BỘ THÔNG TIN VÀ TRUYỀN THÔNG

BỘ THÔNG TIN VÀ TRUYỀN THÔNG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 03/2017/TT-BTTTT	*Hà Nội, ngày 24 tháng 4 năm 2017*

THÔNG TƯ
Quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ

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;

Theo đề nghị của Cục trưởng Cục An toàn thông tin,

Bộ trưởng Bộ Thông tin và Truyền thông ban hành Thông tư quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 về bảo đảm an toàn hệ thống thông tin theo cấp độ.

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

1. Thông tư này quy định chi tiết và hướng dẫn bảo đảm an toàn hệ thống thông tin theo cấp độ, bao gồm: Hướng dẫn xác định hệ thống thông tin và cấp độ an toàn hệ thống thông tin; Yêu cầu bảo đảm an toàn hệ thống thông tin theo cấp độ; Kiểm tra, đánh giá an toàn thông tin; Tiếp nhận và thẩm định hồ sơ đề xuất cấp độ; Báo cáo, chia sẻ thông tin.

2. Hệ thống thông tin phục vụ hoạt động quốc phòng, an ninh do Bộ Quốc phòng, Bộ Công an quản lý không thuộc phạm vi điều chỉnh của Thông tư này.

Điều 2. Đối tượng áp dụng

Đối tượng áp dụng Thông tư này được thực hiện theo quy định tại Điều 2 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 (sau đây gọi tắt là Nghị định số 85/2016/NĐ-CP).

Điều 3. Giải thích từ ngữ

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

1. *Xác thực đa nhân tố* là phương pháp xác thực không chỉ dựa vào một mà là kết hợp một số yếu tố liên quan đến người dùng, bao gồm: những thông tin mà người dùng biết (mật khẩu, mã số truy cập,...), những thông tin mà người dùng sở hữu (chứng thư số, thẻ thông minh,...) hoặc những thông tin về sinh trắc học của người dùng (vân tay, mống mắt,...).

2. *Dự phòng nóng* là khả năng thay thế chức năng của thiết bị khi xảy ra sự cố mà không làm gián đoạn hoạt động của hệ thống.

3. *Độ phức tạp cần thiết của mật khẩu* là việc bảo đảm mật khẩu có trên 8 ký tự, trong đó bao gồm cả ký tự chữ cái hoa, chữ cái thường, ký tự đặc biệt và chữ số.

4. *Thiết bị mạng chính hoặc quan trọng* là các thiết bị khi ngừng một phần hay toàn bộ hoạt động mà không có kế hoạch trước sẽ làm gián đoạn hoạt động bình thường của hệ thống thông tin.

Chương II
HƯỚNG DẪN XÁC ĐỊNH HỆ THỐNG THÔNG TIN VÀ CẤP ĐỘ AN TOÀN HỆ THỐNG THÔNG TIN

Điều 4. Hướng dẫn xác định hệ thống thông tin cụ thể

1. Việc xác định hệ thống thông tin để xác định cấp độ căn cứ trên nguyên tắc quy định tại khoản 1 Điều 5 Nghị định số 85/2016/NĐ-CP.

2. Hệ thống thông tin được thiết lập, hình thành thông qua một hoặc một số hình thức sau: Đầu tư xây dựng, thiết lập mới; nâng cấp, mở rộng, tích hợp với hệ thống đã có; thuê hoặc chuyển giao hệ thống.

3. Hệ thống thông tin phục vụ hoạt động nội bộ là hệ thống chỉ phục vụ hoạt động quản trị, vận hành nội bộ của cơ quan, tổ chức, bao gồm:

a) Hệ thống thư điện tử;

b) Hệ thống quản lý văn bản và điều hành;

c) Hệ thống họp, hội nghị truyền hình trực tuyến;

d) Hệ thống quản lý thông tin cụ thể (nhân sự, tài chính, tài sản hoặc lĩnh vực chuyên môn nghiệp vụ cụ thể khác) hoặc hệ thống quản lý thông tin tổng thể (tích hợp quản lý nhiều chức năng, nghiệp vụ khác nhau);

đ) Hệ thống xử lý thông tin nội bộ.

4. Hệ thống thông tin phục vụ người dân, doanh nghiệp là hệ thống trực tiếp hoặc hỗ trợ cung cấp dịch vụ trực tuyến, bao gồm dịch vụ công trực tuyến và dịch vụ trực tuyến khác trong các lĩnh vực viễn thông, công nghệ thông tin, thương mại, tài chính, ngân hàng, y tế, giáo dục và lĩnh vực chuyên ngành khác, bao gồm:

a) Hệ thống thư điện tử;

b) Hệ thống quản lý văn bản và điều hành;

c) Hệ thống một cửa điện tử;

d) Hệ thống trang, cổng thông tin điện tử;

đ) Hệ thống cung cấp hoặc hỗ trợ cung cấp dịch vụ trực tuyến;

e) Hệ thống chăm sóc khách hàng.

5. Hệ thống cơ sở hạ tầng thông tin là tập hợp trang thiết bị, đường truyền dẫn kết nối phục vụ chung hoạt động của nhiều cơ quan, tổ chức, bao gồm:

a) Mạng nội bộ, mạng diện rộng, mạng truyền số liệu chuyên dùng;

b) Hệ thống cơ sở dữ liệu, trung tâm dữ liệu, điện toán đám mây;

c) Hệ thống xác thực điện tử, chứng thực điện tử, chữ ký số;

d) Hệ thống kết nối liên thông, trục tích hợp các hệ thống thông tin.

6. Hệ thống thông tin điều khiển công nghiệp là hệ thống có chức năng giám sát, thu thập dữ liệu, quản lý và kiểm soát các hạng mục quan trọng phục vụ điều khiển, vận hành hoạt động bình thường của các công trình xây dựng, bao gồm:

a) Hệ thống điều khiển lập trình được (PLCs);

b) Hệ thống điều khiển phân tán (DCS);

c) Hệ thống giám sát và thu thập dữ liệu (SCADA).

7. Hệ thống thông tin khác là hệ thống thông tin không thuộc các loại hình trên, được sử dụng để trực tiếp phục vụ hoặc hỗ trợ hoạt động nghiệp vụ, sản xuất, kinh doanh cụ thể của cơ quan, tổ chức theo lĩnh vực chuyên ngành.

Điều 5. Chủ quản hệ thống thông tin

1. Đối với cơ quan, tổ chức nhà nước, chủ quản hệ thống thông tin là một trong các trường hợp sau:

a) Bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ;

b) Ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương;

c) Cấp có thẩm quyền quyết định đầu tư dự án xây dựng, thiết lập, nâng cấp, mở rộng hệ thống thông tin.

2. Đối với doanh nghiệp và tổ chức khác, chủ quản hệ thống thông tin là cấp có thẩm quyền quyết định đầu tư dự án xây dựng, thiết lập, nâng cấp, mở rộng hệ thống thông tin.

3. Chủ quản hệ thống thông tin có thể ủy quyền cho một tổ chức thay mặt mình thực hiện quyền quản lý trực tiếp đối với hệ thống thông tin và trách nhiệm bảo đảm an toàn hệ thống thông tin theo quy định tại khoản 2 Điều 20 Nghị định số 85/2016/NĐ-CP.

