

Phụ lục III
Quy trình quản lý an toàn máy chủ và ứng dụng
(Kèm theo Quyết định số /QĐ-BNV ngày / /2024
của Bộ trưởng Bộ Nội vụ)

1. Quy trình quản lý an toàn máy chủ

Bước 1: Vị trí máy chủ an toàn

Đặt máy chủ ở vị trí an toàn, kiểm tra điều kiện lý tưởng cho máy chủ như: nhiệt độ; khoảng cách giữa các máy chủ và thiết bị; hệ thống lưu điện đảm bảo cho hệ thống hoạt động liên tục không bị gián đoạn. Vị trí đặt máy chủ phải có khoá và giới hạn người được phép vào ra.

Bước 2: Kiểm soát quyền truy cập

Các quyền truy cập ứng dụng, cấu hình, phần mềm trên máy chủ chỉ được cấp cho một người quản trị duy nhất. Hạn chế quyền truy cập vào máy chủ sẽ hạn chế khả năng máy chủ bị xâm nhập trái phép.

Bước 3: Thiết lập tường lửa

Trên thiết bị tường lửa chỉ mở cổng cần thiết cho máy chủ hoạt động đúng chức năng.

Bước 4: Quản lý cấu hình máy chủ

Trên máy chủ chỉ nên cài đặt các chức năng cần thiết cho máy chủ, không cài đặt nhiều chức năng trên cùng một máy chủ (AD, FTP Server, Web Server, DNS Server, ...). Các máy chủ nên thống nhất về cách đặt tên, mật khẩu, các máy chủ cùng vùng mạng nên có cùng một dải IP

Bước 5: Bảo mật tài khoản người dùng

Mật khẩu của người dùng phải bao gồm chữ hoa, chữ thường, số, ký tự đặc biệt, độ dài của mật khẩu phải trên 8 ký tự, không đặt mật khẩu dễ đoán (các ký tự liên tiếp nhau: 123456, abcde, trùng với tên tài khoản, trùng với ngày sinh nhật của quản trị viên, ...). Đảm bảo rằng tài khoản và mật khẩu chỉ duy nhất một quản trị viên biết.

Bước 6: Cài đặt các bản vá lỗ hổng bảo mật

Để đảm bảo an toàn cho máy chủ quản trị viên phải thường xuyên cập nhật bản vá lỗ hổng bảo mật cho hệ điều hành, ứng dụng, phần mềm theo khuyến cáo của các nhà cung cấp.

Bước 7: Gỡ bỏ các phần mềm không cần thiết

Việc cài đặt các phần mềm không cần thiết trên máy chủ sẽ dẫn đến mất an toàn thông tin, tin tặc rất dễ lợi dụng các lỗ hổng bảo mật của các phần mềm để tấn công hệ thống mạng, nên chỉ cài đặt các phần mềm thực sự cần thiết trên máy chủ.

Bước 8: Sao lưu dự phòng dữ liệu, cấu hình máy chủ

Sao lưu dự phòng dữ liệu, cấu hình máy chủ để đảm bảo các thông tin quan trọng không bị mất và dễ dàng phục hồi lại khi có sự cố về an toàn thông tin xảy ra.

Bước 9: Giám sát liên tục

Thường xuyên, liên tục giám sát các hoạt động của máy chủ, nhằm mục đích phát hiện các hành vi bất thường trên máy chủ như: Tài khoản lạ đăng nhập vào máy chủ, lưu lượng truy cập vào ra Internet tăng đột biến,...

2. Quy trình quản lý an toàn ứng dụng

Bước 1: Xác thực

- Thiết lập cấu hình ứng dụng để xác thực người sử dụng khi truy cập, quản trị, cấu hình ứng dụng;
- Lưu trữ có mã hoá thông tin xác thực hệ thống;
- Thiết lập cấu hình ứng dụng để đảm bảo an toàn mật khẩu người sử dụng, bao gồm các yêu cầu: Yêu cầu thay đổi mật khẩu mặc định; thiết lập quy tắc đặt mật khẩu về số ký tự, loại ký tự; thiết lập thời gian yêu cầu thay đổi mật khẩu; thiết lập thời gian mật khẩu hợp lệ;
- Hạn chế số lần đăng nhập sai trong khoảng thời gian nhất định với tài khoản nhất định;
- Mã hoá thông tin xác thực trước khi gửi qua môi trường mạng;
- Thiết lập cấu hình ứng dụng để ngăn cản việc đăng nhập tự động đối với các ứng dụng, dịch vụ cung cấp và xử lý dữ liệu quan trọng trong hệ thống.

Bước 2: Kiểm soát truy cập

- Thiết lập hệ thống chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị ứng dụng từ xa;
- Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi ứng dụng không nhận được yêu cầu từ người dùng;
- Giới hạn địa chỉ mạng quản trị được phép truy cập, quản trị ứng dụng từ xa;
- Phân quyền truy cập, quản trị, sử dụng tài nguyên khác nhau của ứng dụng với người sử dụng/ nhóm người sử dụng có chức năng, yêu cầu nghiệp vụ khác nhau;
- Giới hạn số lượng các kết nối đồng thời (kết nối khởi tạo và đã thiết lập) đối với các ứng dụng, dịch vụ máy chủ cung cấp.

Bước 3: Nhật ký hệ thống

- Ghi nhật ký hệ thống bao gồm những thông tin cơ bản sau: Thông tin truy cập ứng dụng; thông tin đăng nhập khi quản trị ứng dụng; thông tin các lỗi phát sinh trong quá trình hoạt động; thông tin thay đổi cấu hình ứng dụng;
- Quản lý và lưu trữ nhật ký hệ thống trên hệ thống quản lý tập trung;
- Nhật ký hệ thống phải được lưu trữ trong khoảng thời gian tối thiểu là 03 tháng.

Bước 4: Bảo mật thông tin liên lạc

- Mã hóa thông tin, dữ liệu (không phải là thông tin, dữ liệu công khai) trước khi truyền đưa, trao đổi qua môi trường mạng; sử dụng phương án mã hóa theo quy định về bảo vệ bí mật nhà nước đối với thông tin mật;

- Sử dụng kết nối mạng an toàn, bảo đảm an toàn trong quá trình khởi tạo kết nối kênh truyền và trao đổi thông tin qua kênh truyền.

Bước 5: Chống chối bỏ

Sử dụng chữ ký số khi trao đổi thông tin, dữ liệu quan trọng.

Bước 6: An toàn ứng dụng và mã nguồn

- Có chức năng kiểm tra tính hợp lệ của thông tin, dữ liệu đầu vào trước khi xử lý;

- Có chức năng kiểm tra tính hợp lệ của thông tin, dữ liệu đầu ra trước khi gửi về máy yêu cầu;

- Có phương án bảo vệ ứng dụng chống lại những dạng tấn công phổ biến: SQL Injection, OS command injection, RFI, LFI, Xpath injection, XSS, CSRF;

- Có chức năng kiểm soát lỗi, thông báo lỗi từ ứng dụng.