BỘ THÔNG TIN VÀ TRUYỀN THÔNG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
	Độc lập - Tự do - Hạnh phúc
Số: 31 /2017/TT-BTTTT	*Hà Nội, ngày 15 tháng 11 năm 2017*

THÔNG TƯ

Quy định hoạt động giám sát an toàn hệ thống thông tin

Căn cứ Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015;

Căn cứ Nghị định số 72/2013/NĐ-CP ngày 15 tháng 7 năm 2013 của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng;

Căn cứ Nghị định số 25/2014/NĐ-CP ngày 07 tháng 4 năm 2014 của Chính phủ quy định về phòng, chống tội phạm và vi phạm pháp luật khác có sử dụng công nghệ cao;

Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01 tháng 07 năm 2016 của Chính phủ về bảo đảm an toàn thông tin theo cấp độ;

Căn cứ Nghị định số 17/2017/NĐ-CP ngày 17 tháng 02 năm 2017 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Thông tin và Truyền thông;

Căn cứ Quyết định 05/2017/QĐ-TTg ngày 16 tháng 3 năm 2017 của Thủ tướng Chính phủ ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia;

Thực hiện Nghị quyết 36a/NQ-CP ngày 14 tháng 10 năm 2015 của Chính phủ về Chính phủ điện tử;

Theo đề nghị của Giám đốc Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam,

Bộ trưởng Bộ Thông tin và Truyền thông ban hành Thông tư quy định hoạt động giám sát an toàn hệ thống thông tin.

Chương I

QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Thông tư này quy định về hoạt động giám sát an toàn hệ thống thông tin (sau đây gọi tắt là giám sát) trên toàn quốc, không bao gồm các hệ thống thông tin do Bộ Quốc phòng và Bộ Công an quản lý.

Điều 2. Đối tượng áp dụng

Thông tư này áp dụng đối với cơ quan, tổ chức, doanh nghiệp, cá nhân trực tiếp tham gia hoặc có liên quan đến hoạt động giám sát trên toàn quốc.

Chương II

GIÁM SÁT AN TOÀN HỆ THỐNG THÔNG TIN

Điều 3. Nguyên tắc giám sát

1. Đảm bảo được thực hiện thường xuyên, liên tục.

2. Chủ động theo dõi, phân tích, phòng ngừa để kịp thời phát hiện, ngăn chặn rủi ro, sự cố an toàn thông tin mạng.

3. Đảm bảo hoạt động ổn định, bí mật cho thông tin được cung cấp, trao đổi trong quá trình giám sát.

4. Có sự điều phối, kết hợp chặt chẽ, hiệu quả giữa hoạt động giám sát của Bộ Thông tin và Truyền thông và hoạt động giám sát của chủ quản hệ thống thông tin; từng bước xây dựng khả năng liên thông giữa hệ thống giám sát của Bộ Thông tin và Truyền thông và hệ thống giám sát của chủ quản hệ thống thông tin trên phạm vi toàn quốc.

Điều 4. Phương thức giám sát

1. Giám sát được thực hiện qua phương thức giám sát trực tiếp hoặc phương thức giám sát gián tiếp. Chủ quản hệ thống thông tin có thể trực tiếp triển khai hoặc thuê dịch vụ giám sát. Trong trường hợp cần thiết, căn cứ vào năng lực, tình hình và nguồn lực thực tế chủ quản hệ thống thông tin đề nghị các đơn vị chức năng liên quan của Bộ Thông tin và Truyền thông hỗ trợ giám sát phù hợp với nguồn lực thực tế.

2. Giám sát trực tiếp là hoạt động giám sát được tiến hành bằng cách đặt các thiết bị có chức năng phân tích luồng dữ liệu (quan trắc), thu nhận trực tiếp thông tin nhật ký, cảnh báo hệ thống được giám sát để phát hiện ra các dấu hiệu tấn công, rủi ro, sự cố an toàn thông tin mạng. Giám sát trực tiếp bao gồm các hoạt động sau:

a) Phân tích, thu thập các thông tin an toàn thông tin mạng:

- Phân tích, quan trắc an toàn thông tin mạng trên đường truyền mạng/luồng thông tin tại các cổng kết nối Internet bằng các công cụ có khả năng phân tích đường truyền mạng để phát hiện tấn công, rủi ro, sự cố an toàn thông tin mạng như thiết bị phát hiện/ngăn ngừa tấn công phù hợp với đối tượng được giám sát (ví dụ: IDS/IPS/Web Firewall v.v...);

- Thu thập nhật ký (log file), cảnh báo an toàn thông tin mạng phản ánh hoạt động các ứng dụng, hệ thống thông tin, thiết bị an toàn thông tin.

b) Tổng hợp, đồng bộ, xác minh và xử lý các thông tin an toàn thông tinmạng để phát hiện ra các tấn công, rủi ro, sự cố an toàn thông tin mạng hoặc loại bỏ các thông tin không chính xác.