Việc ủy quyền phải được thực hiện bằng văn bản, trong đó nêu rõ phạm vi và thời hạn ủy quyền. Tổ chức được ủy quyền phải trực tiếp thực hiện quyền và nghĩa vụ của chủ quản hệ thống thông tin mà không được ủy quyền lại cho bên thứ ba.

Điều 6. Đơn vị vận hành hệ thống thông tin

1. Đơn vị vận hành hệ thống thông tin là cơ quan, tổ chức được chủ quản hệ thống thông tin giao nhiệm vụ vận hành hệ thống thông tin.

2. Trong trường hợp hệ thống thông tin bao gồm nhiều hệ thống thành phần hoặc phân tán, có nhiều hơn một đơn vị vận hành hệ thống thông tin, chủ quản hệ thống thông tin phải có trách nhiệm chỉ định một đơn vị làm đầu mối để thực hiện quyền và nghĩa vụ của đơn vị vận hành hệ thống thông tin theo quy định của pháp luật.

3. Trong trường hợp chủ quản hệ thống thông tin thuê ngoài dịch vụ công nghệ thông tin, đơn vị vận hành hệ thống thông tin là bên cung cấp dịch vụ.

Điều 7. Hướng dẫn xác định và thuyết minh cấp độ an toàn hệ thống thông tin

Việc xác định cấp độ và thuyết minh cấp độ an toàn hệ thống thông tin thực hiện như sau:

1. Xác định và phân loại hệ thống thông tin; xác định chủ quản hệ thống thông tin, đơn vị vận hành hệ thống thông tin căn cứ theo quy định tại các Điều 5, 6 Nghị định số 85/2016/NĐ-CP và các Điều 4, 5, 6 Thông tư này.

2. Xác định loại thông tin được xử lý thông qua hệ thống thông tin căn cứ theo quy định tại khoản 1 Điều 6 Nghị định 85/2016/NĐ-CP.

3. Xác định cấp độ căn cứ theo quy định tại các điều từ Điều 7 đến Điều 11 Nghị định số 85/2016/NĐ-CP. Đối với hệ thống thông tin đề xuất là cấp độ 4 hoặc cấp độ 5, thuyết minh đề xuất cấp độ làm rõ các nội dung sau đây:

a) Xác định các hệ thống thông tin khác có liên quan hoặc có kết nối đến hoặc có ảnh hưởng quan trọng tới hoạt động bình thường của hệ thống thông tin được đề

xuất; trong đó, xác định rõ mức độ ảnh hưởng đến hệ thống thông tin đang được đề xuất cấp độ khi các hệ thống này bị mất an toàn thông tin.

b) Danh mục đề xuất các thành phần, thiết bị mạng quan trọng, các loại thông tin quan trọng được xử lý trong hệ thống (nếu có);

c) Thuyết minh về mức độ quan trọng của các thành phần, thiết bị mạng quan trọng, các loại thông tin, dữ liệu được xử lý hoặc lưu trữ trên hệ thống (nếu có);

d) Thuyết minh về các nguy cơ tấn công mạng, mất an toàn thông tin đối với hệ thống, các thành phần hệ thống và các thiết bị mạng quan trọng; ảnh hưởng của các nguy cơ tấn công mạng, mất an toàn thông tin này đối với các tiêu chí xác định cấp độ theo Điều 10, 11 Nghị định số 85/2016/NĐ-CP;

đ) Đánh giá phạm vi và mức độ ảnh hưởng tới lợi ích công cộng, trật tự an toàn xã hội hoặc quốc phòng, an ninh quốc gia khi bị tấn công mạng gây mất an toàn thông tin hoặc gián đoạn hoạt động của từng hệ thống đã được xác định.

Đối với hệ thống thông tin cấp độ 4, thuyết minh yêu cầu cần phải vận hành 24/7 và không chấp nhận ngừng vận hành mà không có kế hoạch trước;

e) Thuyết minh khác (nếu có) trên cơ sở thực tế hoạt động của hệ thống thông tin.

Chương III
YÊU CẦU BẢO ĐẢM AN TOÀN HỆ THỐNG THÔNG TIN THEO CẤP ĐỘ

Điều 8. Yêu cầu chung

1. Việc bảo đảm an toàn hệ thống thông tin theo cấp độ thực hiện theo yêu cầu cơ bản quy định tại Thông tư này; tiêu chuẩn, quy chuẩn kỹ thuật về an toàn thông tin và tiêu chuẩn, quy chuẩn kỹ thuật chuyên ngành có liên quan khác.

2. Yêu cầu cơ bản đối với từng cấp độ quy định tại Thông tư này là yêu cầu tối thiểu để bảo đảm an toàn hệ thống thông tinvà không bao gồm các yêu cầu bảo đảm an toàn vật lý.

3. Yêu cầu cơ bản bao gồm:

a) Yêu cầu kỹ thuật: An toàn hạ tầng mạng; an toàn máy chủ; an toàn ứng dụng và an toàn dữ liệu;

b) Yêu cầu quản lý: Chính sách chung; tổ chức, nhân sự; quản lý thiết kế, xây dựng; quản lý vận hành; kiểm tra, đánh giá và quản lý rủi ro.

4. Việc xây dựng phương án bảo đảm an toàn thông tin đáp ứng yêu cầu cơ bản theo từng cấp độ thực hiện theo nguyên tắc quy định tại khoản 2 Điều 4 Nghị định số 85/2016/NĐ-CP, cụ thể như sau:

a) Đối với hệ thống thông tin cấp độ 1, 2, 3: Phương án bảo đảm an toàn thông tin phải xem xét khả năng dùng chung giữa các hệ thống thông tin đối với các giải pháp bảo vệ, chia sẻ tài nguyên để tối ưu hiệu năng, tránh đầu tư thừa, trùng lặp, lãng phí. Trong trường hợp đầu tư mới, phải có thuyết minh về việc giải pháp đã có không đáp ứng được yêu cầu cơ bản;

b) Đối với hệ thống thông tin cấp độ 4, 5: Phương án bảo đảm an toàn thông tin cần được thiết kế bảo đảm tính sẵn sàng, phân tách và hạn chế ảnh hưởng đến toàn bộ hệ thống khi một thành phần trong hệ thống hoặc có liên quan tới hệ thống bị mất an toàn thông tin.

Điều 9. Yêu cầu cơ bản đối với từng cấp độ

1. Phương án bảo đảm an toàn hệ thống thông tin cấp độ 1 phải đáp ứng yêu cầu quy định chi tiết tại Phụ lục 1 ban hành kèm theo Thông tư này.

2. Phương án bảo đảm an toàn hệ thống thông tin cấp độ 2 phải đáp ứng yêu cầu như đối với cấp độ 1 và bổ sung yêu cầu quy định chi tiết tại Phụ lục 2 ban hành kèm theo Thông tư này.

3. Phương án bảo đảm an toàn hệ thống thông tin cấp độ 3 phải đáp ứng yêu cầu như đối với cấp độ 2 và bổ sung yêu cầu quy định chi tiết tại Phụ lục 3 ban hành kèm theo Thông tư này.

