ liệu trong CSDL.

Khi một ứng dụng CSDL hoạt động, nó có thể trở thành một hệ thống với hàng nghìn, hàng trăm nghìn, thậm chí hàng triệu người truy cập đồng thời và trở nên phần nào giống như một hộp đen, người quản trị không thể biết được hết người dùng đang làm gì, các hoạt động đang diễn ra bên trong hệ thống ra sao, có điều gì bất ổn hay có nguy cơ nào rình rập hay không,... Vì vậy, cũng cần có chính sách, với những kế hoạch cụ thể, tổ chức giám sát hoạt động của hệ thống: số người truy cập, tình trạng thiết bị, máy móc,... Những truy xuất của người dùng có thể cần phải được lưu lại dưới dạng biên bản (thường gọi là *log file*) để khi cần có thể kiểm tra, phân tích. Phải xây dựng kế hoạch xử lý các tình huống dự tính có thể xảy ra.

Cuối cùng cần chú ý khi hệ thống máy tính chứa CSDL được kết nối vào mạng cần phải có kế hoạch cụ thể về các giải pháp an ninh mạng (cả về phần cứng và phần mềm) để chống lại các cuộc tấn công qua mạng.

Công tác bảo mật CSDL cần được thực hiện với một chính sách bảo mật toàn diện bao gồm:

- Quy định liên quan đến ý thức và trách nhiệm của người dùng đối với tài khoản của mình và dữ liệu trong CSDL.
- Quy định về tổ chức đảm bảo an ninh mạng cùng với hệ thống phần cứng và phần mềm cụ thể.
- Danh sách các nhóm người dùng và danh sách tài khoản truy xuất CSDL với quyền hạn tương ứng.
- Biện pháp giám sát trạng thái hoạt động của hệ thống, người dùng. Có những quy định về làm biên bản lưu trữ hoạt động của hệ thống và kế hoạch xử lý những tình huống có thể xảy ra.



Nêu tóm tắt các quyền của các tài khoản moderator và admin.

2. BẢO ĐẢM AN TOÀN DỮ LIỆU

Hoạt động 2

Bảo đảm an toàn dữ liệu là việc đảm bảo để dữ liệu trong CSDL không bị sai lạc, mất mát khi hệ thống phần cứng, phần mềm gặp sự cố rủi ro. Hãy nêu một vài sự cố có thể xảy ra và cách hạn chế, khắc phục các sự cố này.



a) Sự cố về nguồn điện

- Hệ thống cấp điện không đủ công suất. Giải pháp: Xây dựng hệ thống cấp điện đủ công suất.
- Hệ thống cấp điện bị quá tải do nhu cầu sử dụng điện tăng đột biến. Giải pháp: Thường xuyên kiểm tra hệ thống cấp điện, đặc biệt trong những thời gian nhu cầu sử dụng điện tăng vọt.
- Hệ thống cấp điện ngừng đột ngột vì những lí do khác. Giải pháp: Dùng bộ lưu điện để cấp điện ngay cho hệ thống máy tính quản trị CSDL khi mất điện đột ngột.

b) Sự cố hư hỏng thiết bị lưu trữ

Các thiết bị lưu trữ (ví dụ ổ đĩa cứng) có khả năng gặp sự cố. Khi đó, nói chung rất khó lấy lại được toàn bộ và chính xác dữ liệu trong thiết bị lưu trữ bị hỏng.

- Thiết bị lưu trữ bị hư hỏng vì quá tuổi thọ. Giải pháp: Quản lí thời gian sử dụng của thiết bị lưu trữ, thay thế trước khi thiết bị đến giai đoạn thường bị hư hỏng.

- Thiết bị lưu trữ bị hư hỏng vì các lí do khác. Giải pháp: Sao lưu dữ liệu định kì. Tất cả các hệ QTCSDL đều hỗ trợ khả năng sao lưu toàn bộ dữ liệu ra thiết bị dự phòng. Dùng giải pháp thiết bị lưu trữ hỗ trợ bảo vệ dữ liệu (các hãng sản xuất thiết bị lưu trữ có những giải pháp để lưu trữ hai phiên bản dữ liệu, kiểm tra chéo để đảm bảo tính chính xác của dữ liệu).

Tóm lại, tùy theo những yêu cầu cụ thể của mỗi tổ chức, đặc điểm về CSDL để xây dựng những chính sách đảm bảo an toàn dữ liệu. Trong đó cần quan tâm tới các sự cố có thể xảy ra và giải pháp hạn chế, khắc phục. Chính sách này cũng phải bao gồm những quy định về ý thức, trách nhiệm đối với những người vận hành hệ thống.

- Để đảm bảo an toàn dữ liệu cần xây dựng chính sách an toàn dữ liệu cùng kế hoạch xử lí các sự cố có thể xảy ra và giải pháp hạn chế, khắc phục. Chính sách an toàn dữ liệu cũng phải bao gồm những quy định về ý thức, trách nhiệm đối với người dùng và người vận hành hệ thống.
- Các hệ QTCSDL đều hỗ trợ chức năng sao lưu định kì và phục hồi dữ liệu từ bản sao lưu gần nhất.



Vì sao cần phải sao lưu dữ liệu định kì?



LUYỆN TẬP

1. Tại sao cần phải có những quy định về ý thức và trách nhiệm của người dùng đối với tài khoản của mình và dữ liệu trong CSDL?
2. Tại sao cần có những quy định về ý thức trách nhiệm của những người vận hành hệ thống?



VẬN DỤNG

Ở một trung tâm dạy tiếng Anh, có bốn giáo viên dạy bốn môn học là luyện nghe, luyện nói, luyện đọc, luyện viết. CSDL quản lí điểm học tập của học viên có các bảng là *diemnghe*, *diemnnoi*, *diemdoc*, *diemviet*. Các học viên được quyền chỉ xem các bảng điểm, các giáo viên được quyền thêm mới, cập nhật, xoá các bản ghi trong bảng điểm môn học mình dạy, chỉ một người dùng có toàn quyền đối với tất cả các bảng trong CSDL. Hãy xây dựng mô hình phân nhóm người dùng truy cập CSDL nói trên.