Thực trạng an ninh dữ liệu của doanh nghiệp, đặc biệt là các doanh nghiệp vận tải, logistics và đề xuất một số giải pháp khắc phục

■ **ThS. BÙI ĐÌNH VŨ**
Trường Đại học Hàng hải Việt Nam
Email: vubd@vimaru.edu.vn

TÓM TẮT: Hiện nay, an toàn dữ liệu của doanh nghiệp đang là vấn đề được quan tâm rất nhiều không chỉ trong nước mà cả quốc tế. Việc cơ sở dữ liệu (CSDL) của doanh nghiệp mất an toàn, để nhiều lỗ hổng sẽ là cơ hội để cho các hacker khai thác. Thực tế, nhiều doanh nghiệp trong nước hiện nay, đặc biệt là các doanh nghiệp vận tải, logistics mới chỉ tập trung vào việc bảo mật trên đường truyền mà ít quan tâm đến vấn đề bảo mật ngay trên CSDL của hệ quản trị CSDL. Hoặc ngay cả những vấn đề đơn giản như sao chép, export dữ liệu hoặc quyền truy cập người dùng tưởng như vô hại thì đó lại chính là những lỗ hổng đầy nguy hiểm. Bài báo tập trung vào thực trạng an ninh dữ liệu của doanh nghiệp và đề xuất một số nguyên tắc, biện pháp khắc phục.

TỪ KHÓA: An toàn dữ liệu, vận tải, logistics, cơ sở dữ liệu doanh nghiệp, biện pháp bảo mật cơ sở dữ liệu, trigger.

ABSTRACT: Currently, business data security is a very important issue not only domestically but also internationally. The loss of security of a business's database, leaving many vulnerabilities, will be an opportunity for hackers to exploit. In fact, many domestic businesses today, especially transportation and logistics businesses, only focus on security on the transmission line and pay little attention to security issues right on the database of the database management system. Or even simple problems such as copying, exporting data or seemingly harmless user access rights are dangerous vulnerabilities. This article focuses on the current state of enterprise data security and proposes some principles and remedies.

KEYWORDS: Data security, transportation, logistics, enterprise database, database security measures, trigger.

1. ĐẶT VẤN ĐỀ

CSDL của doanh nghiệp là vấn đề sống còn của doanh nghiệp, vì nó chứa nhiều thông tin về doanh nghiệp, về khách hàng - nơi trở thành mục tiêu hấp dẫn cho các tin tặc tấn công. Thực trạng cho thấy nhiều doanh nghiệp hiện nay mới chỉ quan tâm mức độ vừa phải hoặc không quan tâm đến vấn đề bảo mật CSDL của mình. Tin tặc tấn công vào CSDL của các hệ thống máy chủ của doanh nghiệp không chi vì phá hoại mà còn với nhiều mục đích khác nhau, trong đó có mục đích kiếm tiền.

CSDL có thể được nằm trên máy chủ mạng nội bộ hoặc trên nền tảng hệ thống máy chủ web. Với từng vị trí đều có nguy cơ bị tấn công với đa dạng hình thức, hình thức phổ biến nhất là tấn công kiểu SQL injection. Những nền tảng bảo mật của window, firewall hay bảo mật trên đường truyền vẫn chưa thật sự đủ mạnh.

Mặt khác, sự kết nối liên mạng ngày càng phát triển, tác dụng của các hàng rào bảo mật vành ngoài (network perimeter) ngày càng giảm nên vai trò của bảo mật CSDL nhanh chóng tăng lên. Vai trò quan trọng của bảo mật CSDL được xác lập một phần còn là nhờ sự ra đời của các quy định mới như Sarbanes-Oxley, PCI DSS…

Việc bảo mật CSDL của doanh nghiệp hiện nay không được tốt cũng vì nhiều lý do, trong đó:

Thứ nhất, họ chỉ tập trung bảo mật trên đường truyền, trên phần mềm ứng dụng có sẵn từ nhà phát triển.

Thứ hai, họ tin tưởng vào nền tảng bảo mật sẵn có của window.

Thứ ba, nhân viên IT chưa thật sự giỏi về công tác bảo mật.