3. Giám sát gián tiếp là hoạt động giám sát thực hiện các kỹ thuật thu thập thông tin từ các nguồn thông tin có liên quan; kiểm tra, rà soát đối tượng cần giám sát để phát hiện tình trạng hoạt động, khả năng đáp ứng và kết hợp với một số yếu tố khác có liên quan để phân tích nhằm phát hiện ra các tấn công, rủi ro, sự cố an toàn thông tin mạng. Giám sát gián tiếp bao gồm các hoạt động sau:

a) Thu thập, phân tích, xác minh các thông tin về tấn công, rủi ro, sự cố an toàn thông tin mạng liên quan đến đối tượng giám sát từ các nguồn thông tin có liên quan;

b) Kiểm tra, rà soát từ xa hoặc trực tiếp các đối tượng được giám sát để đánh giá tình trạng, phát hiện tấn công, rủi ro, sự cố an toàn thông tin mạng có khả năng bị khai thác, tấn công, gây hại.

Điều 5. Yêu cầu giám sát trực tiếp đối với chủ quản hệ thống thông tin

Chủ quản hệ thống thông tin có trách nhiệm chủ động thực hiện giám sát theo quy định hiện hành. Đối với hệ thống thông tin cấp độ 3 trở lên, hoạt động giám sát của chủ quản hệ thống thông tin cần đáp ứng các yêu cầu tối thiểu sau đây:

1. Thành phần giám sát trung tâm của chủ quản hệ thống thông tin cần đáp ứng các yêu cầu sau:

a) Cung cấp đầy đủ các tính năng thu thập và tổng hợp các thông tin an toàn thông tin mạng;

b) Phân tích các thông tin thu thập để phát hiện và cảnh báo tấn công, rủi ro, sự cố an toàn thông tin mạng có khả năng ảnh hưởng tới hoạt động hệ thống hoặc khả năng cung cấp các dịch vụ của hệ thống thông tin được giám sát;

c) Cung cấp giao diện thuận tiện cho việc theo dõi, giám sát liên tục của cán bộ giám sát;

d) Thực hiện thu thập và phân tích các thông tin đầu vào tối thiểu sau đây: nhật ký máy chủ web (web server) với các ứng dụng web (ví dụ: cổng thông tin điệntử, dịch vụ công trực tuyến v.v...); cảnh báo/nhật ký của thiết bị quan trắc cơ sở; cảnh báo/nhật ký của thiết bị tường lửa được thiết lập bảo vệ luồng kết nối

mạng Internet liên quan đến các đối tượng cần giám sát;

e) Năng lực xử lý thành phần giám sát trung tâm của chủ quản hệ thống thông tin cần phù hợp với khối lượng, định dạng và có khả năng phân tích thông tin an toàn thông tin mạng thu thập từ các hệ thống được giám sát.

2. Thu thập thông tin an toàn thông tin mạng và quan trắc cơ sở cần đáp ứng các yêu cầu sau:

a) Thực hiện thu thập thông tin an toàn thông tin mạng từ nhật ký và cảnh báo của các phần mềm/thiết bị liên quan đến đối tượng cần giám sát để cung cấp cho thành phần giám sát trung tâm của chủ quản hệ thống thông tin hoặc theo yêu cầu của cơ quan chức năng thuộc Bộ Thông tin và Truyền thông. Các thông tin an toàn thông tin mạng tối thiểu cần thu thập và cung cấp bao gồm: nhật ký máy chủ web (web server) của các ứng dụng web (ví dụ: cổng thông tin điện tử, dịch vụ công trực tuyến v.v...); cảnh báo/nhật ký của thiết bị quan trắc cơ sở; cảnh báo/nhật ký của thiết bị tường lửa được thiết lập bảo vệ luồng kết nối mạng Internet liên quan đến các đối tượng cần giám sát;

b) Các thiết bị quan trắc cơ sở đảm bảo các chức năng phát hiện tấn công, rủi ro, sự cố an toàn thông tin mạng; cần được thiết lập để đảm bảo khả năng giám sát bao phủ được tất cả các đường kết nối mạng Internet của đối tượng cần giám sát;