4. Phương án bảo đảm an toàn hệ thống thông tin cấp độ 4 phải đáp ứng yêu cầu như đối với cấp độ 3 và bổ sung yêu cầu quy định chi tiết tại Phụ lục 4 ban hành kèm theo Thông tư này.

5. Phương án bảo đảm an toàn hệ thống thông tin cấp độ 5 phải đáp ứng yêu cầu như đối với cấp độ 4 và bổ sung yêu cầu quy định chi tiết tại Phụ lục 5 ban hành kèm theo Thông tư này.

Chương IV
KIỂM TRA, ĐÁNH GIÁ AN TOÀN THÔNG TIN

Điều 10. Nội dung, hình thức kiểm tra, đánh giá

1. Nội dung kiểm tra, đánh giá:

a) Kiểm tra việc tuân thủ quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ;

b) Đánh giá hiệu quả của biện pháp bảo đảm an toàn hệ thống thông tin;

c) Đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống;

d) Kiểm tra, đánh giá khác do chủ quản hệ thống thông tin quy định.

2. Hình thức kiểm tra, đánh giá:

a) Kiểm tra, đánh giá định kỳ theo kế hoạch của chủ quản hệ thống thông tin;

b) Kiểm tra, đánh giá đột xuất theo yêu cầu của cấp có thẩm quyền.

3. Cấp có thẩm quyền yêu cầu kiểm tra, đánh giá:

a) Bộ trưởng Bộ Thông tin và Truyền thông;

b) Chủ quản hệ thống thông tin đối với hệ thống thông tin thuộc thẩm quyền quản lý;

c) Đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin đối với hệ thống thông tin do đơn vị này phê duyệt hồ sơ đề xuất cấp độ.

4. Đơn vị chủ trì kiểm tra, đánh giá là đơn vị được cấp có thẩm quyền giao nhiệm vụ hoặc được lựa chọn để thực hiện nhiệm vụ kiểm tra, đánh giá.

5. Đối tượng kiểm tra, đánh giá là chủ quản hệ thống thông tin hoặc đơn vị vận hành hệ thống thông tin và các hệ thống thông tin có liên quan.

Điều 11. Kiểm tra việc tuân thủ quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ

1. Kiểm tra việc tuân thủ quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ bao gồm:

a) Kiểm tra việc tuân thủ quy định của pháp luật về xác định cấp độ an toàn hệ thống thông tin;

b) Kiểm tra việc tuân thủ quy định của pháp luật về thực hiện phương án bảo đảm an toàn hệ thống thông tin theo cấp độ.

2. Đơn vị chủ trì kiểm tra là một trong những đơn vị sau đây:

a) Cục An toàn thông tin;

b) Đơn vị chuyên trách về an toàn thông tin.

3. Kế hoạch kiểm tra định kỳ bao gồm các nội dung sau:

a) Danh sách các đơn vị, hệ thống thông tin (nếu có) sẽ tiến hành kiểm tra;

b) Phạm vi và nội dung kiểm tra;

c) Thời gian tiến hành kiểm tra;

d) Đơn vị phối hợp kiểm tra (nếu có).

4. Quyết định kiểm tra được lập sau khi kế hoạch kiểm tra định kỳ được cấp có thẩm quyền phê duyệt hoặc khi có kiểm tra đột xuất của cấp có thẩm quyền.

5. Đối với kiểm tra định kỳ:

a) Đơn vị chủ trì kiểm tra lập kế hoạch kiểm tra định kỳ cho năm sau trình cấp có thẩm quyền phê duyệt để làm cơ sở triển khai thực hiện;

b) Trường hợp có thay đổi so với kế hoạch kiểm tra định kỳ đã được phê duyệt, đơn vị chủ trì kiểm tra lập kế hoạch kiểm tra định kỳ điều chỉnh trình cấp có thẩm quyền phê duyệt điều chỉnh;

c) Kế hoạch kiểm tra định kỳ được gửi cho đối tượng kiểm tra và cơ quan cấp trên của đối tượng kiểm tra trong thời hạn tối đa 10 ngày kể từ ngày được phê duyệt nhưng tối thiểu 10 ngày trước ngày tiến hành kiểm tra.

6. Đối với kiểm tra đột xuất:

Căn cứ yêu cầu kiểm tra đột xuất, quyết định kiểm tra, Trưởng đoàn kiểm tra quy định các nội dung kiểm tra cho phù hợp.

7. Sau khi kết thúc kiểm tra trực tiếp tại cơ sở, Đoàn kiểm tra có trách nhiệm thông báo cho đối tượng kiểm tra biết và bàn giao tài liệu, trang thiết bị sử dụng (nếu có) trong quá trình kiểm tra.

Đoàn kiểm tra có trách nhiệm dự thảo Báo cáo kiểm tra, gửi cho đối tượng kiểm tra để lấy ý kiến. Trong thời hạn 05 ngày kể từ ngày nhận được dự thảo Báo cáo kiểm tra, đối tượng kiểm tra có trách nhiệm có ý kiến đối với các nội dung dự thảo.

8. Trên cơ sở dự thảo Báo cáo kiểm tra, ý kiến tiếp thu giải trình của đối tượng kiểm tra, trong thời hạn 30 ngày kể từ ngày kết thúc kiểm tra tại cơ sở, Đoàn kiểm tra hoàn thiện Báo cáo kiểm tra và dự thảo kết luận kiểm tra trình cấp có thẩm quyền yêu cầu kiểm tra xem xét, phê duyệt.

Kết luận kiểm tra phải gửi cho đối tượng kiểm tra và cơ quan quản lý cấp trên của đối tượng kiểm tra (nếu có) và các đơn vị có liên quan (nếu cần thiết).

Điều 12. Đánh giá hiệu quả của biện pháp bảo đảm an toàn thông tin

1. Đánh giá hiệu quả của biện pháp bảo đảm an toàn thông tin là việc rà soát một cách tổng thể, xác minh mức độ hiệu quả của phương án bảo đảm an toàn thông tin theo từng tiêu chí, yêu cầu cơ bản cụ thể.

Đánh giá hiệu quả của biện pháp bảo đảm an toàn thông tin đã được áp dụng là cơ sở để tiến hành điều chỉnh phương án bảo đảm an toàn thông tin cho phù hợp với yêu cầu thực tiễn.

2. Đơn vị chủ trì đánh giá là một trong những tổ chức sau đây:

a) Cục An toàn thông tin;

b) Đơn vị chuyên trách về an toàn thông tin;

c) Tổ chức sự nghiệp nhà nước có chức năng, nhiệm vụ phù hợp;

d) Doanh nghiệp đã được cấp phép cung cấp dịch vụ kiểm tra, đánh giá an toàn thông tin mạng.

3. Đơn vị vận hành hệ thống thông tin lập kế hoạch đánh giá định kỳ cho năm sau trình cấp có thẩm quyền phê duyệt để làm cơ sở triển khai thực hiện. Kế hoạch đánh giá bao gồm:

a) Danh sách các đơn vị, hệ thống thông tin sẽ tiến hành đánh giá;

b) Thời gian tiến hành đánh giá;

c) Đơn vị thực hiện: Tự thực hiện hoặc do đơn vị chuyên trách về an toàn thông tin thực hiện hoặc thuê ngoài theo quy định của pháp luật.

