BỘ THÔNG TIN VÀ TRUYỀN THÔNG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
	Độc lập - Tự do - Hạnh phúc
DỰ THẢO ver 3.6	Số: /2017/TT-BTTTT

Hà Nội, ngày tháng năm 2017

THÔNG TƯ

Quy định hoạt động giám sát và cảnh báo an toàn thông tin mạng

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

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 Quyết định 63/QĐ-TTg ngày 13 tháng 01 năm 2010 của Thủ tướng Chính phủ phê duyệt Quy hoạch phát triển an toàn thông tin số quốc gia đến năm 2020;

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

Căn cứ Quyết định số 898/QĐ-TTg ngày 27 tháng 5 năm 2016 phê duyệt phương hướng, mục tiêu, nhiệm vụ bảo đảm an toàn thông tin mạng giai đoạn 2016 - 2020;

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

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 và cảnh báo an toàn thông tin mạng.

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Thông tư này quy định về hoạt động giám sát và cảnh báo an toàn thông tin mạng (an toàn mạng) cho dịch vụ cổng thông tin điện tử và các dịch vụ công trực tuyến phục vụ cho Chính phủ điện tử tại các Bộ, Ngành, Tỉnh và Thành phố trực thuộc Trung ương; các điều kiện để nâng cao năng lực giám sát, phát hiện và cảnh báo an toàn mạng trên toàn quốc.

Điều 2. Đối tượng áp dụng

Chủ quản hệ thống thông tin cung cấp dịch vụ cổng thông tin điện tử và dịch vụ công trực tuyến phục vụ Chính phủ điện tử tại các Bộ, Ngành, Tỉnh và Thành phố trực thuộc Trung ương.

Điều 3. Giải thích từ ngữ

Trong Thông tư này, các từ ngữ dưới đây được hiểu như sau:

1. **Đầu mối giám sát** là cá nhân được phép thay mặt bộ phận chuyên trách về an toàn mạng để thực hiện nhiệm vụ cung cấp, trao đổi thông tin và theo dõi, đôn đốc, hỗ trợ hoạt động giám sát trong phạm vi của bộ phận chuyên trách về an toàn mạng.

2. **Giám sát quốc gia** là hoạt động giám sát được Bộ Thông tin và Truyền thông thực hiện thông qua Trung tâm giám sát an toàn mạng quốc gia (viết tắt là TTGS) nhằm mục đích giám sát diện rộng và giám sát cho các hệ thống, dịch vụ công nghệ thông tin Chính phủ điện tử để kịp thời phát hiện, cảnh báo sớm các nguy cơ, sự cố nghiêm trọng và các nguy cơ, sự cố an toàn mạng xảy ra trên diện rộng. Hệ thống giám sát quốc gia được Bộ Thông tin và Truyền thông giao cho Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) vận hành và quản lý.

3. **Giám sát cơ sở** là hoạt động giám sát được chủ quản hệ thống thông tin tự thực hiện nhằm mục đích phát hiện, cảnh báo các sự cố an toàn mạng cho các hệ thống, dịch vụ công nghệ thông tin của mình và cung cấp thông tin/báo cáo cho Bộ Thông tin và Truyền thông.

4. **Đối tượng giám sát** là hệ thống thông tin, thiết bị, hệ thống mạng, ứng dụng, dịch vụ công nghệ thông tin cần được giám sát an toàn mạng.

Chương II
GIÁM SÁT AN TOÀN MẠNG

Điều 4. Nguyên tắc giám sát an toàn mạng

1. Đảm bảo được thực hiện thường xuyên, liên tục 24 giờ trong ngày và 7 ngày trong tuần.

2. Chủ động phòng ngừa, kịp thời phát hiện, ngăn chặn sự cố an toàn mạng.

3. Đảm bảo sự ổn định, bí mật thông tin của đối tượng giám sát.

4. Có sự điều phối, kết hợp chặt chẽ, hiệu quả giữa giám sát quốc gia (do hệ thống giám sát quốc gia thực hiện) và giám sát cơ sở (do hệ thống giám sát cơ sở thực hiện).

5. Từng bước xây dựng khả năng liên thông giữa hệ thống xử lý quốc gia và hệ thống xử lý cơ sở, giữa điểm giám sát/hệ thống quan trắc cơ sở và hệ thống giám sát.

