BỘ THÔNG TIN VÀ TRUYỀN THÔNG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
	Độc lập - Tự do - Hạnh phúc
Số: 20 /2017/TT-BTTTT	

Hà Nội, ngày 12 tháng 9 năm 2017

THÔNG TƯ

Quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc

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

Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống 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 số 05/2017/QĐ-TTg ngày 16 tháng 3 năm 2017 của Thủ tướng Chính phủ 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 về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc.

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi và đối tượng áp dụng

1. Thông tư này quy định về các hoạt động điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc (không bao gồm hoạt động điều phối ứng cứu sự cố an toàn thông tin mạng nghiêm trọng quy định tại Quyết định số 05/2017/QĐ-TTg ngày 16 tháng 3 năm 2017 của Thủ tướng Chính phủ quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia (sau đây gọi tắt là Quyết định số 05/2017/QĐ-TTg));

Các sự cố của hệ thống thông tin do Bộ Quốc phòng, Bộ Công an quản lý không thuộc phạm vi điều chỉnh của Thông tư này.

2. Đối tượng áp dụng là các cơ quan, tổ chức, cá nhân có liên quan tới hoạt động điều phối, ứng cứu sự cố an toàn thông tin mạng.

Điều 2. Giải thích từ ngữ

1. *Sự cố an toàn thông tin mạng* là việc thông tin, hệ thống thông tin bị tấn công hoặc gây nguy hại, ảnh hưởng tới tính nguyên vẹn, tính bảo mật hoặc tính

khả dụng (sau đây gọi tắt là sự cố).

2. *Ứng cứu sự cố an toàn thông tin mạng* là hoạt động nhằm xử lý, khắc phục sự cố gây mất an toàn thông tin mạng gồm: theo dõi, thu thập, phân tích, phát hiện, cảnh báo, điều tra, xác minh sự cố, ngăn chặn sự cố, khôi phục dữ liệu và khôi phục hoạt động bình thường của hệ thống thông tin.

3. *Đầu mối ứng cứu sự cố* là bộ phận hoặc cá nhân được thành viên mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia cử để thay mặt cho thành viên liên lạc và trao đổi thông tin với Cơ quan điều phối quốc gia về ứng cứu sự cố hoặc các thành viên khác trong hoạt động điều phối, ứng cứu sự cố.

Điều 3. Phân cấp tổ chức thực hiện ứng cứu sự cố bảo đảm an toàn thông tin mạng trên toàn quốc

Phân cấp tổ chức thực hiện ứng cứu sự cố bảo đảm an toàn thông tin mạng trên toàn quốc là các cơ quan, tổ chức, đơn vị thực hiện ứng cứu sự cố bảo đảm an toàn thông tin mạng quốc gia được quy định tại Quyết định số 05/2017/QĐ-TTg. Các cơ quan, tổ chức tham gia hoạt động điều phối, ứng cứu sự cố trên toàn quốc gồm:

1. Bộ Thông tin và Truyền thông - Cơ quan thường trực về ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia (gọi tắt là Cơ quan thường trực quốc gia) và Ban điều phối ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia (gọi tắt là Ban điều phối ứng cứu quốc gia); Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam VNCERT - Cơ quan điều phối quốc gia về ứng cứu sự cố (gọi tắt là Cơ quan điều phối quốc gia).

2. Ban Chỉ đạo ứng cứu khẩn cấp sự cố an toàn thông tin mạng của các Bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ và Ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương (gọi tắt là Ban Chỉ đạo ứng cứu sự cố cấp bộ, tỉnh).

3. Đơn vị chuyên trách về ứng cứu sự cố an toàn thông tin mạng (sau đây gọi tắt là Đơn vị chuyên trách về ứng cứu sự cố); Đội ứng cứu sự cố hoặc bộ phận ứng cứu sự cố tại Bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ và Ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương (sau đây gọi tắt là Đội/bộ phận ứng cứu sự cố).

4. Mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia (gọi tắt là Mạng lưới ứng cứu sự cố); và Ban Điều hành mạng lưới.

5. Chủ quản hệ thống thông tin; đơn vị vận hành hệ thống thông tin; các cơ quan, tổ chức, đơn vị chuyên môn được Cơ quan thường trực, Cơ quan điều phối quốc gia hoặc Ban Chỉ đạo ứng cứu sự cố cấp bộ, tỉnh chỉ định hoặc triệu tập tham gia ứng cứu sự cố.

Điều 4. Nguyên tắc điều phối, ứng cứu sự cố

1. Tuân thủ các quy định pháp luật về điều phối, ứng cứu sự cố an toàn thông tin mạng.

2. Chủ động, kịp thời, nhanh chóng, chính xác, đồng bộ và hiệu quả.

3. Phối hợp chặt chẽ, chính xác, đồng bộ và hiệu quả giữa các cơ quan, tổ chức, doanh nghiệp trong nước và nước ngoài.

4. Ứng cứu sự cố trước hết phải được thực hiện, xử lý bằng lực lượng tại chỗ và trách nhiệm chính của chủ quản hệ thống thông tin.