4. Trường hợp có thay đổi so với kế hoạch đánh giá đã được phê duyệt, đơn vị vận hành hệ thống thông tin lập kế hoạch đánh giá điều chỉnh trình cấp có thẩm quyền phê duyệt điều chỉnh.

5. Sau khi kết thúc kiểm tra trực tiếp tại cơ sở, đơn vị chủ trì đánh giá có trách nhiệm thông báo cho đơn vị vận hành hệ thống thông tin biết và bàn giao tài liệu, trang thiết bị sử dụng (nếu có) trong quá trình kiểm tra.

Đơn vị chủ trì đánh giá có trách nhiệm dự thảo Báo cáo đánh giá, gửi cho đơn vị vận hành hệ thống thông tin để lấy ý kiến. Trong thời hạn 05 ngày kể từ ngày nhận được dự thảo Báo cáo đánh giá, đơn vị vận hành hệ thống thông tin có trách nhiệm có ý kiến đối với các nội dung dự thảo.

6. Trên cơ sở dự thảo Báo cáo đánh giá, ý kiến của đơn vị vận hành hệ thống thông tin, đơn vị chủ trì đánh giá hoàn thiện Báo cáo đánh giá, gửi đơn vị vận hành và chủ quản hệ thống thông tin.

Điều 13. Đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống

1. Đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống là việc thực hiện dò quét, phát hiện lỗ hổng, điểm yếu của hệ thống, thử nghiệm tấn công xâm nhập hệ thống và đánh giá nguy cơ, thiệt hại có thể có của hệ thống thông tin khi bị đối tượng tấn công xâm nhập.

2. Đơn vị chủ trì đánh giá là một trong những tổ chức sau đây:

a) Cục An toàn thông tin;

b) Đơn vị chuyên trách về an toàn thông tin;

c) Tổ chức sự nghiệp nhà nước có chức năng, nhiệm vụ phù hợp;

d) Doanh nghiệp đã được cấp phép cung cấp dịch vụ kiểm tra, đánh giá an toàn thông tin mạng hoặc tổ chức khác được chủ quản hệ thống thông tin cho phép thực hiện đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống.

3. Đơn vị chủ trì đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống có trách nhiệm:

a) Thông báo cho chủ quản hệ thống thông tin về điểm yếu an toàn thông tin phát hiện ra nhằm khắc phục, phòng tránh các sự cố an toàn thông tin;

b) Thực hiện công tác bảo đảm an toàn cho dữ liệu liên quan đến hệ thống được đánh giá, không công bố dữ liệu liên quan khi chưa được sự đồng ý của chủ quản hệ thống thông tin;

c) Việc đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống phải bảo đảm không ảnh hưởng đến hoạt động bình thường của hệ thống.

Chương V
TIẾP NHẬN VÀ THẨM ĐỊNH HỒ SƠ ĐỀ XUẤT CẤP ĐỘ

Điều 14. Nộp và tiếp nhận hồ sơ đề xuất cấp độ để thẩm định

1. Đối với hệ thống thông tin được đề xuất cấp độ 1, 2, 3:

Đơn vị vận hành hệ thống thông tin gửi 01 bản chính và 02 bản sao hợp lệ hồ sơ đề xuất cấp độ tới đơn vị chuyên trách về an toàn thông tin để thẩm định.

2. Đối với hệ thống thông tin được đề xuất cấp độ 4, 5:

a) Chủ quản hệ thống thông tin gửi 01 bản chính và 04 bản sao hợp lệ hồ sơ đề xuất cấp độ về Bộ Thông tin và Truyền thông (Cục An toàn thông tin) để thẩm định;

b) Tổ chức tiếp nhận hồ sơ và địa chỉ tiếp nhận hồ sơ đối với hệ thống thông tin được đề xuất cấp độ 4, 5:

Bộ Thông tin và Truyền thông (Cục An toàn thông tin), Tầng 8, Tòa nhà 115 Trần Duy Hưng, Quận Cầu Giấy, Hà Nội.

Trong trường hợp thay đổi địa chỉ tiếp nhận hồ sơ, Cục An toàn thông tin thông báo công khai việc thay đổi địa chỉ theo quy định.

3. Trong vòng 05 ngày làm việc kể từ ngày tiếp nhận, tổ chức tiếp nhận hồ sơ đề xuất cấp độ kiểm tra tính hợp lệ của hồ sơ. Trong trường hợp hồ sơ không hợp lệ, tổ chức tiếp nhận hồ sơ đề xuất cấp độ thông báo bằng văn bản cho tổ chức nộp hồ sơ biết để bổ sung, hoàn thiện hồ sơ.

Điều 15. Tổ chức thẩm định hồ sơ đề xuất cấp độ

1. Đối với hệ thống thông tin được đề xuất cấp độ 1, 2, 3:

Đơn vị chuyên trách về an toàn thông tin thực hiện thẩm định hồ sơ đề xuất cấp độ theo quy định tại Điều 16 Nghị định số 85/2016/NĐ-CP.

Trong quá trình thẩm định, trong trường hợp cần thiết, đơn vị chuyên trách về an toàn thông tin lấy ý kiến bằng văn bản của các đơn vị liên quan.

2. Đối với hệ thống thông tin được đề xuất cấp độ 4, 5:

Bộ Thông tin và Truyền thông thực hiện thẩm định hồ sơ đề xuất cấp độ theo quy định tại Điều 16 Nghị định số 85/2016/NĐ-CP. Việc tổ chức thẩm định hồ sơ đề xuất cấp độ được thực hiện theo quy trình sau:

a) Cục An toàn thông tin lấy ý kiến bằng văn bản của Vụ Pháp chế và đơn vị liên quan khác thuộc Bộ Thông tin và Truyền thông trong trường hợp cần thiết theo chức năng, nhiệm vụ của các đơn vị;

b) Bộ Thông tin và Truyền thông lấy ý kiến bằng văn bản của Bộ Quốc phòng, Bộ Công an theo quy định;

c) Căn cứ ý kiến bằng văn bản của Bộ Quốc phòng, Bộ Công an và các đơn vị liên quan, trong trường hợp cần thiết, Bộ Thông tin và Truyền thông thành lập Hội đồng thẩm định để trao đổi, thảo luận, cho ý kiến cụ thể. Chủ tịch Hội đồng thẩm định do Bộ trưởng Bộ Thông tin và Truyền thông phân công, đại diện Lãnh đạo Cục An toàn thông tin, Vụ Pháp chế, Trung tâm VNCERT - Bộ Thông tin và Truyền thông, đại diện Lãnh đạo đơn vị chức năng của Bộ Công an, Bộ Quốc phòng và một số chuyên gia độc lập (nếu cần thiết) làm thành viên.

Điều 16. Cơ chế phối hợp thẩm định

1. Đơn vị vận hành hệ thống thông tin có trách nhiệm phối hợp với đơn vị thẩm định hồ sơ đề xuất cấp độ trong việc xác định sự phù hợp của hồ sơ đề xuất cấp độ đối với yêu cầu hoạt động của hệ thống thông tin tương ứng.