6. Hoạt động giám sát phải tuân thủ đúng quy trình giám sát và các quy định tại thông tư này và các quy định pháp luật có liên quan.

Điều 5. Đối tượng giám sát

Các hệ thống thông tin cung cấp dịch vụ cổng thông tin điện tử và các dịch vụ công trực tuyến phục vụ cho Chính phủ điện tử của các Bộ, Ngành, Tỉnh, Thành phố trực thuộc Trung ương, nằm trong khung kiến trúc Chính phủ điện tử Việt Nam.

Điều 6. Phương thức giám sát

1. Giám sát an toàn thông tin mạng được thực hiện qua hai phương thức: phương thức giám sát trực tiếp hoặc phương thức giám sát gián tiếp.

2. Giám sát trực tiếp là hoạt động giám sát được tiến hành bằng cách đặt các thiết bị chuyên dụng phân tích luồng dữ liệu hoặc thu nhận trực tiếp thông tin hệ thống được giám sát sau đó tổng hợp, đồng bộ, phân tích nhằm phát hiện ra các tấn công, sự cố an toàn mạng. Khi tiến hành giám sát trực tiếp, thường cần tiến hành các hoạt động sau:

a) Phân tích, thu thập các thông tin an toàn mạng (information security event) bằng các kỹ thuật khác nhau:

- Phân tích, quan trắc an toàn thông tin trên đường truyền mạng/luồng thông tin (là các gói tin thuộc lớp mạng) tại các cổng kết nối Internet;

- Thu thập nhật ký (log file) đã được lưu lại, 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 mạng để phát hiện ra các tấn công, sự cố an toàn 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, kiểm tra từ xa 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 để phân tích nhằm

phát hiện ra các nguy cơ, sự cố hoặc tấn công mạng. Giám sát gián tiếp được tiến hành bằng cách sau đây:

a) Thu thập thông tin về nguy cơ, sự cố gây mất an toàn mạng liên quan đến đối tượng giám sát từ các nguồn thông tin khác.

b) Kiểm tra, rà soát từ xa các đối tượng được giám sát để đánh giá tình trạng, phát hiện các điểm yếu, nguy cơ có khả năng bị khai thác, tấn công, gây hại.

Điều 7. Mô hình giám sát an toàn mạng quốc gia

1. Trung tâm giám sát an toàn mạng quốc gia được Trung tâm VNCERT tổ chức triển khai và vận hành để thực hiện công tác hỗ trợ giám sát an toàn thông tin mạng trên toàn quốc. Trung tâm giám sát an toàn mạng quốc gia bao gồm Hệ thống giám sát trung tâm và hệ thống quan trắc cơ sở.

2. Hệ thống giám sát trung tâm:

a) Là hệ thống được sử dụng để thực hiện việc thu thập, theo dõi, phát hiện, phân tích, xử lý, báo cáo, thu thập chứng cứ về các sự cố, các dấu hiệu tấn công, các nguy cơ gây mất an toàn mạng dựa trên các dữ liệu/thông tin trạng thái 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 VNCERT chịu trách nhiệm xây dựng, thiết lập, quản lý và vận hành.

3. Hệ thống quan trắc cơ sở

a) Là tập hợp các thiết bị, phần mềm có khả năng cung cấp thông tin nhật ký, trạng thái, cảnh báo cho Hệ thống 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 Trung tâm VNCERT.

c) Do cơ quan chủ quản của các đối tượng giám sát hoặc VNCERT xây dựng, thiết lập, quản lý và vận hành.

d) Được kết nối vào Hệ thống giám sát trung tâm để chia sẻ và cung cấp các thông tin giám sát.

Điều 8. Mô hình và triển khai hệ thống giám sát cơ sở

Chủ quản hệ các hệ thống thông tin phục vụ Chính phủ điện tử có mức độ an toàn cấp độ 3 trở lên có trách nhiệm triển khai hệ thống giám sát cơ sở phục vụ để phát hiện các sự cố, dấu hiệu tấn công, nguy cơ có khả năng ảnh hưởng an toàn thông tin, hoạt động của hệ thống và khả năng cung cấp dịch vụ.

