

Phụ lục II
Quy trình quản lý an toàn mạng
(Kèm theo Quyết định số /QĐ-BNV ngày / /2024
của Bộ trưởng Bộ Nội vụ)

Quy trình quản lý an toàn mạng của hệ thống thông tin được thực hiện thông qua các quy trình sau:

1. Quy trình Quản lý, vận hành hoạt động bình thường của hệ thống

Bước 1: Kiểm tra, đánh giá thiết bị mạng, hệ điều hành, phần mềm cài đặt trên các máy chủ hoạt động liên tục, ổn định và an toàn:

- Kiểm tra nhật ký hoạt động (log) của thiết bị mạng, hệ điều hành, phần mềm nhằm phát hiện ra các hành vi mất an toàn, an ninh thông tin (kiểm tra, phát hiện, loại bỏ các tài khoản người dùng lạ trên thiết bị mạng, máy chủ, phần mềm; kiểm tra hành vi của các tài khoản đăng nhập vào thiết bị mạng, máy chủ, phần mềm);

- Kiểm tra tình trạng hoạt động của CPU, RAM, Ổ cứng của máy chủ;

- Kiểm tra lưu lượng truy cập mạng của máy chủ, phần mềm.

Bước 2: Kiểm tra, cập nhật các bản vá lỗi của thiết bị phần cứng, hệ điều hành, phần mềm, từ nhà cung cấp.

Bước 3: Kiểm tra, loại bỏ các thành phần không cần thiết hoặc không sử dụng của hệ điều hành, phần mềm.

Bước 4: Kiểm tra đường truyền Internet: tốc độ mạng; lưu lượng mạng.

2. Cập nhật, sao lưu dự phòng và khôi phục hệ thống sau khi xảy ra sự cố

a. Cập nhật bản vá

Bước 1: Kiểm tra các bản cập nhật mới:

- Các nhà phát triển thường phát hành các bản cập nhật mới cho phần mềm, ứng dụng hoặc hệ điều hành thông qua các kênh chính thức như trang web của nhà phát triển;

- Qua báo cáo của Cục An toàn thông tin, Bộ Thông tin và Truyền thông gửi hàng tháng cho các Bộ, ngành, địa phương.

Bước 2: Sao lưu hệ thống trước khi cập nhật bản vá để tránh các trường hợp khi cài bản cập nhật mới sẽ xảy ra lỗi hệ thống, gây gián đoạn hệ thống. Trong trường hợp xảy ra lỗi sẽ khôi phục lại hệ thống lúc chưa cài bản cập nhật.

Bước 3: Tải xuống và cài đặt bản cập nhật: Sau khi đã xác định được các bản cập nhật cần thiết, tải xuống và cài đặt bản cập nhật.

Bước 4: Kiểm tra các bản cập nhật sau khi cài đặt: Sau khi cài đặt bản cập nhật, cần phải kiểm tra hệ thống hoạt động bình thường hay không.

b. Quy trình sao lưu dữ liệu

Bước 1: Xác định nguồn dữ liệu sao lưu (tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ và các dữ liệu quan trọng khác)

Người được giao quản lý hệ thống, cơ sở dữ liệu, mã nguồn thực hiện xác định nguồn dữ liệu cần lưu trữ để tiến hành sao lưu định kỳ.

Bước 2: Chuẩn bị, kiểm tra (Mạng, phương tiện lưu trữ, phần mềm lưu trữ,...).

Việc chuẩn bị nhằm bảo đảm an toàn, hạn chế tối đa lỗi có thể xảy ra trong quá trình tiến hành sao lưu.

Bước 3: Tiến hành sao lưu dữ liệu

Sau khi đã thực hiện xác định nguồn dữ liệu sao lưu và chuẩn bị các phương tiện lưu trữ, phần mềm để phục vụ việc sao lưu, người được giao quản lý hệ thống, cơ sở dữ liệu, mã nguồn tiến hành sao lưu dữ liệu cần thiết vào phương tiện lưu trữ.