2. Trong trường hợp cần thiết, đơn vị thẩm định hồ sơ đề xuất cấp độ thực hiện kiểm tra, đánh giá thực tế các phương án bảo đảm an toàn hệ thống thông tin theo cấp độ được đề xuất. Việc kiểm tra, đánh giá bảo đảm không gây ảnh hưởng đến hoạt động bình thường của hệ thống thông tin và có thông báo cho chủ quản hệ thống thông tin, đơn vị vận hành khi phát hiện các điểm yếu an toàn thông tin cần khắc phục.

Chương VI
BÁO CÁO, CHIA SẺ THÔNG TIN

Điều 17. Chế độ báo cáo

1. Chủ quản hệ thống thông tin cấp độ 1, 2 chỉ đạo đơn vị vận hành hệ thống thông tin thực hiện chế độ báo cáo định kỳ hoặc đột xuất theo quy định tại khoản 4 Điều 22 Nghị định số 85/2016/NĐ-CP.

2. Chủ quản hệ thống thông tin cấp độ 3, 4, 5 thực hiện chế độ báo cáo định kỳ hàng năm hoặc báo cáo đột xuất theo yêu cầu của Bộ Thông tin và Truyền thông.

3. Nội dung báo cáo:

a) Tình hình an toàn thông tin của hệ thống thông tin trong kỳ báo cáo;

b) Tiến độ triển khai, áp dụng phương án bảo đảm an toàn hệ thống thông tin theo hồ sơ xác định cấp độ đã được phê duyệt;

c) Hiệu quả áp dụng phương án bảo đảm an toàn hệ thống thông tin theo hồ sơ xác định cấp độ đã được phê duyệt;

d) Đề xuất thay đổi cấp độ, phương án bảo đảm an toàn hệ thống thông tin (nếu có);

đ) Nội dung khác phục vụ công tác bảo đảm an toàn hệ thống thông tin theo cấp độ.

4. Báo cáo định kỳ gửi về Bộ Thông tin và Truyền thông (Cục An toàn thông tin) trước ngày 30 tháng 11 hàng năm.

Điều 18. Chia sẻ thông tin

1. Chủ quản hệ thống thông tin, đơn vị vận hành hệ thống thông tin cấp 4, 5 và chủ quản hệ thống thông tin là cơ quan, tổ chức nhà nước có trách nhiệm tham gia chia sẻ thông tin với cơ quan quản lý nhà nước về an toàn thông tin đối với công tác bảo đảm an toàn thông tin. Các chủ quản hệ thống thông tin, đơn vị vận hành hệ thống thông tin còn lại tham gia chia sẻ thông tin trên tinh thần tự nguyện.

2. Thông tin được chia sẻ thông qua các hình thức trực tiếp, thư điện tử, văn bản, hệ thống chia sẻ thông tin được vận hành bởi Bộ Thông tin và Truyền thông. Đối với thông tin được xác định là thông tin bí mật nhà nước, việc chia sẻ thông tin thực hiện theo quy định của pháp luật về bảo vệ bí mật nhà nước.

3. Việc chia sẻ thông tin dựa trên nguyên tắc bí mật, chọn lọc và bảo đảm lợi ích của các bên tham gia. Đơn vị nhận thông tin được chia sẻ có trách nhiệm bảo vệ bí mật nguồn gốc, nội dung thông tin theo thống nhất giữa các bên tham gia chia sẻ thông tin.

4. Việc chia sẻ thông tin được thực hiện ít nhất mỗi quý một lần và phù hợp với thực tế hoạt động của hệ thống thông tin tương ứng.

5. Các thông tin được chia sẻ bao gồm:

a) Thông tin chưa được phân tích hoặc đã được phân tích về nguy cơ mất an toàn thông tin; thông tin về các cuộc tấn công mạng đã xảy ra:

- Các loại hình tấn công mạng ghi nhận được tại hệ thống;

- Số lượng các sự kiện tấn công mạng ghi nhận được tại hệ thống;

- Mẫu dữ liệu tấn công mạng thu thập được;

- Các dữ liệu khác theo thống nhất của các bên tham gia chia sẻ thông tin.

b) Các hoạt động bảo đảm an toàn hệ thống thông tin như tuyên truyền, đào tạo, diễn tập và các thông tin khác.

Chương VII
TỔ CHỨC THỰC HIỆN

Điều 19. Hiệu lực thi hành

1. Thông tư này có hiệu lực thi hành kể từ ngày 01 tháng 7 năm 2017.

2. Trong quá trình thực hiện Thông tư này, nếu có vướng mắc, các cơ quan, đơn vị liên hệ với Bộ Thông tin và Truyền thông (Cục An toàn thông tin) để phối hợp giải quyết./.

BỘ TRƯỞNG

Trương Minh Tuấn

PHỤ LỤC 1

YÊU CẦU CƠ BẢN BẢO ĐẢM AN TOÀN HỆ THỐNG THÔNG TIN ĐỐI VỚI HỆ THỐNG THÔNG TIN CẤP ĐỘ 1

(Ban hành kèm theo Thông tư số 03/2017/TT-BTTTT ngày 24 tháng 4 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông)

1. Yêu cầu kỹ thuật:

a) An toàn máy chủ:

- Có xác thực bằng cơ chế mật khẩu và ghi nhật ký hệ thống đối với hoạt động truy cập, quản trị máy chủ;

- Không sử dụng kết nối không được mã hóa trong việc quản trị máy chủ từ xa;

b) An toàn ứng dụng:

Có xác thực bằng cơ chế mật khẩu và ghi nhật ký đối với hoạt động truy cập ứng dụng và đăng nhập chức năng quản trị;

c) An toàn dữ liệu:

Có sao lưu dự phòng định kỳ dữ liệu trên hệ thống tùy theo yêu cầu, mục đích sử dụng.

2. Yêu cầu quản lý:

a) Chính sách chung: Có chính sách an toàn thông tin cho đối tượng quản trị, vận hành hệ thống;

b) Tổ chức, nhân sự: Có đầu mối liên hệ để thông báo, trao đổi, xử lý vấn đề phát sinh hoặc sự cố mất an toàn thông tin xảy ra với hệ thống thông tin.

PHỤ LỤC 2

YÊU CẦU CƠ BẢN BẢO ĐẢM AN TOÀN HỆ THỐNG THÔNG TIN ĐỐI VỚI HỆ THỐNG THÔNG TIN CẤP ĐỘ 2

(Ban hành kèm theo Thông tư số 03/2017/TT-BTTTT ngày 24 tháng 4 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông)

1. Yêu cầu kỹ thuật:

a) An toàn hạ tầng mạng:

- Có phân vùng hạ tầng mạng thành các vùng mạng khác nhau tùy theo yêu cầu, mục đích sử dụng;

- Có phương án sử dụng thiết bị có chức năng tường lửa để ngăn chặn truy cập trái phép giữa các vùng mạng với mạng Internet;

- Có cơ chế xác thực và mã hóa khi sử dụng mạng không dây (nếu có);

- Có phương án xác thực tài khoản quản trị trên các thiết bị mạng quan trọng;

- Có phương án quản trị các thiết bị từ xa (nếu có) thông qua các giao thức hỗ trợ mã hóa;

b) An toàn máy chủ:

- Có sử dụng phần mềm phòng, chống mã độc trên máy chủ và có cơ chế tự động cập nhật phiên bản mới hoặc dấu hiệu nhận dạng mã độc mới cho phần mềm này;