Hệ thống giám sát cơ sở cần triển khai đáp ứng các yêu cầu tối thiểu sau đây:

1. Thiết lập trung tâm giám sát cơ sở

Trung tâm giám sát cơ sở được thiết lập cần đáp ứng các yêu cầu sau:

a) Có khả năng thu thập, tổng hợp, đồng bộ, phân tích để phát hiện ra nguy cơ, sự cố, dấu hiệu tấn công có khả năng ảnh hưởng an toàn thông tin, hoạt động hệ thống và khả năng cung cấp dịch vụ

b) Thu thập và phân tích các thông tin tối thiểu sau đây: Nhật ký WebServer với các ứng dụng web, cổng thông tin điện tử; Cảnh báo của thiết bị quan trắc cơ sở; Cảnh báo/nhật ký của thiết bị tường lửa được thiết lập bảo vệ luồng dữ liệu

c) Năng lực xử lý trung tâm giám sát cơ sở cần phù hợp với khối lượng thông tin an toàn mạng thu thập được.

d) Có khả năng kết nối với Hệ thống giám sát trung tâm khi có yêu cầu.

2. Thiết lập thiết bị quan trắc cơ sở đáp ứng các yêu cầu tối thiểu sau

a) Đặt thiết bị quan trắc để phát hiện tấn công bao phủ được tất cả các đường kết nối mạng Internet của hệ thống thông tin phục vụ Chính phủ điện tử. Thiết bị quan trắc cần đáp ứng tối thiểu các chức năng phát hiện tấn công mạng, tấn công hệ điều hành, tấn công dò quét.

b) Thiết bị quan trắc được triển khai cần có chức năng cho phép tạo lập các 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.

c) Đối với các hệ thống thông tin phục vụ chính phủ điện tử sử dụng giao thức có mã hóa (ví dụ: HTTPS) để cung cấp dịch vụ cho người sử dụng, cần có phương án kỹ thuật đảm bảo thiết bị quan trắc an toàn thông tin có được đầy đủ thông tin dưới dạng không mã để có thể phân tích, phát hiện được các tấn công.

d) Thiết lập hệ thống quan trắc cơ sở theo hướng dẫn của VNCERT.

3. Các nhiệm vụ triển khai trong quá trình giám sát cơ sở:

a) Theo dõi, trực giám sát liên tục, lập báo cáo hàng ngày, đảm bảo hệ thống giám sát cơ sở hoạt động và thu thập thông tin ổn định.

b) Thực hiện phân tích, thu thập chứng cứ, lập báo cáo kết quả phân tích, tiến hành điều tra, xác minh nhằm xác định nguy cơ hoặc sự cố xảy ra đối với các đối tượng giám sát cơ sở.

c) Tiến hành phân loại nguy cơ, sự cố mất ATTT tuỳ theo tình hình cụ thể.

d) Định kỳ thống kê kết quả xử lý nguy cơ và sự cố gây mất ATTT và lưu hồ sơ báo cáo cấp trên.

e) Cung cấp và cập nhật thông tin mô tả phương án kỹ thuật triển khai Hệ thống giám sát cơ sở cho Trung tâm VNCERT gồm những thông tin: thông tin chi tiết về đối tượng giám sát cơ sở, vị trí đặt hệ thống giám sát cơ sở, dung lượng các đường truyền kết nối vào đối tượng giám sát cơ sở, các thông tin dự kiến thu thập (cảnh báo ids, log firewall, log webserver,...,theo chuẩn syslog), sơ đồ luồng thông tin.

f) Năng lực lưu trữ thông tin giám sát tối thiểu đạt mức trung bình 30 ngày hoạt động bình thường.

g) Cung cấp thông tin giám sát theo yêu cầu của VNCERT.

h) Báo cáo hoạt động giám sát cơ sở định kỳ 06 tháng theo mẫu tại Phụ lục 1.

Điều 9. Hoạt động giám sát an toàn mạng quốc gia

1. Trung tâm VNCERT có trách nhiệm thực hiện thiết lập Hệ thống giám sát trung tâm 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 giám sát gián tiếp.

