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 tậm 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;

k) Báo cáo hoạt động giám sát của chủ quản hệ thống thông tin định kỳ 06 tháng theo mẫu tại Phụ lục 2.

Điều 6. Hoạt động giám sát của doanh nghiệp

Doanh nghiệp viễn thông, doanh nghiệp cung cấp dịch vụ công nghệ thông tin, doanh nghiệp cung cấp dịch vụ an toàn thông tin mạng có trách nhiệm:

1. Phối hợp với chủ quản hệ thống thông tin trong việc giám sát theo yêu cầu của Bộ Thông tin và Truyền thông.

2. Cung cấp các thông tin về hạ tầng, kỹ thuật, hệ thống mạng và thực hiện các hỗ trợ kỹ thuật theo yêu cầu của Bộ Thông tin và Truyền thông phục vụ cho hoạt động giám sát của Bộ Thông tin và Truyền thông.

3. Thực hiện các nhiệm vụ giám sát theo quy định tại Điều 7 Quyết định số 05/2017/QĐ-TTg của Thủ tướng Chính phủ.

Điều 7. Đầu mối giám sát, cảnh báo

1. Chủ quản hệ thống thông tin có trách nhiệm cử cá nhân hoặc bộ phận làm đầu mối giám sát, cảnh báo an toàn thông tin mạng để phối hợp với đơn vị chức năng của Bộ Thông tin và Truyền thông.

2. Đầu mối giám sát phải đảm bảo khả năng cung cấp, tiếp nhận thông tin kịp thời, liên tục. Đầu mối giám sát có chức năng thực hiện hoạt động giám sát trong phạm vi hệ thống thông tin của mình.

3. Đầu mối giám sát thực hiện cung cấp, trao đổi thông tin theo một hay đồng thời nhiều cách như công văn, thư điện tử, điện thoại, fax, hoặc trao đổi trên một phần mềm trao đổi thông tin chuyên biệt nhằm đảm bảo thông tin được bảo mật.

4. Thông tin đầu mối giám sát bao gồm: Họ tên cá nhân, tên bộ phận, chức vụ, địa chỉ, số điện thoại (cố định và di động), địa chỉ thư điện tử, chữ ký số (nếu đã có).

Điều 8. Trao đổi, cung cấp, chia sẻ thông tin

1. Khuyến khích các đầu mối giám sát trao đổi, cung cấp thông tin cho nhau nhằm mục đích phối hợp trong công tác giám sát, cảnh báo, ứng cứu sự cố và tăng tính chủ động đối phó với các nguy cơ, mối đe dọa, phương thức, thủ đoạn tấn công an toàn thông tin mạng của tổ chức, cá nhân.

2. Các thông tin chia sẻ, cung cấp và trao đổi bao gồm các thông tin về tấn công, rủi ro, sự cố an toàn thông tin mạng; các phương thức, thủ đoạn, nguồn

gốc tấn công; các tác động, ảnh hưởng do sự cố gây ra; biện pháp quản lý, kỹ thuật để xử lý, khắc phục.

3. Nguyên tắc trao đổi, cung cấp thông tin

a) Kịp thời, chính xác và áp dụng các biện pháp quản lý, kỹ thuật phù hợp để bảo mật thông tin trao đổi;

b) Chủ động xác minh thông tin trao đổi nhằm đảm bảo tính xác thực của thông tin;

c) Sử dụng một hoặc đồng thời nhiều hình thức trao đổi thông tin như website, công văn, thư điện tử, tin nhắn, điện thoại, fax;

d) Khi cung cấp, trao đổi thông tin với đơn vị chức năng của Bộ Thông tin và Truyền thông cần thực hiện theo hướng dẫn của Bộ Thông tin và Truyền thông.

Điều 9. Hoạt động nâng cao năng lực giám sát

1. Tổ chức giao ban, hội thảo định kỳ về hoạt động giám sát.

2. Bồi dưỡng, huấn luyện, diễn tập nhằm nâng cao năng lực giám sát.

3. Đôn đốc, kiểm tra việc thực hiện hoạt động giám sát, cảnh báo của các bộ phận chuyên trách về an toàn thông tin mạng.