2. CÁC NGUY CƠ ĐE DỌA CSDL CỦA DOANH NGHIỆP

Ngày nay, rất nhiều CSDL của doanh nghiệp bị tấn công vì những lỗ hổng trong các hệ thống quản trị CSDL như Micosoft SQL Server, Oracle... Hacker hoàn toàn có thể tạo ra các loại virus chuyên lây lan qua hệ quản trị CSDL và thậm chí là các rootkit trong bản thân hệ quản trị CSDL. Những mối đe dọa đó hầu như không thể ngăn chặn bằng các biện pháp phòng vệ "cổ điển" do tường lửa và các hệ thống IDS/IPS cung cấp, vì lỗ hổng bảo mật CSDL thường liên quan đến từng phiên bản cụ thể của mỗi hệ quản trị CSDL và thay đổi liên tục. Nhưng điều đó không có nghĩa là

CSDL chỉ có thể bị tấn công bằng những kỹ thuật cao cấp. Theo Top 20 - 2007 Security Risks của SANS Institute thì các lỗ hổng trên máy chủ CSDL thuộc nhóm 20 rủi ro bảo mật hàng đầu, trong đó những lỗ hổng thường gặp nhất là:

- Dùng cấu hình chuẩn với tên người dùng và mật khẩu mặc định;
- Tấn công SQL Injection qua công cụ của CSDL, ứng dụng thứ ba hay các ứng dụng web của người dùng;
- Dùng mật khẩu dễ dò tìm cho các tài khoản cao cấp;
- Các lỗi tràn bộ đệm trong các tiến trình "lắng nghe" các cổng phổ biến (ví dụ như listenr của Oracle với cổng 1521).

Điều đó chứng tỏ một thực tế là CSDL có thể bị tấn công bằng những phương pháp rất đơn giản. Nếu xét kỹ hơn, chúng ta sẽ thấy có rất nhiều lỗ hổng trong hệ thống CSDL do con người tự tạo ra. Dữ liệu của doanh nghiệp có thể nằm rải rác ở những điểm khác nhau bên ngoài máy chủ chính, đó có thể là các đĩa/băng lưu trữ, các máy chủ dự phòng hay máy chủ phục vụ nhu cầu báo cáo hay thậm chí là máy chủ dành cho phát triển/kiểm thử ứng dụng. Trong khi các hệ thống lưu trữ, dự phòng có thể cũng được bảo vệ nghiêm ngặt gần như các hệ thống chính thì CSDL cho phát triển và kiểm thử ứng dụng thường không được quan tâm nhiều. Đó là một lỗ hổng lớn vì các CSDL đó thường chứa cả những thông tin nhạy cảm như số dư, giao dịch thực tế của khách hàng nhưng lại có thể bị những nhóm người dùng đông đảo và không có thẩm quyền truy cập.

Một trường hợp nữa là hệ thống máy chủ chứa CSDL không được cài đặt phần mềm diệt virus an toàn dẫn đến nó dễ bị nhiễm mã độc thông qua email hoặc các đường link không chính thống xâm nhập... Các mã độc này có thể chiếm quyền điều khiển hệ quả trị CSDL của doanh nghiệp bằng cách tạo ra các tài khoản lạ và thay đổi hết mật khẩu của tất cả các tài khoản chính thống (chẳng hạn tài khoản sa của Microsoft SQL Server, tài khoản Sys của Oracle). Điều này đồng nghĩa hệ thống phần mềm của doanh nghiệp sẽ không thể truy cập vào được CSDL, ngược lại hacker có thể dùng các tài khoản lạ do chúng tạo ra để truy cập vào CSDL của doanh nghiệp.

3. ĐỀ XUẤT MỘT SỐ NGUYÊN TẮC VÀ BIỆN PHÁP BẢO MẬT CSDL

Cũng như công tác bảo mật nói chung, phòng ngự theo chiều sâu (defense-in-depth) và bảo vệ có trọng điểm là những nguyên tắc cơ bản của bảo mật CSDL. Để thực hiện được điều này, doanh nghiệp cần biết rõ họ đã triển khai những CSDL nào, chúng đang được sử dụng để lưu thông tin gì, chúng đang có những điểm yếu nào. Vì vậy, bảo mật CSDL phải bắt đầu bằng việc thu thập thông tin, phân loại và xác định mức độ ưu tiên.

Một biện pháp khá đơn giản và hiệu quả nhưng ít người chú ý thực hiện là gỡ bớt các mô-đun không cần thiết để giảm thiểu bình diện tấn công. Hầu hết các hệ quản trị CSDL hiện nay (đặc biệt là các phiên bản dành cho doanh nghiệp) đều chứa rất nhiều mô-đun hay tùy chọn với những công dụng mà bình thường ít dùng tới. Tất nhiên, càng có nhiều chức năng thì khả năng có lỗ hổng và bị lợi dụng để tấn công càng lớn. Vì vậy, hãy rà soát cấu hình CSDL theo định kỳ để loại bỏ những thành phần không cần thiết.