2. Trung tâm VNCERT thực hiện các hoạt động giám sát an toàn mạng quốc gia sau:

a) Quản lý, cập nhật danh sách đối tượng giám sát của TTGS;

b) Theo dõi, trực trung tâm giám sát, lập báo cáo hàng ngày;

c) Tổng hợp, lưu trữ, phân loại thông tin thu thập được từ các Hệ thống quan trắc cơ sở;

d) Kiểm tra, đôn đốc công tác theo dõi, trực giám sát.

e) Thực hiện phân tích, thu thập chứng cứ, lập báo cáo kết quả phân tích, kiểm tra các thông tin được tổng hợp, lưu trữ và phân loại. Trong trường hợp chưa xác minh rõ nguy cơ, sự cố xảy ra, VNCERT tiếp tục theo dõi, trực giám sát nhằm thu thập thêm các thông tin cần thiết để tăng tính chính xác của cảnh báo.

f) Tiến hành điều tra, xác minh nhằm xác định nguy cơ hoặc sự cố xảy ra đối với các đối tượng giám sát.

g) Tiến hành phân loại nguy cơ, sự cố mất ATTT tuỳ theo tình hình cụ thể.

h) Cảnh báo cho đơn vị chuyên trách về an toàn mạng của chủ quản hệ thống thông tin khi phát hiện các nguy cơ xảy ra đối với đối tượng giám sát.

i) Định kỳ thống kê kết quả xử lý nguy cơ và sự cố gây mất ATTT và lưu hồ sơ báo cáo cấp trên.

j) Hỗ trợ chủ quản hệ thống thông tin thực hiện việc xử lý đối với các sự cố, nguy cơ mất an toàn mạng trong trường hợp cần thiết.

k) Hỗ trợ một số chủ quản hệ thống thông tin thực hiện thiết lập hệ thống quan trắc cơ sở theo yêu cầu thực tế.

2. Chủ quản hệ thống thông tin cung cấp dịch vụ chính phủ điện tử thực hiện các hoạt động giám sát an toàn mạng quốc gia sau:

a) Tổ chức đội ngũ tiếp nhận các cảnh báo và xử lý các sự cố, nguy cơ mất an toàn mạng theo cảnh báo của Trung tâm VNCERT.

b) Định kỳ thống kê kết quả xử lý nguy cơ và sự cố gây mất ATTT và lưu hồ sơ báo cáo.

Điều 10.Giám sát gián tiếp

1. Cơ quan chủ quản của đối tượng giám sát thực hiện giám sát gián tiếp đối với các hệ thống, dịch vụ công nghệ thông tin.

2. Cơ quan chủ quản của đối tượng giám sát có trách nhiệm gửi kết quả giám sát gián tiếp cho Trung tâm VNCERT.

3. Bộ Thông tin và Truyền thông (Trung tâm VNCERT) thực hiện giám sát gián tiếp đối với hệ thống thông tin quan trọng của Chính phủ điện tử, các cơ quan Đảng, Nhà nước và các lĩnh vực quan trọng cần ưu tiên đảm bảo an toàn thông tin mạng.

Chương III
GIẢI PHÁP ĐẢM BẢO CHO HOẠT ĐỘNG GIÁM SÁT, CẢNH BÁO

Điều 11. Đầu mối giám sát, cảnh báo

1. Chủ quản đối tượng giám sát có trách nhiệm cử cá nhân làm đầu mối giám sát an toàn mạng để phối hợp với Trung tâm VNCERT.

2. Đầu mối giám sát phải đảm bảo khả năng tiếp nhận thông tin cảnh báo liên tục 24 giờ trong một ngày và 07 ngày trong tuần, chịu trách nhiệm đảm bảo kết nối từ hệ thống quan trắc cơ sở đến Hệ thống giám sát trung tâm.

3. Đầu mối giám sát phải gồm những người có trình độ chuyên môn và kỹ năng nghiệp vụ để tiếp nhận và truyền đạt lại với các bộ phận khác.

a) Đối với cá nhân là lãnh đạo phải được quyền chỉ đạo, ra quyết định liên quan tới hoạt động giám sát, cảnh báo.

b) Đối với cán bộ kỹ thuật phải đáp ứng yêu cầu tại Điều 12.

4. 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 hay trao đổi trên một phần mềm trao đổi thông tin chuyên biệt nhằm đảm bảo thông tin được bảo mật.