4. Chia sẻ kiến thức, kinh nghiệm về giám sát, cảnh báo, ứng cứu sự cố.

5. Nghiên cứu, xây dựng các công cụ hỗ trợ hoạt động phối hợp, trao đổi thông tin trong công tác giám sát, cảnh báo, ứng cứu sự cố.

6. Phát triển các sản phẩm, dịch vụ giám sát, phân tích, cảnh báo chuyên sâu cho từng đối tượng giám sát cụ thể.

7. Thúc đẩy xây dựng các thỏa thuận hợp tác song phương, đa phương giữa bộ phận chuyên trách về an toàn thông tin mạng nhằm nâng cao năng lực giám sát, cảnh báo.

8. Tăng cường hợp tác quốc tế trong công tác giám sát, cảnh báo, ứng cứu sự cố.

Chương III

HOẠT ĐỘNG GIÁM SÁT CỦA BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Điều 10. Mô hình giám sát của Bộ Thông tin và Truyền thông

1. Hoạt động giám sát trung tâm:

a) Là việc thu thập, theo dõi, phát hiện, phân tích, xử lý, báo cáo, thu thập

chứng cứ về các dấu hiệu tấn công, rủi ro, sự cố an toàn thông tin mạng dựa trên các dữ liệu/thông tin an toàn thông tin mạng được thu thập bởi giám sát trực tiếp thông qua các hệ thống quan trắc cơ sở hoặc giám sát gián tiếp, đồng thời thực hiện việc lưu trữ các dữ liệu thu thập được dưới dạng sự kiện và quản lý tập trung các hệ thống quan trắc cơ sở;

b) Được thực hiện thông qua các Hệ thống giám sát các sự cố an toàn mạng và Hệ thống xử lý tấn công mạng Internet Việt Nam do các đơn vị chức năng của Bộ Thông tin và Truyền thông quản lý và vận hành trên nguyên tắc chia sẻ dữ liệu, hoạt động liên thông để nâng cao hiệu quả giám sát.

2. Hệ thống quan trắc cơ sở

a) Là tập hợp các thiết bị, phần mềm có khả năng theo dõi, thu thập, phân tích, cung cấp thông tin nhật ký, trạng thái, cảnh báo cho hoạt động giám sát trung tâm phục vụ cho việc phân tích, phát hiện các sự cố, điểm yếu, nguy cơ, lỗ hổng an toàn thông tin mạng;

b) Được cung cấp các điều kiện kỹ thuật và vị trí đặt phù hợp cho việc hoạt động, thu thập dữ liệu từ đối tượng giám sát theo hướng dẫn của đơn vị chức năng của Bộ Thông tin và Truyền thông;

c) Do đơn vị chức năng của Bộ Thông tin và Truyền thông chủ trì, phối hợp với chủ quản hệ thống thông tin xây dựng, thiết lập, quản lý và vận hành theo quy định pháp luật;

d) Thiết bị/phần mềm thực hiện quan trắc cơ sở được thiết lập để kết nối và phục vụ cho hoạt động giám sát trung tâm dựa trên các tiêu chuẩn, quy chuẩn kỹ thuật hoặc hướng dẫn nghiệp vụ của Bộ Thông tin và Truyền thông.

Điều 11. Hoạt động giám sát của Bộ Thông tin và Truyền thông

1. Bộ Thông tin và Truyền thông thực hiện giám sát hệ thống, dịch vụ công nghệ thông tin phục vụ Chính phủ điện tử.

2. Theo đề nghị của chủ quản hệ thống thông tin, Bộ Thông tin và Truyền thông tổ chức thực hiện giám sát đối với hệ thống thông tin thuộc lĩnh vực quan trọng cần ưu tiên đảm bảo an toàn thông tin mạng phù hợp với nguồn lực thực tế.

3. Hoạt động giám sát trung tâm của Bộ Thông tin và Truyền thông đảm bảo có khả năng tiếp nhận, phân tích thông tin giám sát thu thập được từ hệ thống quan trắc cơ sở và các thiết bị, hệ thống phục vụ giám sát gián tiếp.