5. Tuân thủ các điều kiện, nguyên tắc ưu tiên về duy trì hoạt động của hệ thống thông tin đã được cấp thẩm quyền phê duyệt trong kế hoạch ứng phó sự cố.

6. Thông tin trao đổi trong mạng lưới phải được kiểm tra, xác thực đối tượng trước khi thực hiện các bước tác nghiệp tiếp theo.

7. Bảo đảm bí mật thông tin biết được khi tham gia, thực hiện các hoạt động ứng cứu sự cố theo yêu cầu của Cơ quan điều phối quốc gia hoặc cơ quan, tổ chức, cá nhân gặp sự cố.

Chương II

MẠNG LƯỚI ỨNG CỨU SỰ CỐ

Điều 5. Mạng lưới ứng cứu sự cố

1. Mạng lưới ứng cứu sự cố hoạt động trên toàn quốc, gồm thành viên là các đơn vị chuyên trách về ứng cứu sự cố và các cơ quan, tổ chức, doanh nghiệp liên quan được quy định chi tiết tại Điều 7 Quyết định số 05/2017/QĐ-TTg.

2. Mạng lưới ứng cứu sự cố hoạt động theo Quy chế hoạt động của Mạng lưới và hướng dẫn liên quan của Cơ quan điều phối quốc gia (Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam). Ban điều hành mạng lưới do Bộ Thông tin và Truyền thông thành lập theo quy định tại Điều 7 Quyết định số 05/2017/QĐ-TTg.

3. Các thành viên mạng lưới khai báo hồ sơ theo Biểu mẫu số 01 ban hành kèm theo Thông tư này, định kỳ cập nhật hàng năm, gửi Cơ quan điều phối quốc gia. Các tổ chức, doanh nghiệp, cá nhân tự nguyện đăng ký tham gia mạng lưới phải có đơn đăng ký tham gia theo Biểu mẫu số 02, gửi Cơ quan điều phối quốc gia.

Điều 6. Trách nhiệm, quyền hạn của các thành viên mạng lưới

1. Thành viên mạng lưới có các trách nhiệm và quyền hạn sau:

a) Thực hiện các trách nhiệm và quyền hạn quy định tại Quyết định số 05/2017/QĐ-TTg;

b) Cử Đầu mối ứng cứu sự cố có đủ năng lực, trình độ chuyên môn và kỹ năng nghiệp vụ để thực hiện các hoạt động phối hợp ứng cứu sự cố; bảo đảm duy trì liên lạc thông suốt, liên tục 24/7; công bố thông tin về địa chỉ tiếp nhận sự cố trên Trang/Cổng thông tin điện tử; cung cấp, cập nhật thông tin về Đầu mối ứng cứu sự cố, nhân lực kỹ thuật an toàn thông tin, ứng cứu sự cố thuộc phạm vi quản lý tới Cơ quan điều phối quốc gia; cập nhật thông tin về Đầu mối

ứng cứu sự cố, trong vòng 24 giờ khi có thay đổi;

c) Tổng hợp, xây dựng báo cáo định kỳ 06 tháng (trước ngày 20 tháng 6), 01 năm (trước ngày 15 tháng 12) theo Biểu mẫu số 05 gửi Cơ quan điều phối quốc gia; báo cáo đột xuất khi có yêu cầu của Cơ quan điều phối quốc gia;

d) Báo cáo với Cơ quan điều phối quốc gia khi tiếp nhận thông tin, phát hiện các sự cố đối với hệ thống thông tin trong phạm vi quản lý;

đ) Xây dựng và triển khai kế hoạch ứng phó sự cố, hướng dẫn hoạt động ứng cứu sự cố, tổ chức và điều hành hoạt động của Đội ứng cứu sự cố trong phạm vi quản lý;

e) Có quyền đề nghị thành viên mạng lưới hướng dẫn, hỗ trợ xử lý và ứng cứu sự cố khi cần thiết; được tham gia các hội thảo, hội nghị giao ban, tập huấn, bồi dưỡng, đào tạo, huấn luyện, diễn tập và các hoạt động khác trong mạng lưới;

g) Có quyền được chia sẻ thông tin, kinh nghiệm, cảnh báo về sự cố và tình hình an toàn thông tin mạng trong và ngoài nước;

h) Các thành viên mạng lưới là cơ quan, đơn vị chức năng thuộc Bộ Công an và Bộ Quốc phòng không phải thực hiện Điểm c và Điểm d Khoản này.