Bước 4: Kiểm tra kết quả sao lưu dữ liệu

Sau khi hoàn thành quá trình sao lưu, người được giao quản lý hệ thống, cơ sở dữ liệu, mã nguồn thực hiện kiểm tra kết quả sao lưu. Trường hợp kết quả sao lưu không đạt yêu cầu thì quay lại Bước 2 để kiểm tra, tìm hướng khắc phục lỗi và báo cáo Lãnh đạo; Trường hợp việc sao lưu đạt yêu cầu thì chuyển phương tiện lưu trữ chứa dữ liệu sao lưu vào nơi bảo quản.

Bước 5: Bảo quản phương tiện lưu trữ.

- Việc tiêu hủy thiết bị, phương tiện lưu trữ phải bảo đảm yêu cầu bảo mật thông tin theo cấp độ được quy định.

- Việc rà soát, huỷ bỏ các thiết bị lưu trữ và các nội dung quá hạn được thực hiện vào tháng 12 hàng năm.

- Trưởng phòng có trách nhiệm quyết định thêm thời gian lưu trữ của các thiết bị đã hết hạn lưu giữ nếu thấy cần thiết. Xem xét phân loại các thiết bị lưu trữ đã hết hạn cần huỷ bỏ. Thiết bị hết hạn lưu phải được huỷ bỏ an toàn. Tuỳ theo tính cơ học của từng thiết bị lưu trữ và nội dung lưu trữ để xác định phương pháp huỷ, lập biên bản huỷ trình lãnh đạo phê duyệt huỷ.

- Việc tiêu hủy thiết bị lưu trữ và nội dung quá hạn phải được lập hồ sơ cho việc tiêu hủy bao gồm:

- + Quyết định tiêu hủy thiết bị lưu trữ và nội dung quá hạn.

- + Biên bản huỷ thiết bị lưu trữ và nội dung quá hạn.

- Hồ sơ về việc huỷ bỏ thiết bị lưu trữ và nội dung quá hạn phải được bảo quản tại Phòng Hành chính tổng hợp, Phòng QHTTTT ít nhất là 05 năm, kể từ ngày bị tiêu hủy.

- Phòng QHTTTT, Phòng Hành chính tổng hợp có nhiệm vụ rà soát các thiết bị lưu trữ và nội dung quá hạn báo cáo Lãnh đạo trung tâm và thành lập Hội đồng tiêu hủy.

Bước 6: Ghi nhật ký, lập hồ sơ.

Kết thúc quá trình sao lưu, người được giao quản lý hệ thống, cơ sở dữ liệu, mã nguồn của các Phòng ghi nhật ký quá trình sao lưu quy định theo Mẫu số 01, lập và lưu hồ sơ việc phục vụ hoạt động quản lý và theo dõi định kỳ.

c. Quy trình khôi phục hệ thống

Bước 1: Xác định sự cố tin học

Người được giao quản lý hệ thống, cơ sở dữ liệu, mã nguồn xác định nguyên nhân xảy ra sự cố tin học do lỗi phần cứng hoặc lỗi phần mềm để tìm hướng khắc phục.

Bước 2: Thực hiện cách ly, xử lý hệ thống, các dịch vụ bảo đảm an toàn, an ninh trước khi thực hiện phục hồi

Người được giao quản lý hệ thống, cơ sở dữ liệu, mã nguồn thực hiện cách ly máy chủ, dịch vụ hay cơ sở dữ liệu bằng cách sửa chữa, thay thế thiết bị, chặn tấn công xâm nhập mạng, tắt tiến trình phần mềm, rà quét bóc gỡ mã độc,... bảo đảm cho hệ thống được vận hành bình thường.