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

Điều 12.Yêu cầu đối với nhân sự thực hiện công tác giám sát, cảnh báo

1. Nhân sự thực hiện công tác giám sát phải đáp ứng yêu cầu sau:

a) Có trình độ chuyên môn, chứng chỉ về an toàn mạng hoặc đáp ứng chuẩn kỹ năng về an toàn mạng.

b) Có ít nhất 01 năm kinh nghiệm trong công tác giám sát an toàn mạng.

c) Đáng tin cậy, có tính kỷ luật, đảm bảo bí mật trong nhiệm vụ được giao.

d) Có kỹ năng phân tích thông tin, trao đổi, chia sẻ thông tin, khả năng làm việc theo nhóm.

2. Nhân sự thực hiện công tác giám sát phải hiểu rõ các quy trình, quy định về giám sát an toàn mạng.

Điều 13. Hoạt động nâng cao năng lực giám sát

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

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

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

4. Phối hợp nghiên cứu phát triển sản phẩm và 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 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.

Điều 14.Trao đổi, cung cấp, chia sẻ thông tin

1. Khuyến khích các bộ phận chuyên trách về an toàn mạng 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 mạng của tổ chức, cá nhân.

2. Các thông tin cần chia sẻ, cung cấp và trao đổi bao gồm các thông tin về nguy cơ, sự cố an toàn 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.

4. 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

5. Khi cung cấp thông tin cho Cơ quan điều phối thì phải áp dụng các biện pháp bảo mật theo hướng dẫn của Cơ quan điều phối.

Điều 15. Chính sách cho lực lượng giám sát, cảnh báo an toàn mạng

Lực lượng giám sát, cảnh báo và ứng cứu sự cố an toàn mạng làm việc theo ca, đảm bảo thường trực 24 giờ trong ngày và 07 ngày trong tuần, được hưởng đầy đủ quyền lợi về chế độ lương, thưởng, chế độ nghỉ ca và tăng ca và các quyền lợi khác theo quy định hiện hành của nhà nước.

Chương V
QUYỀN VÀ TRÁCH NHIỆM CỦA CÁC TỔ CHỨC

Điều 16. Trung tâm VNCERT

1. Vận hành và quản lý Hệ thống giám sát trung tâm.

2. Xây dựng các quy trình, hướng dẫn triển khai công tác giám sát an toàn mạng quốc gia.

3. 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 trung tâm.

4. Thực hiện hoạt động giám sát, cảnh báo, đôn đốc, theo dõi, kiểm tra hoạt động giám sát, cảnh báo trên phạm vi toàn quốc gia.

5. Thực hiện cảnh báo các nguy cơ, sự cố có khả năng xảy ra trên diện rộng và các nguy cơ, sự cố phát hiện được đối với những đối tượng giám sát được giao theo thẩm quyền.

Điều 17. Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ, UBND các tỉnh thành phố trực thuộc Trung ương.

1. Xây dựng, quản lý, vận hành hệ thống giám sát cơ sở và hệ thống quan trắc cơ sở.

2. Có quyền thực hiện hoạt động giám sát, cảnh báo trên phạm vi quản lý của mình.

3. Thực hiện hoạt động giám sát cơ sở, hoạt động giám sát an toàn mạng quốc gia.

4. Đôn đốc, theo dõi, kiểm tra hoạt động giám sát trên phạm vi trách nhiệm của mình; thực hiện cảnh báo nguy cơ, sự cố đối với những đối tượng giám sát thuộc phạm vi trách nhiệm của mình và đôn đốc thực hiện các biện pháp phát hiện, phòng ngừa, ngăn chặn, xử lý đối với các nguy cơ, sự cố.

5. Tuân thủ các hướng dẫn và phối hợp chặt chẽ với Trung tâm VNCERT trong hoạt động giám sát, cảnh báo, ứng cứu sự cố.

6. Thực hiện báo cáo kết quả giám sát, cảnh báo theo định kỳ hàng tháng, quý, 6 tháng, năm hoặc khi có yêu cầu của Trung tâm VNCERT theo mẫu tại Phụ lục 1.