4. Hoạt động giám sát của Bộ Thông tin và Truyền thông bao gồm:

a) Lựa chọn, quản lý, cập nhật danh sách đối tượng giám sát quy định tại

Thông tư này và các văn bản pháp luật có liên quan;

b) Theo dõi, trực trung tâm giám sát, lập báo cáo phân tích giám sát; kiểm tra, đôn đốc công tác theo dõi, trực giám sát;

c) Tổng hợp, lưu trữ, phân tích, phân loại thông tin, dữ liệu thu thập được từ các hệ thống quan trắc cơ sở, các thiết bị, hệ thống phục vụ giám sát gián tiếp và các nguồn thông tin khác;

d) Thực hiện kiểm tra, phân tích chứng cứ, dữ liệu để phát hiện các dấu hiệu bất thường, nguy cơ mất an toàn thông tin mạng. Trong trường hợp chưa xác minh rõ nguy cơ, sự cố xảy ra, thực hiện các giải pháp bổ sung nhằm thu thập thêm các thông tin, dữ liệu cần thiết để tăng tính chính xác của kết quả phân tích và thông tin cảnh báo;

đ) Tiến hành điều tra, xác minh nhằm xác định nguy cơ, sự cố xảy ra đối với các đối tượng giám sát. Phân tích, phân loại tấn công, rủi ro, sự cố an toàn thông tin mạng tuỳ theo tình hình cụ thể. Cảnh báo cho bộ phận phụ trách về an toàn thông tin mạng, đơn vị vận hành hệ thống thông tin, chủ quản hệ thống thông tin khi phát hiện các tấn công, rủi ro, sự cố xảy ra đối với đối tượng giám sát;

e) Hướng dẫn việc triển khai giám sát của chủ quản hệ thống thông tin; tổ chức thiết lập và hướng dẫn kết nối từ hệ thống giám sát của chủ quản hệ thống thông tin đến các hệ thống phục vụ giám sát trung tâm của Bộ Thông tin và Truyền thông. Bảo mật dữ liệu an toàn thông tin mạng trong quá trình thu thập và phân tích;

g) Định kỳ thống kê kết quả giám sát, tình hình cảnh báo và xử lý tấn công, rủi ro, sự cố an toàn thông tin mạng để phục vụ công tác lữu trữ, báo cáo;

h) Hướng dẫn, hỗ trợ đơn vị vận hành hệ thống thông tin, chủ quản hệ thống thông tin thực hiện ứng cứu, xử lý các tấn công, rủi ro, sự cố an toàn thông tin mạng trong trường hợp cần thiết;

i) Hỗ trợ một số đơn vị vận hành hệ thống thông tin, chủ quản hệ thống thông tin thiết lập hệ thống quan trắc cơ sở phù hợp với nguồn lực thực tế;

k) Các đơn vị chức năng của Bộ Thông tin và Truyền thông hàng năm lập dự toán và phê duyệt, phân bổ kinh phí thực hiện nhiệm vụ giám sát từ nguồn ngân sách nhà nước và các nguồn vốn hợp pháp khác theo quy định của pháp luật và hướng dẫn của cơ quan chức năng để trình Bộ trưởng hoặc trình cấp có thẩm quyền phê duyệt.

Chương IV

TRÁCH NHIỆM CỦA CÁC CƠ QUAN, TỔ CHỨC

Điều 12. Cục An toàn thông tin

1. Quản lý và vận hành Hệ thống xử lý tấn công mạng Internet Việt Nam để thực hiện hoạt động giám sát trung tâm.

2. Tổng hợp kết quả giám sát và các thông tin, số liệu về an toàn thông tin mạng phục vụ công tác quản lý nhà nước về an toàn thông tin.

3. Đôn đốc việc thực hiện các yêu cầu cơ bản về bảo đảm an toàn hệ thống thông tin và giám sát theo quy định pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ.

4. Chủ trì, phối hợp với Trung tâm VNCERT nghiên cứu xây dựng tiêu chí kỹ thuật và hướng dẫn chi tiết việc kết nối giữa Hệ thống quan trắc cơ sở và Hệ thống xử lý tấn công mạng Internet Việt Nam trình Bộ trưởng Bộ Thông tin và Truyền thông ban hành.