- Có cơ chế xác thực bằng mật khẩu bảo đảm độ phức tạp cần thiết, yêu cầu thay đổi mật khẩu định kỳ theo quy định của tổ chức và có cơ chế phòng chống dò quét mật khẩu; Các thông tin xác thực phải được lưu trữ trên hệ thống dưới dạng mã hóa;

- Có phương án vô hiệu hóa các tài khoản mặc định hoặc không hoạt động trên hệ thống; vô hiệu hóa các dịch vụ, phần mềm không sử dụng trên máy chủ;

- Có ghi nhật ký hệ thống đối với hoạt động truy cập, quản trị máy chủ;

- Có thiết lập cơ chế cập nhật bản vá điểm yếu an toàn thông tin cho hệ điều hành và các dịch vụ hệ thống trên máy chủ;

c) An toàn ứng dụng:

- Có thiết lập yêu cầu bảo đảm mật khẩu trên ứng dụng đủ độ phức tạp cần thiết để hạn chế tấn công dò quét mật khẩu; các thông tin xác thực phải được lưu trữ dưới dạng mã hóa;

- Có thiết lập yêu cầu ghi nhật ký truy cập, lỗi phát sinh;

- Không sử dụng kết nối mạng không mã hóa trong việc quản trị ứng dụng từ xa.

d) An toàn dữ liệu: Có phương án sử dụng hệ thống hoặc phương tiện lưu trữ độc lập để sao lưu dự phòng các dữ liệu quan trọng trên máy chủ. Việc sao lưu được thực hiện định kỳ theo quy định của tổ chức.

2. Yêu cầu quản lý:

a) Chính sách chung:

- Có chính sách an toàn thông tin cho người sử dụng bao gồm các nội dung: chính sách truy cập và sử dụng mạng và tài nguyên trên Internet; truy cập và sử dụng ứng dụng;

- Có chính sách an toàn thông tin cho người quản trị, vận hành hệ thống bao gồm nhưng không giới hạn bởi chính sách quản lý an toàn hạ tầng mạng, an toàn máy chủ, an toàn ứng dụng và an toàn dữ liệu;

b) Tổ chức, nhân sự:

Có quy trình, thủ tục để cấp phát, loại bỏ tài khoản, quyền truy cập của cán bộ mới tham gia sử dụng hệ thống, cán bộ thay đổi nhiệm vụ hoặc cán bộ ngừng sử dụng hệ thống;

c) Quản lý thiết kế, xây dựng:

- Có tài liệu thiết kế, mô tả về các phương án bảo đảm an toàn hệ thống thông tin;

- Có phương án kiểm tra, xác minh hệ thống được triển khai tuân thủ theo đúng tài liệu thiết kế và yêu cầu bảo đảm an toàn thông tin trước khi nghiệm thu, bàn giao;

- Có hồ sơ cấp độ được thẩm định, phê duyệt bởi đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin;

d) Quản lý vận hành:

- Có quy trình quản lý, vận hành hệ thống phù hợp yêu cầu kỹ thuật cơ bản; quản lý sự thay đổi, di chuyển hệ thống; kết thúc vận hành, khai thác, thanh lý, hủy bỏ hệ thống;

- Có phương án ứng cứu sự cố trong tình huống xảy ra sự cố an toàn thông tin;

đ) Kiểm tra, đánh giá và quản lý rủi ro:

- Có phương án định kỳ 02 năm hoặc đột xuất khi cần thiết thực hiện kiểm tra, đánh giá an toàn thông tin và quản lý rủi ro an toàn thông tin theo quy định của pháp luật;

- Việc kiểm tra, đánh giá an toàn thông tin và đánh giá rủi ro phải do đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin thực hiện hoặc thuê ngoài thực hiện theo quy định của pháp luật.

PHỤ LỤC 3

YÊU CẦU CƠ BẢN BẢO ĐẢM AN TOÀN HỆ THỐNG THÔNG TIN ĐỐI VỚI HỆ THỐNG THÔNG TIN CẤP ĐỘ 3

(Ban hành kèm theo Thông tư số 03/2017/TT-BTTTT ngày 24 tháng 4 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông)

1. Yêu cầu kỹ thuật:

a) An toàn hạ tầng mạng:

- Có thiết kế vùng mạng dành riêng bao gồm vùng mạng riêng cho máy chủ nội bộ, vùng mạng riêng cho các máy chủ cung cấp các dịch vụ hệ thống cần thiết (như dịch vụ DNS, DHCP, NTP và các dịch vụ khác), vùng mạng riêng cho máy chủ cơ sở dữ liệu và các vùng mạng riêng khác theo yêu cầu của tổ chức;

- Có thiết kế vùng mạng nội bộ thành các mạng chức năng riêng theo yêu cầu nghiệp vụ; phân vùng mạng riêng cho mạng không dây tách biệt với các vùng mạng chức năng; phân vùng mạng riêng cho các máy chủ cung cấp dịch vụ ra ngoài mạng Internet;

- Có phương án cân bằng tải và giảm thiểu tấn công từ chối dịch vụ;

- Có thiết kế hệ thống quản lý lưu trữ tập trung và giám sát an toàn thông tin;

- Có phương án sử dụng thiết bị có chức năng tường lửa giữa các vùng mạng quan trọng;

- Có phương án phát hiện, phòng chống xâm nhập và chặn lọc phần mềm độc hại giữa mạng Internet và các mạng bên trong;

- Có lưu trữ nhật ký các thiết bị mạng và quản lý tập trung trong vùng mạng quản trị đối với các thiết bị mạng có hỗ trợ tính năng này hoặc thiết bị mạng quan trọng;

- Có lưu trữ tối thiểu trong 03 tháng đối với nhật ký của các thiết bị mạng và bảo đảm đồng bộ thời gian nhật ký với máy chủ thời gian thực theo múi giờ Việt Nam;

- Có thiết kế dự phòng cho các thiết bị mạng chính trong hệ thống bảo đảm duy trì hoạt động bình thường của hệ thống khi một thiết bị mạng gặp sự cố;

- Có phương án cập nhật phần mềm, xử lý điểm yếu an toàn thông tin và cấu hình tối ưu thiết bị mạng trước khi đưa vào sử dụng trong mạng;

- Có phương án xác thực tài khoản quản trị trên tất cả các thiết bị mạng trong đó bảo đảm yêu cầu về mật khẩu có độ phức tạp cần thiết, phòng chống dò quét mật khẩu;

- Có phương án giới hạn các nguồn truy cập, quản trị các thiết bị mạng;

- Có phương án chỉ cho phép quản trị các thiết bị mạng thông qua mạng Internet bằng mạng riêng ảo hoặc các phương pháp khác tương đương;

- Có ghi nhật ký đối với các hoạt động trên thiết bị mạng nội bộ và bảo đảm đồng bộ thời gian nhật ký với máy chủ thời gian;

- Có mã hóa thông tin xác thực lưu trên thiết bị mạng;

b) An toàn máy chủ:

- Có phương án quản lý xác thực tập trung; chống đăng nhập tự động và tự động hủy phiên đăng nhập sau một khoảng thời gian chờ phù hợp với chính sách của tổ chức;