Bước 3: Xác định trường hợp cần phục hồi

Người được giao quản lý hệ thống, cơ sở dữ liệu, mã nguồn cần xác định trường hợp phục hồi là do sự cố hệ thống, phần cứng hay dữ liệu, phần mềm quản trị cơ sở dữ liệu, phần mềm ứng dụng để từ đó đưa ra cách phục hồi nhanh chóng, chính xác.

Bước 4: Xác định nguồn cơ sở dữ liệu tài liệu lưu trữ phục hồi

Người được giao quản lý hệ thống, cơ sở dữ liệu, mã nguồn xác định và lấy bản sao lưu dự phòng gần nhất trước thời điểm xảy ra sự cố để tiến hành phục hồi.

Bước 5: Tiến hành phục hồi

Người được giao quản lý hệ thống, cơ sở dữ liệu, mã nguồn thực hiện khôi phục lại phần mềm ứng dụng bằng cách sử dụng phần mềm ứng dụng đã được sao lưu gần nhất trước thời điểm xảy ra sự cố.

Bước 6: Kiểm tra kết quả phục hồi

Khi hệ thống hoạt động trở lại bình thường, người được giao quản lý hệ thống, cơ sở dữ liệu, mã nguồn thực hiện kiểm tra dữ liệu để bảo đảm dữ liệu sau khi phục hồi hoàn toàn đầy đủ, chính xác so với trước thời điểm xảy ra sự cố. Trường hợp dữ liệu không đạt yêu cầu thì quay lại Bước 4 để kiểm tra nguồn dữ liệu phục hồi; Trường hợp đạt yêu cầu thì tiến hành chuyển sang bước tiếp theo.

Bước 7: Ghi biên bản, lập hồ sơ.

3. Truy cập và quản lý cấu hình hệ thống

Bước 1: Xác định cấu hình:

- Xác định tất cả các thành phần cấu tạo nên hệ thống, bao gồm phần cứng, phần mềm, mạng và dữ liệu;

- Thu thập thông tin chi tiết về từng thành phần, chẳng hạn như tên, nhà cung cấp, phiên bản, v.v;
- Lưu trữ thông tin cấu hình trong một kho lưu trữ trung tâm.

Bước 2: Theo dõi cấu hình:

- Theo dõi các thay đổi đối với cấu hình hệ thống;
- Ghi lại lịch sử thay đổi, bao gồm ai đã thực hiện thay đổi, khi nào thay đổi được thực hiện và thay đổi gì đã được thực hiện;
- Lưu trữ lịch sử thay đổi trong kho lưu trữ trung tâm.

Bước 3: Kiểm soát cấu hình:

- Xác định các chính sách và quy trình để quản lý thay đổi đối với cấu hình hệ thống;
- Yêu cầu phê duyệt cho các thay đổi cấu hình trước khi được thực hiện;
- Kiểm tra các thay đổi cấu hình để đảm bảo rằng chúng đáp ứng các yêu cầu kinh doanh và không gây ra sự cố.

Triển khai các thay đổi cấu hình một cách có kiểm soát.

Bước 4: Báo cáo cấu hình:

- Tạo các báo cáo về cấu hình hệ thống;
- Sử dụng các báo cáo này để theo dõi trạng thái của hệ thống và xác định các nguy cơ tiềm ẩn;
- Sử dụng các báo cáo này để cải thiện hiệu suất của hệ thống.

NHẬT KÝ SAO LƯU DỰ PHÒNG DỮ LIỆU

ĐƠN VỊ
PHÒNG.....

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập – Tự do – Hạnh phúc

NHẬT KÝ SAO LƯU DỰ PHÒNG DỮ LIỆU

STT	Người Thực hiện	Ứng dụng/Dịch vụ/Máy chủ	Hình thức Sao lưu, Phục hồi dữ liệu	Thời gian thực hiện	Kết quả thực hiện	Mô tả file/Thư mục	Phương tiện lưu trữ

Người ghi nhật ký