5. Phối hợp hoặc chủ trì giám sát các hệ thống thông tin thuộc lĩnh vực quan trọng cần ưu tiên đảm bảo an toàn thông tin mạng theo đề nghị của chủ quản hệ thống thông tin.

Điều 13. Trung tâm VNCERT

1. Quản lý và vận hành Hệ thống giám sát các sự cố an toàn mạng để thực hiện hoạt động giám sát trung tâm.

2. Tổng hợp kết quả giám sát và các thông tin, số liệu về an toàn thông tin mạng phục vụ công tác điều phối, ứng cứu sự cố.

3. Chủ trì, phối hợp với Cục An toàn thông tin xây dựng hướng dẫn quy trình giám sát; tổ chức triển khai các hoạt động nâng cao năng lực giám sát; đôn đốc, theo dõi, kiểm tra hoạt động giám sát, cảnh báo an toàn thông tin mạng theo phân công của Bộ trưởng Bộ Thông tin và Truyền thông.

4. Chủ trì, phối hợp với Cục An toàn thông tin nghiên cứu xây dựng tiêu chí kỹ thuật và hướng dẫn chi tiết việc kết nối giữa hệ thống quan trắc cơ sở và Hệ thống giám sát các sự cố an toàn mạng trình Bộ trưởng Bộ Thông tin và Truyền thông ban hành.

5. Chủ trì thực hiện giám sát, cảnh báo an toàn thông tin mạng đối với các hệ thống thông tin, dịch vụ công nghệ thông tin phục vụ Chính phủ điện tử. Phối hợp hoặc chủ trì giám sát các hệ thống thông tin thuộc lĩnh vực quan trọng cần

ưu tiên đảm bảo an toàn thông tin mạng theo đề nghị của chủ quản hệ thống thông tin.

6. Tổng hợp, báo cáo kết quả giám sát, cảnh báo an toàn thông tin mạng quốc gia và thống kê các tấn công, rủi ro, sự cố an toàn thông tin mạng.

Điều 14. Chủ quản các hệ thống thông tin

1. Chỉ đạo thực hiện giám sát đối với các hệ thống thông tin thuộc phạm vi quản lý, phối hợp với đơn vị chức năng của Bộ Thông tin và Truyền thông thực hiện giám sát theo quy định.

2. Thực hiện theo các hướng dẫn và phối hợp chặt chẽ với đơn vị chức năng của Bộ Thông tin và Truyền thông trong hoạt động giám sát.

3. Cung cấp các thông tin về hoạt động giám sát theo yêu cầu của của Bộ Thông tin và Truyền thông.

4. Thực hiện báo cáo kết quả giám sát định kỳ 6 tháng theo mẫu tại Phụ lục 2 hoặc khi có yêu cầu của của Bộ Thông tin và Truyền thông.

5. Chuẩn bị các cổng kết nối, giao diện kết nối dự phòng tại các điểm kết nối Internet theo các tiêu chí kỹ thuật đã quy định để thiết lập điểm giám sát của Bộ Thông tin và Truyền thông khi cần.

6. Chủ quản hệ thống thông tin do Bộ Thông tin và Truyền thông thực hiện giám sát có trách nhiệm:

a) Xác định, lập danh sáchcác hệ thống, đối tượng cần thực hiện giám sát, và cung cấp các thông tin kỹ thuật liên quan của các hệ thống, đối tượng cần thực hiện giám sát gửi Bộ Thông tin và Truyền thông;

b) Tiến hành triển khai hệ thống giám sát của chủ quản hệ thống thông tin theo quy định tại Thông tư này và quy định pháp luật có liên quan; phối hợp cung cấp các thông tin về hạ tầng, hệ thống thông tin cần giám sát và thực hiện các hỗ trợ kỹ thuật theo yêu cầu của các đơn vị chức năng của Bộ Thông tin và Truyền thông;

c) Tổ chức đội ngũ tiếp nhận các cảnh báo và xử lý các tấn công, rủi ro, sự cố an toàn thông tin mạng theo cảnh báo, yêu cầu của các đơn vị chức năng của Bộ Thông tin và Truyền thông;

d) Định kỳ thống kê kết quả xử lý tấn công, rủi ro, sự cố an toàn thông tin mạng phục vụ công tác lưu trữ, báo cáo.