- Có thiết lập quyền truy cập, quản trị, sử dụng tài nguyên của từng tài khoản trên hệ thống phù hợp với nhiệm vụ, yêu cầu nghiệp vụ khác nhau;

- Có phương án quản lý bản vá, nâng cấp phần mềm hệ thống tập trung;

- Có phương án lưu trữ và quản lý tập trung nhật ký máy chủ. Nhật ký được lưu tối thiểu 03 tháng;

- Có phương án đồng bộ nhật ký máy chủ với hệ thống giám sát an toàn thông tin;

- Có phương án giới hạn các nguồn cho phép truy cập, quản trị máy chủ; việc quản trị máy chủ thông qua mạng Internet phải sử dụng mạng riêng ảo hoặc các phương pháp khác tương đương;

- Có phương án sử dụng tường lửa trên từng máy chủ nhằm thiết lập chỉ cho phép các kết nối hợp pháp theo các dịch vụ được máy chủ cung cấp;

- Có phương án sao lưu dự phòng hệ điều hành máy chủ, cấu hình máy chủ phù hợp với yêu cầu của tổ chức;

- Có ghi nhật ký đối với các hoạt động truy cập, quản trị, phát sinh lỗi;

c) An toàn ứng dụng:

- Có thiết lập yêu cầu thay đổi mật khẩu định kỳ đối với tài khoản quản trị ứng dụng; giới hạn thời gian chờ để đóng phiên kết nối khi ứng dụng không nhận được yêu cầu từ người dùng;

- Có thiết lập tách biệt ứng dụng quản trị với ứng dụng cung cấp dịch vụ cho người sử dụng và bảo đảm ứng dụng hoạt động với quyền tối thiểu trên hệ thống;

- Có phương án giới hạn các nguồn cho phép truy cập, quản trị ứng dụng; việc quản trị ứng dụng thông qua mạng Internet phải sử dụng mạng riêng ảo hoặc các phương pháp khác tương đương;

- Có phương án kiểm tra, lọc các dữ liệu đầu vào từ phía người sử dụng, bảo đảm các dữ liệu này không ảnh hưởng đến an toàn thông tin của ứng dụng.

d) An toàn dữ liệu:

- Có phương án mã hóa dữ liệu lưu trữ (không phải là thông tin, dữ liệu công khai) trên hệ thống lưu trữ/phương tiện lưu trữ;

- Có phương án tự động sao lưu dự phòng đối với thông tin/dữ liệu phù hợp với tần suất thay đổi của dữ liệu;

2. Yêu cầu quản lý:

a) Chính sách chung: Định kỳ 02 năm hoặc đột xuất khi cần thiết thực hiện rà soát, cập nhật chính sách chung về an toàn thông tin;

b) Tổ chức, nhân sự:

- Có kế hoạch và định kỳ tổ chức đào tạo, bồi dưỡng, tuyên truyền, phổ biến nâng cao kiến thức, kỹ năng về an toàn thông tin cho cán bộ quản lý và cán bộ kỹ thuật có liên quan;

- Có chính sách yêu cầu cán bộ liên quan khi thôi việc cần cam kết giữ bí mật thông tin liên quan đến dữ liệu trên hệ thống, thông tin riêng của tổ chức hoặc thông tin nhạy cảm khác;

c) Thiết kế, xây dựng hệ thống:

Có hồ sơ đề xuất cấp độ được thẩm định bởi đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin;

d) Quản lý vận hành:

- Có phương án giám sát an toàn thông tin cho hệ thống trong quá trình vận hành theo quy định của pháp luật;

- Có kế hoạch và định kỳ tổ chức diễn tập bảo đảm an toàn thông tin cho hệ thống; cử cán bộ tham gia vào các cuộc diễn tập quốc gia hoặc quốc tế do cơ quan chức năng triệu tập;

- Có kế hoạch khôi phục hoạt động bình thường của hệ thống trong trường hợp xảy ra sự cố hoặc thảm họa;

đ) Kiểm tra, đánh giá và quản lý rủi ro:

- Định kỳ hàng năm thực hiện kiểm tra, đánh giá an toàn thông tin và quản lý rủi ro an toàn thông tin theo quy định của pháp luật;

- Việc kiểm tra, đánh giá an toàn thông tin và đánh giá rủi ro phải do tổ chức chuyên môn được cơ quan có thẩm quyền cấp phép hoặc tổ chức sự nghiệp nhà nước có chức năng, nhiệm vụ phù hợp do chủ quản hệ thống thông tin chỉ định thực hiện theo quy định của pháp luật.

PHỤ LỤC 4

YÊU CẦU CƠ BẢN BẢO ĐẢM AN TOÀN HỆ THỐNG THÔNG TIN ĐỐI VỚI HỆ THỐNG THÔNG TIN CẤP ĐỘ 4

(Ban hành kèm theo Thông tư số 03/2017/TT-BTTTT ngày 24 tháng 4 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông)

1. Yêu cầu về kỹ thuật:

a) An toàn hạ tầng mạng:

- Có phương án phát hiện phòng chống xâm nhập giữa các vùng mạng quan trọng;

- Có phương án quản lý mạng không dây (nếu có) tập trung;

- Có hệ thống quản lý phòng chống mã độc tập trung. Trong đó, hệ thống có chức năng cơ bản bao gồm: cập nhật dữ liệu, gửi cảnh báo, nhận thông tin điều khiển từ hệ thống quản lý tập trung tới các phần mềm được cài đặt trên máy chủ/ máy trạm trong mạng;

- Có phương án dự phòng nóng cho các thiết bị mạng chính bảo đảm khả năng vận hành liên tục của hệ thống; năng lực của thiết bị dự phòng phải đáp ứng theo quy mô hoạt động của hệ thống;

- Có phương án sử dụng thêm các phương pháp xác thực đa nhân tố đối với các thiết bị mạng quan trọng;

- Có phương án lưu trữ nhật ký độc lập và phù hợp với hoạt động của các thiết bị mạng. Dữ liệu nhật ký phải được lưu tối thiểu 06 tháng;

- Có phương án cảnh báo thời gian thực trực tiếp đến người quản trị hệ thống thông qua hệ thống giám sát khi phát hiện sự cố trên các thiết bị mạng;

- Có phương án duy trì ít nhất 02 kết nối mạng Internet từ các ISP sử dụng hạ tầng kết nối trong nước khác nhau (nếu hệ thống buộc phải có kết nối mạng Internet);

- Có phương án chống thất thoát dữ liệu trong hệ thống;

b) An toàn máy chủ:

- Có phương án sử dụng cơ chế xác thực đa nhân tố khi truy cập vào các máy chủ trong hệ thống;

- Có phương án lưu trữ nhật ký độc lập và phù hợp với hoạt động của máy chủ. Dữ liệu nhật ký phải được lưu tối thiểu 06 tháng;

- Có phương án kiểm tra tính toàn vẹn của các tệp tin hệ thống và tính toàn vẹn của các quyền đã được cấp trên các tài khoản hệ thống;

c) An toàn ứng dụng:

- Có phương án sử dụng cơ chế xác thực đa nhân tố khi truy cập vào các tài khoản quản trị của ứng dụng; có cơ chế yêu cầu người sử dụng thay đổi thông tin xác thực định kỳ;