7. Lắp đặt sẵn 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 quốc gia khi cần.

Điều 18.Bộ phận chuyên trách về giám sát an toàn mạng

1. Thực hiện theo các hướng dẫn và phối hợp chặt chẽ với Trung tâm VNCERT trong hoạt động giám sát an toàn mạng.

2. Cung cấp các thông tin về hoạt động giám sát an toàn mạng theo yêu cầu của Trung tâm VNCERT

3. Thực hiện báo cáo, thống kê kết quả giám sát theo định kỳ hàng tháng, quý, 6 tháng, năm hoặc khi có yêu cầu của Trung tâm VNCERT theo mẫu tại Phụ lục 2.

Chương VI
ĐIỀU KHOẢN THI HÀNH

Điều 19. Hiệu lực thi hành

Thông tư này có hiệu lực thi hành kể từ ngày 15 tháng 2 năm 2016.

Điều 20. Hướng dẫn thi hành

1. Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam trong phạm vi chức năng, quyền hạn của mình có trách nhiệm tổ chức hoạt động giám sát và cảnh báo an toàn mạng hiệu quả trên toàn quốc.

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

Nơi nhận:
- Ban Bí thư Trung ương Đảng;

BỘ TRƯỞNG

- Thủ tướng, các Phó Thủ tướng Chính phủ;
- Các Bộ, cơ quan ngang Bộ, cơ quan thuộc CP;
- HĐND, UBND các tỉnh, TP trực thuộc TW;
- Văn phòng Trung ương và các Ban của Đảng;
- Văn phòng Tổng Bí thư;
- Văn phòng Chủ tịch nước;
- Hội đồng Dân tộc và các Ủy ban của Quốc hội;
- Văn phòng Quốc hội;
- Tòa án nhân dân tối cao;
- Viện Kiểm sát nhân dân tối cao;
- Kiểm toán Nhà nước;
- Ủy ban Giám sát tài chính Quốc gia;
- Ngân hàng Chính sách xã hội;
- Ngân hàng Phát triển Việt Nam;
- UBTW Mặt trận Tổ quốc Việt Nam;
- Cơ quan Trung ương của các đoàn thể;
- VPCP: BTCN, các PCN, Trợ lý TTCP, TGĐ Cổng TTĐT, các Vụ, Cục, đơn vị trực thuộc, Công báo;
- Lưu: VT, VNCERT.

Trương Minh Tuấn

Phụ lục 1: Mẫu báo cáo định kỳ của chủ quản Hệ thống giám sát cơ sở

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

Tỉnh (thành phố), ngày ..... tháng ..... năm .....

BÁO CÁO
ĐỊNH KỲ CỦA CHỦ QUẢN HỆ THỐNG GIÁM SÁT CƠ SỞ
(từ ngày……. đến ngày …….)

Kính gửi: Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam

I. Thông tin giám sát tổng hợp

Trong tuần từ ngày ……. đến ngày …….. hệ thống giám sát của …… đã phát hiện sàng lọc ra …….. sự kiện dò quét và tấn công vào mỗi điểm giám sát hệ thống thông tin. Trong đó có khoảng …….. sự kiện có khả năng gây nguy hiểm dẫn đến sự cố an toàn mạng ở mức cao.

II. Các loại tấn công điển hình

Nhìn chung tình hình tấn công không gian mạng trong từ ngày ……. đến ngày …….. vừa qua có nhiều tấn công đặc biệt nguy hiểm, tạo ra các sự cố nghiêm trọng, dưới đây là một số loại tấn công điển hình:

1. Kỹ thuất tấn công……
2. Kỹ thuật tấn công……
3. Kỹ thuất tấn công……
4. Kỹ thuật tấn công……
5. Lây nhiễm mã độc trong mạng……...

III. Tổng hợp các loại tấn công

1. Danh sách 5 kỹ thuật tấn công được phát hiện nhiều nhất

STT	Kỹ thuật tấn công	Số lượng cuộc tấn công
1		
2		

3		
4		
5		

2. Danh sách 5 cổng dịch vụ bị tấn công nhiều nhất

STT	Cổng dịch vụ bị tấn công	Dịch vụ bị tấn công	Số lượng cuộc tấn công
1			
2			
3			
4			
5			

3. Danh sách một số hình thức tấn công điển hình

STT	Hình thức tấn công điển hình
1	Loại kỹ thuật tấn công: ……
1.1	Tên kỹ thuật tấn công: …… Mô tả kỹ thuật tấn công: …….....
1.2	Tên kỹ thuật tấn công: …… Mô tả kỹ thuật tấn công: …….....
2	Loại kỹ thuật tấn công: ……
2.1	Tên kỹ thuật tấn công: …… Mô tả kỹ thuật tấn công: …….....
2.2	Tên kỹ thuật tấn công: …… Mô tả kỹ thuật tấn công: …….....