7. Hàng năm lập dự toán và phê duyệt, phân bổ kinh phí thực hiện nhiệm

vụ giám sát từ nguồn ngân sách nhà nước và các nguồn vốn hợp pháp khác theo quy định của pháp luật và hướng dẫn của cơ quan chức năng.

Chương V

TỔ CHỨC THỰC HIỆN

Điều 15. Hiệu lực thi hành

1. Thông tư này có hiệu lực thi hành kể từ ngày 15 tháng 01 năm 2018.

2. Trong quá trình thực hiện, nếu có vướng mắc, phát sinh tổ chức, cá nhân có liên quan kịp thời phản ánh về Bộ Thông tin và Truyền thông để được hướng dẫn hoặc xem xét bổ sung và sửa đổi./.

Nơi nhận:
- Thủ tướng, các Phó Thủ tướng Chính phủ;
- Văn phòng Chính phủ;
- Văn phòng Trung ương và các Ban của Đảng;
- Văn phòng Tổng Bí thư;
- Văn phòng Quốc hội;
- Văn phòng Chủ tịch nước;
- Các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- Tòa án nhân dân tối cao;
- Viện Kiểm sát nhân dân tối cao;
- Kiểm toán Nhà nước;
- HĐND, UBND các tỉnh, thành phố trực thuộc Trung ương;
- Cơ quan Trung ương của các đoàn thể;
- Ủy ban quốc gia về ứng dụng CNTT;
- Ban chỉ đạo an toàn thông tin quốc gia;
- Các đơn vị chuyên trách về CNTT, ATTT của Bộ, cơ quan ngang Bộ, Cơ quan thuộc Chính phủ;
- Sở Thông tin và Truyền thông các tỉnh, thành phố trực thuộc Trung ương;
- Các Công ty dịch vụ hạ tầng viễn thông, Internet;
- Công báo, Cổng Thông tin điện tử Chính phủ;
- Cục Kiểm tra văn bản QPPL (Bộ Tư pháp);
- Bộ TTTT: Bộ trưởng và các Thứ trưởng, các cơ quan, đơn vị thuộc Bộ, Cổng thông tin điện tử Bộ;
- Lưu: VT, VNCERT (250)

BỘ TRƯỞNG

BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Trương Minh Tuấn

Phụ lục 1: Mẫu Phiếu cung cấp thông tin phục vụ giám sát

ĐƠN VỊ CẤP TRÊN **TÊN ĐƠN VỊ**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**

....., ngày ..... tháng ..... năm 20.....

PHIẾU CUNG CẤP/CẬP NHẬT THÔNG TIN VỀ HỆ THỐNG THÔNG TIN CẦN THỰC HIỆN GIÁM SÁT AN TOÀN THÔNG TIN MẠNG

Kính gửi: Bộ Thông tin và Truyền thông

I. Thông tin về đơn vị vận hành và đầu mối cung cấp thông tin

- Tên cơ quan/đơn vị quản lý vận hành hệ thống thông tin:. .....
- Địa chỉ: .....
- Tên người/đầu mối cung cấp thông tin:.....
- Chức danh: .....
- Số điện thoại:.....
- Email: .....

II. Các hệ thống thông tin cần giám sát

A. Các hệ thống thông tin hiện có:

☐ Cổng thông tin điện tử: .....

☐ Hệ thống dịch vụ công trực tuyến: .....

☐ Hệ thống thư điện tử: .....

☐ Hệ thống quản lý văn bản điều hành: .....

☐ Hệ thống cơ sở dữ liệu: .....

☐ Hệ thống khác *(ghi rõ)*:.....

B. Thông tin cụ thể các hệ thống thông tin cần giám sát

1. Hệ thống thông tin thứ nhất:

1.1. Tên hệ thống thông tin: .....

1.2. Mô tả tóm tắt chức năng, quy mô, phạm vi phục vụ của hệ thống thông tin:

.....