- Có phương án lưu trữ nhật ký độc lập và phù hợp với hoạt động của ứng dụng. Dữ liệu nhật ký phải được lưu tối thiểu 06 tháng;

- Có cơ chế mã hóa thông tin xác thực của người sử dụng trước khi gửi đến ứng dụng qua môi trường mạng;

- Có cơ chế xác thực thông tin, nguồn gửi khi trao đổi thông tin trong quá trình quản trị ứng dụng (không phải là thông tin, dữ liệu công khai) qua môi trường mạng;

d) An toàn dữ liệu:

- Có phương án kiểm tra tính toàn vẹn của dữ liệu và phát hiện, cảnh báo khi dữ liệu có sự thay đổi;

- Có phương án phân loại và quản lý các dữ liệu được lưu trữ theo từng loại/nhóm thông qua việc gán các nhãn khác nhau;

- Có phương án sử dụng hệ thống sao lưu dự phòng có khả năng chịu lỗi, bảo đảm dữ liệu có khả năng phục khôi phục khi xảy ra sự cố;

2. Yêu cầu quản lý:

a) Chính sách chung: Định kỳ 01 năm hoặc đột xuất khi cần thiết thực hiện rà soát, cập nhật chính sách chung về an toàn thông tin;

b) Tổ chức, nhân sự:

- Có chính sách thẩm tra, xác minh lý lịch của cán bộ quản lý và cán bộ kỹ thuật vận hành, chịu trách nhiệm về an toàn thông tin cho hệ thống, bảo đảm sự phù hợp về mặt chuyên môn nghiệp vụ, đạo đức nghề nghiệp và phù hợp với yêu cầu, tính chất đặc thù của công việc;

- Có kế hoạch và định kỳ hàng năm tổ chức đào tạo, bồi dưỡng, tuyên truyền, phổ biến nâng cao kiến thức, kỹ năng về an toàn thông tin cho cán bộ quản lý và cán bộ kỹ thuật có liên quan;

- Có chính sách xây dựng đội ngũ chuyên trách về an toàn thông tin và phân công lãnh đạo đơn vị trực tiếp phụ trách an toàn thông tin;

c) Thiết kế, xây dựng hệ thống:

- Có hồ sơ cấp độ được thẩm định bởi Bộ Thông tin và Truyền thông;

- Có phương án kiểm tra tính tương thích, tác động của các bản vá, cập nhật an toàn thông tin đối với hoạt động của hệ thống;

- Có phương án cấu hình tối ưu, bảo đảm an toàn thông tin cho các thiết bị mạng, máy chủ trước khi đưa vào hoạt động trong hệ thống;

- Có phương án thực hiện kiểm tra, đánh giá tổng thể về an toàn thông tin của hệ thống trước khi đưa vào vận hành, khai thác;

d) Quản lý vận hành:

- Có phương án giám sát an toàn thông tin riêng cho hệ thống theo quy định của pháp luật; tổ chức trực giám sát 24/7;

- Có kế hoạch và định kỳ hàng năm tổ chức diễn tập bảo đảm an toàn thông tin cho hệ thống;

- Có phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng theo quy định của pháp luật;

đ) Kiểm tra, đánh giá và quản lý rủi ro:

- Định kỳ hàng năm thực hiện kiểm tra, đánh giá an toàn thông tin và quản lý rủi ro an toàn thông tin;

- Việc kiểm tra, đánh giá an toàn thông tin và quản lý rủi ro phải do tổ chức chuyên môn được cơ quan có thẩm quyền cấp phép hoặc tổ chức sự nghiệp nhà nước có chức năng, nhiệm vụ phù hợp do chủ quản hệ thống thông tin chỉ định thực hiện theo quy định của pháp luật.

PHỤ LỤC 5

YÊU CẦU CƠ BẢN BẢO ĐẢM AN TOÀN HỆ THỐNG THÔNG TIN ĐỐI VỚI HỆ THỐNG THÔNG TIN CẤP ĐỘ 5

(Ban hành kèm theo Thông tư số 03/2017/TT-BTTTT ngày 24 tháng 4 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông)

1. Yêu cầu kỹ thuật:

a) An toàn hạ tầng mạng:

- Có hệ thống tường lửa, hệ thống phát hiện và phòng chống xâm nhập giữa các vùng mạng của hệ thống;

- Có phương án lưu dữ liệu nhật ký của các thiết bị mạng tối thiểu 12 tháng;

- Có phương án dự phòng cho tất cả các thiết bị mạng bảo đảm hoạt động của hệ thống không bị gián đoạn;

b) An toàn máy chủ:

- Có phương án sử dụng giải pháp phòng chống xâm nhập mức máy trạm đối với các máy chủ;

- Có phương án lưu trữ nhật ký độc lập và phù hợp với hoạt động của máy chủ. Nhật ký của hệ thống phải được lưu tối thiểu 12 tháng;

c) An toàn ứng dụng:

- Có phương án áp dụng cơ chế xác thực hai chiều khi trao đổi dữ liệu quan trọng qua môi trường mạng;

- Có phương án sử dụng thiết bị lưu trữ chuyên dụng để lưu trữ thông tin xác thực;

- Có phương án lưu nhật ký của ứng dụng lưu tối thiểu 12 tháng;

d) An toàn dữ liệu:

- Có phương án sử dụng kênh riêng khi truyền đưa, trao đổi dữ liệu qua môi trường mạng;

- Có phương án lưu trữ dự phòng các dữ liệu trên hệ thống ở các vị trí địa lý khác nhau;

- Có phương án duy trì ít nhất 02 kết nối mạng từ hệ thống sao lưu dự phòng chính với hệ thống sao lưu dự phòng phụ.

2. Yêu cầu quản lý:

a) Chính sách chung:

Định kỳ 06 tháng hoặc đột xuất khi cần thiết thực hiện rà soát, cập nhật chính sách chung về an toàn thông tin;

b) Chính sách tổ chức, nhân sự:

- Các vị trí công việc khác nhau phải bố trí cán bộ chuyên trách khác nhau, không được sử dụng cán bộ kiêm nhiệm;

- Các vị trí vận hành khai thác quan trọng cần bố trí ít nhất 02 cán bộ cùng tham gia thực hiện;

c) Thiết kế, xây dựng hệ thống:

Sản phẩm, thiết bị được đầu tư trong hệ thống phải được kiểm định an toàn thông tin trước khi đưa vào vận hành khai thác;

d) Quản lý vận hành:

Có kế hoạch và định kỳ 06 tháng tổ chức diễn tập bảo đảm an toàn thông tin cho hệ thống;

đ) Kiểm tra, đánh giá và quản lý rủi ro:

- Định kỳ 06 tháng hoặc theo yêu cầu thực tế hoặc theo yêu cầu, cảnh báo của cơ quan chức năng thực hiện kiểm tra, đánh giá an toàn thông tin và quản lý rủi ro an toàn thông tin;

- Việc kiểm tra, đánh giá an toàn thông tin và đánh giá rủi ro an toàn thông tin phải do tổ chức chuyên môn được cơ quan có thẩm quyền cấp phép hoặc tổ chức sự nghiệp nhà nước có chức năng, nhiệm vụ phù hợp do chủ quản hệ thống thông tin chỉ định thực hiện theo quy định của pháp luật.