4. Danh sách năm quốc gia và nền kinh tế có số lượng sự kiện tấn công cao nhất

Phân tích nguồn gốc phát tán tấn công, quốc gia….. có số lượng sự kiện tấn công gây mất an toàn mạng lớn nhất trong khoảng thời gian từ ngày…….. đến ngày…… chiếm ……% tổng số sự kiện tấn công an toàn mạng có địa chỉ IP nguồn do nước ngoài quản lý, tiếp sau đó là các quốc gia……

…….

(Biểu đồ thống kê các quốc gia có số lượng/ tỉ lệ % sự kiện nhiều nhất)

Tỷ lệ trên được tính trên tổng số sự kiện an toàn mạng có địa chỉ IP nguồn do nước ngoài quản lý, không tính các sự kiện an toàn mạng có địa chỉ IP của Việt Nam.

STT	Kỹ thuật tấn công	Thời gian phát hiện
1	Loại kỹ thuật tấn công: ……	
1.1	Tên kỹ thuật tấn công: …… Mô tả kỹ thuật tấn công: …… Đối tượng bị tấn công: …… Phiên bản ứng dụng tồn tại lỗ hổng: …… Bằng chứng:…… Kết quả giả lập tấn công:…… Tài liệu tham khảo:……	…..(h):….(m):…(s) Ngày…tháng…năm….
1.2	Tên kỹ thuật tấn công: …… Mô tả kỹ thuật tấn công: …… Đối tượng bi tấn công: …… Phiên bản ứng dụng tồn tại lỗ hổng: …… Bằng chứng:…… Kết quả giả lập tấn công:…… Tài liệu tham khảo:……	…..(h):….(m):…(s) Ngày…tháng…năm….
2	Loại kỹ thuật tấn công: ……	
2.1	Tên kỹ thuật tấn công: …… Mô tả kỹ thuật tấn công: …… Đối tượng bị tấn công: …… Phiên bản ứng dụng tồn tại lỗ hổng: …… Bằng chứng:…… Kết quả giả lập tấn công:…… Tài liệu tham khảo:……	…..(h):….(m):…(s) Ngày…tháng…năm….

2.2	Tên kỹ thuật tấn công: …… Mô tả kỹ thuật tấn công: …… Đối tượng bị tấn công:…… Phiên bản ứng dụng tồn tai lỗ hổng: …… Bằng chứng:…… Kết quả giả lập tấn công:…… Tài liệu tham khảo:……	…..(h):….(m):…(s) Ngày…tháng…năm….

IV. Đề xuất và kiến nghị:

.....
.....

Thủ trưởng đơn vị tiếp nhận sự cố nhận xét, xác nhận
(ký, đóng dấu)

Thủ trưởng đơn vị
(ký, đóng dấu)

Phụ lục 2: Mẫu báo cáo định kỳ của Bộ phận chuyên trách

ĐƠN VỊ CẤP TRÊN
TÊN ĐƠN VỊ

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Tỉnh (thành phố), ngày ..... tháng ..... năm .....

BÁO CÁO
TÌNH HÌNH AN TOÀN MẠNG ĐỊNH KỲ
(từ ngày……. đến ngày …….)

Kính gửi: Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam

I. Thông tin giám sát tổng hợp

Trong tuần từ ngày ……. đến ngày …….. hệ thống giám sát của …… đã phát hiện sàng lọc ra …….. sự kiện dò quét và tấn công vào mỗi điểm giám sát hệ thống thông tin. Trong đó có khoảng …….. sự kiện có khả năng gây nguy hiểm dẫn đến sự cố an toàn mạng ở mức cao.