1.3. Cấp độ của hệ thống thông tin: .....

1.4. Hệ thống thông tin được đặt tại:

☐ Trung tâm dữ liệu của cơ quan, đơn vị, tại: .....,
được quản lý bởi *(tên đơn vị quản lý, vận hành trung tâm dữ liệu)*:.....

☐ Thuê hosting ngoài, tại Trung tâm dữ liệu của *(tên đơn vị cung cấp dịch vụ hosting, trung tâm dữ liệu)*:.....,
tại *(địa chỉ trung tâm dữ liệu)*: .....

1.5. Tên miền, UPL của hệ thống thông tin: .....

1.6. Các (dải) địa chỉ IP Internet sử dụng trong hệ thống thông tin:

.....

1.7. Thiết bị hạ tầng mạng phục vụ cho hệ thống thông tin:

☐ Switch *(chủng loại, model)*: .....

☐ Router *(chủng loại, model)*: .....

☐ IDS/IPS (Thiết bị phát hiện/ngăn chặn tấn công) *(chủng loại, model)*: .....

☐ Tường lửa, Firewall *(chủng loại, model)*: .....

☐ Thiết bị mạng khác *(chủng loại, model)*: .....

1.8. Các phần mềm nền tảng, phần mềm hệ thống, công cụ (PMNT), hệ điều hành (HĐH) sử dụng trong hệ thống thông tin

☐ Các HĐH máy chủ: .....

☐ Các PMNT ứng dụng: .....

☐ Các HĐH máy trạm: .....

☐ Các phần mềm nền tảng, hệ thống, công cụ, hệ điều hành khác *(ghi rõ)*: .....

1.9. Các thông tin kỹ thuật khác của hệ thống thông tin (ghi rõ):

.....

1.10. Giải pháp giám sát an toàn thông tin cho hệ thống thông tin:

☐ Đã có *(ghi rõ các thông tin dưới đây)* ☐ Chưa có

a. Giám sát của chủ quản hệ thống thông tin:

☐ Tự thực hiện.

☐ Thuê dịch vụ *(ghi rõ đơn vị cung cấp dịch vụ)*: .....

- Hình thức giám sát *(trực tiếp hay gián tiếp)*: .....
- Mô tả công nghệ, kỹ thuật giám sát: .....

.....

- Khả năng phân tích số lượng sự kiện an toàn mạng/mỗi giây (EPS): ..... EPS.
- Dung lượng ổ cứng lưu trữ sự kiện an toàn mạng /ngày (GB/day): .....GB/Day.
- Hệ thống giám sát có sử dụng các bộ luật xử lý tương quan: □ Có; □ Không.
- Mức độ giám sát *(Chọn các mức độ dưới đây)* :

☐ Giám sát mức cơ bản (lớp mạng và vành đai): thực hiện giám sát đối với các thiết bị mạng như router, switch, tường lửa (firewall), IDS/IPS.

☐ Giám sát mức lớp hệ điều hành: có thu thập và phân tích nhật ký của hệ điều hành.

☐ Giám sát lớp ứng dụng: có thu thập, phân tích, giám sát nhật ký các dịch vụ ứng dụng (ví dụ: web server; mail server v.v…)

☐ Giám sát lớp cơ sở dữ liệu: có thu thập, phân tích, giám sát nhật ký dịch vụ cơ sở dữ liệu.

- Các thành phần của hệ thống giám sát *(Chọn các thành phần dưới đây)* :

☐ Thành phần quan trắccơ sở (như các Sensor thu thập thông tin, thiết bị IDS/IPS, thiết bị Firewall...)

☐ Thành phần thu thập/chuẩn hóa dữ liệu đã thu thập thông tin an toàn mạng (Connector)

☐ Thành phần lưu trữ dữ liệu giám sát (Logger)

☐ Thành phần phân tích, giám sát trung tâm(ESM)

- Mô tả các thiết bị quan trắc cơ sở: .....

.....

.....

b. Giải pháp giám sát khác *(nếu có, ghi rõ đơn vị thực hiện, mô tả tóm tắt công nghệ, kỹ thuật giám sát):*

.....

.....