Với việc các lỗ hổng bảo mật của các hệ quản trị CSDL liên tiếp được phát hiện, công việc không thể bỏ qua đối với các doanh nghiệp là áp dụng các bản vá do các nhà cung cấp phân phối. Việc áp dụng các bản vá không đơn giản là tải xuống và cài đặt. Đối với các hệ quản trị CSDL, việc áp các bản vá còn phức tạp hơn nhiều so với các thiết bị mạng hay các ứng dụng phần mềm khác. Vì các CSDL là yếu tố sống còn của các hệ thống ứng dụng chính nên một sai sót nhỏ cũng có thể ảnh hưởng rất lớn. Trước khi cài đặt bất kỳ bản vá nào đều cần phải thử nghiệm thật cẩn thận và lên kế hoạch để đảm bảo hệ thống hoạt động ổn định sau khi triển khai cũng như giảm thiểu thời gian dừng (downtime).

Trong bảo mật CSDL, kiểm soát truy cập là yếu tố thiết yếu và điều đó phải được thực hiện dựa trên nguyên tắc quyền tối thiểu. Mỗi người dùng hay ứng dụng chỉ được phép có những quyền đủ để phục vụ cho công việc. Điều này không chỉ áp dụng cho quá trình phân quyền đầu tiên mà cần phải được kiểm tra định kỳ. Không ít doanh nghiệp cấp quyền truy cập sâu cho nhân viên tư vấn hay lập trình viên bên ngoài cho một dự án ngắn ngày nhưng lại quên không cắt hay thay đổi quyền khi công việc hoàn tất. Vì những quyền đọc có vẻ rất vô hại cũng có thể dùng làm bàn đạp cho những cuộc tấn công quy mô trong tương lai nên chúng ta cần xem xét việc phân quyền của cả những quyền nhỏ nhất. Bên cạnh đó, cần có biện pháp kiểm soát và theo dõi việc truy cập từ các phương tiện lưu trữ dữ liệu cũng như hạn chế những mối đe dọa đối với bảo mật CSDL từ quá trình phát triển và kiểm thử phần mềm. Phải đảm bảo dữ liệu thật không được dùng vào quá trình phát triển hay kiểm thử, CSDL dùng vào những công việc đó cũng không được nằm chung trên máy chủ chứa CSDL thật.

Mã hóa CSDL là biện pháp tiếp theo cần áp dụng để bảo mật CSDL, là lớp bảo vệ trong trường hợp các biện pháp kiểm soát truy cập đã bị vượt qua. Việc mã hóa này phải được thực hiện một cách đúng đắn để đảm bảo người dùng có toàn quyền trên hệ điều hành cũng không thể đọc được dữ liệu nếu không thông qua kiểm soát của ứng dụng. Yếu tố quan trọng đầu tiên cần xét đến trong quy trình mã hóa dữ liệu là quản lý khóa, nếu hệ thống quản lý khóa không đảm bảo thì tác dụng của mã hóa cũng giảm rất nhiều. Vấn đề cần lưu ý là lựa chọn phương án mã hóa như thế nào để đảm bảo an toàn thông tin mà không ảnh hưởng đến hiệu năng của hệ thống? Chúng ta sẽ xem xét một số lựa chọn. Nếu nhấn mạnh vấn đề bảo mật, có thể lựa chọn mã hóa tất cả các trường trừ trường mã số (ví dụ như mã khách hàng). Cách làm này chỉ có thể áp dụng nếu mọi yêu cầu truy cập CSDL (dù là truy vấn, thêm mới, cập nhật hay xóa) đều dựa trên trường mã số. Nếu có yêu cầu truy cập dữ liệu dựa trên các trường khác, ảnh hưởng của việc mã hóa/giải mã dữ liệu sẽ rất lớn (ví dụ như việc tìm kiếm theo tên khách hàng sẽ yêu cầu giải mã tất cả các bản ghi). Điều đó dẫn đến một phương án khác là chỉ mã

hóa những trường chứa dữ liệu nhạy cảm, cần bảo vệ như số thẻ tín dụng… Cách làm này chỉ ảnh hưởng đến những câu lệnh truy cập dựa trên số thẻ tín dụng. Nhưng rất có thể ứng dụng lại có chức năng tìm kiếm chỉ dựa trên số thẻ tín dụng. Vì vậy, trước khi quyết định mã hóa một trường dữ liệu nào đó, chúng ta cần xem xét các câu lệnh truy cập dữ liệu hay dùng để biết việc mã hóa ảnh hưởng thế nào đến hiệu năng của hệ thống.

Cần lưu ý rằng các hệ thống CSDL thường rất phức tạp vì chúng liên kết với nhiều ứng dụng khác nhau. Chỉ một lỗi trong một cấu phần cũng có thể làm lộ dữ liệu của hệ thống. Vì thế, việc bảo mật riêng CSDL là không đủ, tất cả các ứng dụng và cấu phần liên quan phải được bảo mật. Việc áp dụng hệ thống mã hóa trong suốt với người dùng cho tất cả các thiết bị nhớ di động khá phức tạp và tốn kém nhưng vẫn có thể coi là đơn giản nếu so với nhiệm vụ ngăn chặn rò rỉ thông tin.

