

Phụ lục VII
Quy trình quản lý giám sát an toàn hệ thống thông tin
(Kèm theo Quyết định số /QĐ-BNV ngày / /2024
của Bộ trưởng Bộ Nội vụ)

Bước 1: Tiếp nhận, phân tích, đánh giá cảnh báo

- Nhân sự trực giám sát an toàn thông tin tiếp nhận cảnh báo từ: hệ thống vận hành an toàn thông tin; thông báo thông tin về cảnh báo sự cố cho nhân sự quản trị hệ thống;

- Đơn vị phụ trách hệ thống giám sát an toàn thông tin: Thu thập bổ sung các sự kiện, thông tin liên quan đến cảnh báo; phân tích, đánh giá xác định hệ thống có bị tấn công hay không;

Trong trường hợp xác định hệ thống không bị tấn công, chuyển Bước 2, hệ thống bị tấn công, chuyển Bước 3.

Bước 2: Đóng cảnh báo

Đối với cảnh báo được nhân sự trực giám sát phân tích đánh giá:

- Không có tấn công do liên quan tới nghiệp vụ quản trị, tác động của quản trị viên hệ thống được thông báo trước;

- Các hành vi được phép và không được phép của hệ thống giám sát bất rộng hoặc chưa tối ưu dẫn tới cảnh báo sai;

Nhân sự trực giám sát thực hiện đóng cảnh báo với đầy đủ các thông tin đã xác minh. Hành động này để ghi nhận giúp đánh giá chất lượng của các hành vi được phép và không được phép phát sinh cảnh báo, từ đó triển khai các hoạt động tối ưu các hành vi được phép và không được phép không đảm bảo chất lượng.

Bước 3: Xác định trường hợp cảnh báo an toàn thông tin mạng cần được xử lý

Chuẩn bị các trường hợp có thể xảy ra xác minh thêm thông tin về hành vi hoặc phản ứng ngăn chặn tấn công đang nhằm vào hệ thống nhưng chưa thành công hoặc các hành động khắc phục khi tấn công thành công.

Hệ thống có bị tấn công nhưng chưa thành công hoặc chưa xác định (cần xác minh thêm) chuyển Bước 4. Nếu hệ thống bị tấn công thành công, chuyển Bước 8.

Bước 4: Trên hệ thống giám sát tạo cảnh báo cho cán bộ quản trị hệ thống

Bộ phận trực giám sát tạo cảnh báo mô tả rõ thông tin cho cán bộ quản trị hệ thống cần thực hiện:

- Xác minh hành vi tác động vào hệ thống: Tùy theo thông tin cảnh báo, cần xác minh hành vi liên quan đến nghiệp vụ quản trị, khai thác hoặc tác động của cán bộ quản trị hệ thống;

- Phản ứng tấn công: Căn cứ vào loại tấn công để đưa ra phương án ngăn chặn phù hợp, bao gồm các phương án:

- + Chặn IP đang thực hiện tấn công dò quét từ Internet;
- + Thiết lập luật chặn thư điện tử theo người gửi, tiêu đề,...

Bước 5: Xử lý cảnh báo

Cán bộ quản trị hệ thống thực hiện xử lý cảnh báo trong phạm vi nghiệp vụ quản trị, vận hành theo yêu cầu của bộ phận trực giám sát được mô tả, hướng dẫn trong cảnh báo.

Bước 6: Cập nhật kết quả xử lý và đóng cảnh báo

Cán bộ quản trị hệ thống thực hiện xử lý cảnh báo theo nghiệp vụ quản trị và vận hành. Cập nhật chi tiết thông tin đã xác minh, xử lý vào cảnh báo. Đóng cảnh báo xác nhận hoàn thành xử lý.

Bộ phận trực giám sát kiểm tra lại kết quả xử lý cảnh báo của cán bộ quản trị hệ thống.

Trường hợp cảnh báo tấn công chưa được ngăn chặn triệt để, quay lại Bước 4. Nếu tấn công đã được ngăn chặn thành công, hoặc hành vi liên quan nghiệp vụ quản trị chuyển Bước 7.

Dựa vào kết quả xác minh nghiệp vụ của cán bộ quản trị hệ thống, đánh giá có sự cố, chuyển Bước 8.

Bước 7: Đóng cảnh báo

Bộ phận trực giám sát thực hiện đóng cảnh báo kết thúc quy trình xử lý cảnh báo.

Bước 8: Xác định mức độ sự cố

Mức độ nghiêm trọng của sự cố được quy định trong bảng dưới đây:

| Phạm vi Mức độ | Toàn hệ thống | Nhiều hệ thống, dịch vụ hoặc toàn bộ site | Một hệ thống, dịch vụ | Người dùng cá nhân |
|---|----------------------|--|------------------------------|---------------------------|
| Gián đoạn dịch vụ/Lộ lọt thông tin | Nghiêm trọng | Nghiêm trọng | Cao | Trung bình |
| Ảnh hưởng hiệu năng dịch vụ | Cao | Cao | Trung bình | Thấp |
| Không ảnh hưởng dịch vụ | Trung bình | Trung bình | Thấp | Thấp |

Bước 9: Báo cáo sự cố

Hàng tháng bộ phận giám sát an toàn thông tin lập báo cáo sự cố đã xảy ra trong tháng gửi Giám đốc Trung tâm Thông tin.