.....

c. Giám sát an toàn thông tin Bộ Thông tin và Truyền thông cho hệ thống thông tin:

- Đề nghị Bộ Thông tin và Truyền thông:

☐ Triển khai kết nối giám sát;

☐ Chưa đề nghị thực hiện;

☐ Khác .....

- Đề nghị hỗ trợ giám sát của chủ quản hệ thống thông tin:

☐ Có *(ghi rõ mong muốn giám sát trực tiếp/gián tiếp hoặc cả hai):*.....

☐ Không

- Yêu cầu/Đề nghị khác: .....

.....

2. Hệ thống thông tin thứ hai: *(ghi như hệ thống thông tin thứ nhất)*

.....

n. Hệ thống thông tin thứ n: *(ghi như hệ thống thông tin thứ nhất)*

.....

III. Nhân lực thực hiện công tác giám sát an toàn thông tin (giám sát)

1. Lãnh đạo chỉ đạo công tác giám sát của đơn vị *(ghi rõ họ tên, chức vụ, điện thoại, email)*:.....

.....

.....

2. Trưởng bộ phận giám sát của đơn vị *(ghi rõ họ tên, chức vụ, điện thoại, email)*:.....

.....

.....

3. Danh sách cán bộ giám sát của đơn vị:

TT	Họ tên	**Đào tạo** (bằng cấp chuyên môn)	**Chứng chỉ kỹ thuật, nghiệp vụ liên quan** (nếu có)

4. Kiến nghị của đơn vị đối với công tác giám sát: .....

.....

Người điền phiếu

(Ký, ghi rõ họ tên, điện thoại, email)

Thủ trưởng đơn vị

(Ký tên, đóng dấu)

Phụ lục 2: Mẫu báo cáo hoạt động giám sát của chủ quản hệ thống thông tin

ĐƠN VỊ CẤP TRÊN **TÊN ĐƠN VỊ**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**

....., ngày ..... tháng ..... năm .....

BÁO CÁO

ĐỊNH KỲ CỦA CHỦ QUẢN HỆ THỐNG THÔNG TIN

(từ ngày……. đến ngày …….)

Kính gửi: Bộ Thông tin và Truyền thông

I. Thông tin giám sát tổng hợp

- Thời gian giám sát: ... giờ ... phút ngày ... đến ... giờ … phút ngày ...
- Tổng số sự kiện an toàn thông tin thu thập được:
- Tổng số sự kiện an toàn thông tin nguy hiểm mức cao:
- Tình trạng an toàn thông tin: [Nghiêm trọng/Nguy Hiểm/Bình Thường/An toàn]
- Số lượng các sự cố xảy ra:
- Tóm tắt tình hình an toàn thông tin trong thời gian giám sát :

.....

.....

II. Kết quả giám sát

1. Danh sách kỹ thuật tấn công được phát hiện nhiều nhất (tối thiểu 05 kỹ thuật tấn công nhiều nhất)

STT	Kỹ thuật tấn công	Số lượng cuộc tấn công
1		
2		
3		
4		
5		

2. Danh sách dịch vụ bị tấn công nhiều nhất (tối thiểu 05 dịch vụ bị tấn công nhiều nhất)

STT	Số cổng dịch vụ/ địa chỉ IP	Dịch vụ	Số lượng cuộc tấn công
1			
2			
3			
4			
5			

3. Danh sách địa chỉ IP bị tấn công nhiều nhất (tối thiểu 05 địa chỉ IP)

STT	Địa chỉ IP	Mô tả về thiết bị/phần mềm có địa chỉ IP bị tấn công	Số lượng cuộc tấn công
1		- Các dịch vụ cung cấp: 1. Tên dịch vụ: + Mã số cổng cung cấp dịch vụ: + Giao thức hoạt động: + Phần mềm, phiên bản cung cấp dịch vụ: + Thời gian 2. Tên dịch vụ:.....	
2			
3			
4			
5			