2. Trách nhiệm và quyền hạn của Cơ quan điều phối quốc gia:

a) Thực hiện các trách nhiệm và quyền hạn quy định tại Quyết định số 05/2017/QĐ-TTg;

b) Công khai trên Trang thông tin điện tử của mình số điện thoại, số fax, địa chỉ thư điện tử (email), đường dây nóng và bảo đảm nguồn lực để duy trì trực đường dây nóng liên tục, kịp thời tiếp nhận và xử lý sự cố; tổng hợp thông tin liên lạc (địa chỉ, số điện thoại, số fax, địa chỉ thư điện tử) và thông tin về đầu mối ứng cứu sự cố, nhân lực kỹ thuật an toàn thông tin, ứng cứu sự cố của các thành viên mạng lưới và Đội ứng cứu sự cố của các thành viên mạng lưới;

c) Xây dựng, triển khai và vận hành cổng thông tin mạng lưới, hệ thống kỹ thuật hỗ trợ cho hoạt động liên lạc, trao đổi thông tin trong mạng lưới và các hệ thống kỹ thuật phục vụ các hoạt động điều phối, ứng cứu, xử lý, khắc phục sự cố;

d) Hướng dẫn hoạt động thông báo và hỏi đáp về sự cố an toàn thông tin mạng trên toàn quốc; điều hành mạng lưới; nghiên cứu, đề xuất các biện pháp nhằm tăng cường nguồn lực cho mạng lưới hoạt động có hiệu quả;

đ) Tập hợp, tiếp nhận, xử lý, chuẩn bị thông tin, cảnh báo tới người có thẩm quyền và các cơ quan, tổ chức, đơn vị liên quan về các nguy cơ, sự cố an toàn thông tin mạng và các biện pháp phòng ngừa, ngăn chặn, xử lý;

e) Tổ chức hội thảo, hội nghị giao ban, phổ biến, trao đổi thông tin, tập huấn, bồi dưỡng, đào tạo, huấn luyện, diễn tập về an toàn thông tin mạng, ứng cứu sự cố; tổ chức các hoạt động chung của mạng lưới.

Điều 7. Các hoạt động chính của mạng lưới ứng cứu sự cố

Ban điều hành mạng lưới tổ chức triển khai các nhiệm vụ của mạng lưới ứng cứu sự cố, gồm các hoạt động chính sau:

1. Nghiên cứu, thu thập, tiếp nhận, phân tích, xác minh, đánh giá, cảnh báo về sự cố, rủi ro an toàn thông tin mạng và phần mềm độc hại.

2. Phối hợp thực hiện ứng cứu, xử lý, ngăn chặn và khắc phục sự cố; kiểm tra, đốc thúc việc xây dựng, triển khai kế hoạch ứng phó sự cố an toàn thông tin mạng và việc thực hiện các trách nhiệm, nghĩa vụ của thành viên mạng lưới;

3. Xây dựng, nâng cao năng lực cho các thành viên mạng lưới và các Đội ứng cứu sự cố, gồm:

a) Huấn luyện, diễn tập, đào tạo, tập huấn nâng cao trình độ, kỹ năng và nghiệp vụ; tổ chức các chuyến công tác trong và ngoài nước để khảo sát, học hỏi kinh nghiệm, trao đổi, hợp tác;

b) Giao ban định kỳ, tổ chức hội thảo, hội nghị, tọa đàm trao đổi và chia sẻ thông tin, kinh nghiệm về điều phối, ứng cứu sự cố, bảo đảm an toàn thông tin mạng;

c) Hỗ trợ xây dựng và áp dụng các quy trình quản lý, vận hành hệ thống thông tin theo các tiêu chuẩn quốc gia, quy chuẩn kỹ thuật quốc gia và tiêu chuẩn quốc tế về an toàn thông tin, ứng cứu sự cố;

d) Tổ chức các nghiên cứu chuyên môn, xây dựng các báo cáo, tài liệu, hướng dẫn, thống kê về an toàn thông tin mạng và các vấn đề liên quan để chia sẻ, phổ biến trong mạng lưới.

4. Tham gia các hoạt động thông tin, tuyên truyền nâng cao nhận thức về phòng ngừa, ứng cứu sự cố, bảo đảm an toàn thông tin mạng.

5. Tổ chức, duy trì hoạt động của Ban điều hành mạng lưới; và triển khai các hoạt động khác liên quan đến điều phối, ứng cứu sự cố, bảo đảm an toàn thông tin mạng.

Chương III
HOẠT ĐỘNG ĐIỀU PHỐI, ỨNG CỨU SỰ CỐ

Điều 8. Hoạt động điều phối ứng cứu sự cố

1. Điều phối ứng cứu sự cố là hoạt động của Cơ quan điều phối quốc gia và cơ quan có thẩm quyền nhằm huy động, điều hành, phối hợp thống nhất các nguồn lực gồm: nhân lực, vật lực (trang thiết bị), tài lực (tài chính, ngân sách) để phòng ngừa, theo dõi, thu thập, phát hiện, cảnh báo sự cố; tiếp nhận, phân tích, xác minh, phân loại sự cố; điều hành, phối hợp, tổ chức ứng cứu sự cố, sẵn sàng, ứng phó, khắc phục sự cố nhằm giảm thiểu các rủi ro, thiệt hại do sự cố gây ra.

2. Cơ quan điều phối quốc gia thực hiện chức năng cảnh báo, điều phối ứng cứu sự cố trên toàn quốc; có quyền huy động, điều phối các thành viên