Gần đây, trên thị trường đang nổi lên một mảng giải pháp và sản phẩm mới với tên gọi DLP (data loss prevention). Mặc dù còn nhiều tranh cãi nhưng các giải pháp đều có tâm điểm là hệ thống giám sát và lọc nội dung. Khả năng phân tích nội dung cho phép các công cụ rà soát mọi luồng thông tin trao đổi trên mạng cũng như dữ liệu nằm trên đĩa, gỡ bỏ các lớp vỏ (ví dụ như các bảng tính hay tệp PDF được nén) để xác định các thông tin nhạy cảm dựa trên chính sách bảo mật thông tin của doanh nghiệp. Bắt đầu với các công cụ giám sát nhằm phát hiện rò rỉ thông tin qua các kênh trao đổi phổ biến như thư điện tử, tin nhắn tức thời (IM), FTP và HTTP, các giải pháp DLP dần phát triển thêm những tính năng như rà soát các kho dữ liệu và các thư mục được chia sẻ trong mạng để phát hiện thông tin nhạy cảm chưa được bảo vệ, giám sát việc sử dụng dữ liệu trên máy tính của người dùng (ví dụ như chép tài liệu quan trọng ra thiết bị nhớ USB, cắt dán thông tin).

Giải pháp không cho mã độc tạo mới CSDL, tài khoản truy cập, thay đổi mật khẩu của tài khoản truy cập trên hệ quản trị CSDL là tạo các trigger ngăn chặn:

- Trigger ngăn chặn không cho phép tạo mới database:

```
IF EXISTS (SELECT * FROM sys.server_triggers
WHERE name = 't_DoNotAllowCreateDatabase')
DROP TRIGGER t_DoNotAllowCreateDatabase
ON ALL SERVER
GO
CREATE TRIGGER t_DoNotAllowCreateDatabase
ON ALL SERVER
FOR CREATE_DATABASE
AS
PRINT N'Phải DROP trigger t_
DoNotAllowCreateDatabase trước khi tạo mới database'
Rollback tran
GO
```

- Triger ngăn chặn không cho tạo mới login:

```
IF EXISTS (SELECT * FROM sys.server_triggers
WHERE name = 't_DoNotAllowCreateNewLogin')
DROP TRIGGER t_DoNotAllowCreateNewLogin
ON ALL SERVER
GO
CREATE TRIGGER t_DoNotAllowCreateNewLogin
ON ALL SERVER
FOR CREATE_LOGIN
AS
PRINT N'Phải DROP trigger t_
DoNotAllowCreateNewLogin trước khi tạo account'
Rollback tran
GO
```

- Trigger ngăn chặn không cho thay đổi login:

```
IF EXISTS (SELECT * FROM sys.server_triggers
WHERE name = 't_DoNotAllowAlterLogin')
DROP TRIGGER t_DoNotAllowAlterLogin
ON ALL SERVER
GO
CREATE TRIGGER t_DoNotAllowAlterLogin
ON ALL SERVER
FOR ALTER_LOGIN
AS
PRINT N'Phải DROP trigger t_DoNotAllowAlterLogin
trước khi sửa account'
Rollback tran
GO
```

- Trigger này sẽ ngăn chặn các lệnh DROP TABLE và ALTER TABLE:

```
Create trigger t_safety
on database
for CREATE_TABLE, DROP_TABLE
as
Print N'Phải xóa trigger t_safety trước khi ALTER hay
DROP bảng'
Rollback tran
```

4. KẾT LUẬN

An ninh dữ liệu là nhiệm vụ sống còn của doanh nghiệp, đặc biệt là các doanh nghiệp vận tải, logistics. Ngoài những cơ chế bảo mật thông thường như bảo mật môi trường mạng, doanh nghiệp phải nắm rõ môi trường bảo mật hiện hành và cần trú trọng đến công tác bảo mật trên hệ thống CSDL và những ứng dụng truy cập CSDL. Những giải pháp có thể giúp tốt cho việc bảo vệ CSDL của doanh nghiệp như:

- Kiểm soát đăng nhập;
- Mã hóa dữ liệu;
- Kiểm soát tốt những ứng dụng truy cập vào CSDL;
- Tạo trigger ngăn chặn những truy cập, phép toán trái phép.

Tài liệu tham khảo

[1]. Alfred Basta, Melissa Zgola (2011), *Database Security*, Cengage Learning, ISBN: 1133708145, 9781133708148.

Ngày nhận bài: 08/02/2024
Ngày nhận bài sửa: 01/3/2024
Ngày chấp nhận đăng: 18/3/2024