4. Danh sách địa chỉ IP nguồn tấn công nhiều nhất từ trong nước (tối thiểu 05 địa chỉ IP)

STT	Địa chỉ IP	Số lượng cuộc tấn công
1		
2		
3		
4		
5		

5. Danh sách địa chỉ IP nguồn tấn công nhiều nhất từ nước ngoài (tối thiểu 05 địa chỉ IP)

STT	Địa chỉ IP	Số lượng cuộc tấn công
1		
2		
3		
4		
5		

III. Các loại tấn công điển hình

1. Các loại tấn công nguy hiểm nhất (tối thiểu 05):

1.1. Kỹ thuật tấn công thứ 1:

- Tên kỹ thuật tấn công:.....
- Mã hiệu quốc tế (nếu có) :.....
- Các đối tượng bị tấn công:.....
- Dấu hiệu nhận biết:.....
- Mô tả :.....
- Số lượng và thời gian xảy ra:.....
- Đánh giá mức độ nguy hiểm:.....
- Ảnh hưởng:.....
- Các biện pháp xử lý đã được triển khai:.....
- Tài liệu tham khảo:.....
- Ghi chú khác:.....

1.2. Kỹ thuật tấn công thứ 2: (Mô tả tương tự kỹ thuật tấn công thứ 1)

1.3. Kỹ thuật tấn công thứ 3: (Mô tả tương tự kỹ thuật tấn công thứ 1)

1.4. Kỹ thuật tấn công thứ 4: (Mô tả tương tự kỹ thuật tấn công thứ 1)

1.5. Kỹ thuật tấn công thứ 5: (Mô tả tương tự kỹ thuật tấn công thứ 1)

.....

1.n. Kỹ thuật tấn công n:.....

2. Các loại tấn công diễn ra nhiều nhất (tối thiểu 05)

2.1. Kỹ thuật tấn công thứ 1:

- Tên kỹ thuật tấn công:.....

- Mã hiệu quốc tế (nếu có) :.....
- Các đối tượng bị tấn công:.....
- Dấu hiệu nhận biết:.....
- Mô tả :.....
- Số lượng và thời gian xảy ra:.....
- Đánh giá mức độ nguy hiểm:.....
- Ảnh hưởng:.....
- Các biện pháp xử lý đã được triển khai:.....
- Tài liệu tham khảo:.....
- Ghi chú khác:.....

2.2. Kỹ thuật tấn công thứ 2: (Mô tả tương tự kỹ thuật tấn công thứ 1)

2.3. Kỹ thuật tấn công thứ 3: (Mô tả tương tự kỹ thuật tấn công thứ 1)

2.4. Kỹ thuật tấn công thứ 4: (Mô tả tương tự kỹ thuật tấn công thứ 1)

2.5. Kỹ thuật tấn công thứ 5: (Mô tả tương tự kỹ thuật tấn công thứ 1)

.....

2.n. Kỹ thuật tấn công n:.....

3. Các loại tấn công mới xuất hiện (tối thiểu 05)

3.1. Kỹ thuật tấn công thứ 1:

- Tên kỹ thuật tấn công:.....
- Mã hiệu quốc tế (nếu có) :.....
- Các đối tượng bị tấn công:.....
- Dấu hiệu nhận biết:.....
- Mô tả :.....
- Số lượng và thời gian xảy ra:.....
- Đánh giá mức độ nguy hiểm:.....
- Ảnh hưởng:.....
- Các biện pháp xử lý đã được triển khai:.....
- Tài liệu tham khảo:.....
- Ghi chú khác:.....

3.2. Kỹ thuật tấn công thứ 2: (Mô tả tương tự kỹ thuật tấn công thứ 1)

3.3. Kỹ thuật tấn công thứ 3: (Mô tả tương tự kỹ thuật tấn công thứ 1)

3.4. Kỹ thuật tấn công thứ 4: (Mô tả tương tự kỹ thuật tấn công thứ 1)

3.5. Kỹ thuật tấn công thứ 5: (Mô tả tương tự kỹ thuật tấn công thứ 1)

.....

3.n. Kỹ thuật tấn công n:.....

IV. Các vấn đề khác về an toàn thông tin trong kỳ giám sát

.....

.....

.....

V. Đề xuất và kiến nghị:

.....

.....

Nơi nhận:
- *Như trên;*
- *Trung tâm VNCERT;*
- *Cục ATTT;*
- *Lưu ....*

Thủ trưởng đơn vị

(ký, đóng dấu)