II. Các loại tấn công điển hình

Nhìn chung tình hình tấn công không gian mạng trong từ ngày ……. đến ngày …….. vừa qua có nhiều tấn công đặc biệt nguy hiểm, tạo ra các sự cố nghiêm trọng, dưới đây là một số loại tấn công điển hình:

1. Kỹ thuất tấn công……
2. Kỹ thuật tấn công……
3. Kỹ thuất tấn công……
4. Kỹ thuật tấn công……
5. Lây nhiễm mã độc trong mạng……...

III. Tổng hợp các loại tấn công

1. Danh sách 5 kỹ thuật tấn công được phát hiện nhiều nhất

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

4		
5		

2. Danh sách 5 cổng dịch vụ bị tấn công nhiều nhất

STT	Cổng dịch vụ bị tấn công	Dịch vụ bị tấn công	Số lượng cuộc tấn công
1			
2			
3			
4			
5			

3. Danh sách một số hình thức tấn công điển hình

STT	Hình thức tấn công điển hình
1	Loại kỹ thuật tấn công: ……
1.1	Tên kỹ thuật tấn công: …… Mô tả kỹ thuật tấn công: …….....
1.2	Tên kỹ thuật tấn công: …… Mô tả kỹ thuật tấn công: …….....
2	Loại kỹ thuật tấn công: ……
2.1	Tên kỹ thuật tấn công: …… Mô tả kỹ thuật tấn công: …….....
2.2	Tên kỹ thuật tấn công: …… Mô tả kỹ thuật tấn công: …….....

4. Danh sách năm quốc gia và nền kinh tế có số lượng sự kiện tấn công cao nhất

Phân tích nguồn gốc phát tán tấn công, quốc gia….. có số lượng sự kiện tấn công gây mất an toàn mạng lớn nhất trong khoảng thời gian từ ngày…….. đến ngày…… chiếm ……% tổng số sự kiện tấn công an toàn mạng có địa chỉ IP nguồn do nước ngoài quản lý, tiếp sau đó là các quốc gia……

…….

(Biểu đồ thống kê các quốc gia có số lượng/ tỉ lệ % sự kiện nhiều nhất)

Tỷ lệ trên được tính trên tổng số sự kiện an toàn mạng có địa chỉ IP nguồn do nước ngoài quản lý, không tính các sự kiện an toàn mạng có địa chỉ IP của Việt Nam.

STT	Kỹ thuật tấn công	Thời gian phát hiện
1	Loại kỹ thuật tấn công: ……	
1.1	Tên kỹ thuật tấn công: …… Mô tả kỹ thuật tấn công: …… Đối tượng bị tấn công: …… Phiên bản ứng dụng tồn tại lỗ hổng: …… Bằng chứng:…… Kết quả giả lập tấn công:…… Tài liệu tham khảo:……	…..(h):….(m):…(s) Ngày…tháng…năm….
1.2	Tên kỹ thuật tấn công: …… Mô tả kỹ thuật tấn công: …… Đối tượng bị tấn công: …… Phiên bản ứng dụng tồn tại lỗ hổng: …… Bằng chứng: …… Kết quả giả lập tấn công: …… Tài liệu tham khảo: ……	…..(h):….(m):…(s) Ngày…tháng…năm….
2	Loại kỹ thuật tấn công: ……	
2.1	Tên kỹ thuật tấn công: …… Mô tả kỹ thuật tấn công: …… Đối tượng bị tấn công: …… Phiên bản ứng dụng tồn tại lỗ hổng: ……	…..(h):….(m):…(s) Ngày…tháng…năm….

	Bằng chứng:…… Kết quả giả lập tấn công:…… Tài liệu tham khảo:……	
2.2	Tên kỹ thuật tấn công: …… Mô tả kỹ thuật tấn công: …… Đối tượng bị tấn công: …… Phiên bản ứng dụng tồn tại lỗ hổng: …… Bằng chứng:…… Kết quả giả lập tấn công:…… Tài liệu tham khảo:……	…..(h):….(m):…(s) Ngày…tháng…năm….

IV. Đề xuất và kiến nghị:

.....
.....

Thủ trưởng đơn vị tiếp nhận cảnh báo nhận xét, xác nhận
(ký, đóng dấu)

Thủ trưởng đơn vị
(ký, đóng dấu)