c) Thiết bị quan trắc cần đáp ứng tối thiểu các chức năng phát hiện, tạo lập luật phát hiện tấn công riêng dựa trên các thông tin như: địa chỉ IP nguồn, địa chỉ IP đích, địa chỉ cổng nguồn, địa chỉ cổng đích, các đoạn dữ liệu đặc biệt trong gói tin được truyền qua. Đối với các cơ quan, tổ chức nhà nước tự triển khai thiết bị quan trắc cơ sở, ưu tiên sử dụng các thiết bị phát hiện tấn công đã có (ví dụ: IDS, IPS, tường lửa Web,v.v...) để kết hợp làm thiết bị quan trắc cơ sở;

d) Đối với các hệ thống thông tin phục vụ Chính phủ điện tử sử dụng giao thức có mã hóa (ví dụ: https), cần có phương án kỹ thuật đảm bảo thiết bị quan trắc an toàn thông tin mạng có được đầy đủ thông tin để có thể phát hiện được các tấn công, rủi ro, sự cố an toàn thông tin mạng;

e) Thiết lập, kết nối các thiết bị quan trắc cơ sở với hệ thống giám sát của Bộ Thông tin và Truyền thông theo hướng dẫn và yêu cầu của cơ quan chức năng.

3. Nội dung thực hiện giám sát:

a) Theo dõi, trực giám sát liên tục, lập báo cáo hàng ngày, đảm bảo hệ

thống giám sát của chủ quản hệ thống thông tin hoạt động và thu thập thông tin ổn định, liên tục;

b) Xây dựng và ban hành các quy chế giám sát an toàn thông tin mạng, trong đó quy định cụ thể về thời hạn định kỳ thống kê kết quả xử lý, lập báo cáo;

c) Theo dõi, vận hành các thiết bị quan trắc cơ sở đảm bảo ổn định, liên tục, điều chỉnh kịp thời khi có các thay đổi và thực hiện đầy đủ các hướng dẫn của Bộ Thông tin và Truyền thông để đảm bảo hiệu quả giám sát;

d) Lập báo cáo kết quả giám sát hàng tuần để báo cáo chủ quản hệ thống thông tin, nội dung báo cáo tuần bao gồm đầy đủ các thông tin sau: thời gian giám sát; danh mục đối tượng bị tấn công cần chú ý (địa chỉ IP, mô tả dịch vụ cung cấp, thời điểm bị tấn công); kỹ thuật tấn công đã phát hiện được và chứng cứ liên quan; các đối tượng thực hiện tấn công; các thay đổi trong hệ thống được giám sát và hệ thống giám sát; v.v...;

đ) Tiến hành phân loại nguy cơ, rủi ro, sự cố an toàn thông tin mạng tuỳ theo tình hình cụ thể;

e) Định kỳ thống kê kết quả xử lý nguy cơ, rủi ro, sự cố an toàn thông tin mạng để phục vụ công tác lưu trữ, báo cáo;

g) Trong trường hợp chủ quản hệ thống thông tin đề nghị đơn vị chức năng của Bộ Thông tin và Truyền thông thực hiện giám sát cơ sở hoặc hệ thống thuộc trách nhiệm giám sát của Bộ Thông tin và Truyền thông, chủ quản hệ thống thông tin có trách nhiệm cung cấp và cập nhật thông tin về hệ thống thông tin cần giám sát và mô tả phương án kỹ thuật triển khai hệ thống giám sát của chủ quản hệ thống thông tin cho Bộ Thông tin và Truyền thông theo mẫu phiếu cung cấp thông tin tại Phụ lục 1, trong đó có các thông tin:

- Mô tả đối tượng được giám sát, bao gồm các thông tin cơ bản sau đây: địa chỉ IP, tên miền, dịch vụ cung cấp, tên và phiên bản hệ điều hành, phần mềm ứng dụng web;

- Vị trí đặt hệ thống giám sát của chủ quản hệ thống thông tin, dung lượng các đường truyền kết nối vào đối tượng giám sát của chủ quản hệ thống thông tin, các thông tin dự kiến thu thập và giao thức thu thập, ví dụ cảnh báo của IDS, nhật ký tường lửa (log firewall), nhật ký máy chủ web (log web server), v.v...

h) Năng lực lưu trữ thông tin giám sát tối thiểu đạt mức trung bình 30 ngày hoạt động trong điều kiện bình thường;

i) Cung cấp thông tin giám sát theo định kỳ hoặc đột xuất có yêu cầu của Bộ Thông tin và Truyền thông theo quy định của pháp luật;