BỘ THÔNG TIN VÀ TRUYỀN THÔNG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
	Độc lập - Tự do - Hạnh phúc
Số: 2291/BTTTT-CATTT	
V/v đôn đốc, hướng dẫn thực hiện công tác xác định cấp độ và xây dựng Hồ sơ đề xuất cấp độ an toàn hệ thống thông tin	*Hà Nội, ngày 17 tháng 7 năm 2018*

Kính gửi:

- Các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ;
- UBND các tỉnh, thành phố trực thuộc Trung ương.

Thực hiện Nghị quyết số 131/NQ-CP ngày 06/12/2017 Phiên họp thường kỳ Chính phủ tháng 11 năm 2017 giao "Các bộ, cơ quan ngang bộ khẩn trương triển khai thực hiện các các nhiệm vụ quy định tại Nghị định 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn thông tin theo cấp độ".

Để tăng cường công tác bảo đảm an toàn thông tin mạng trong tình hình mới, Bộ Thông tin và Truyền thông (TT&TT) yêu cầu các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ; UBND các tỉnh, thành phố trực thuộc Trung ương thực hiện:

1) Xác định cấp độ an toàn hệ thống thông tin của các hệ thống thông tin thuộc phạm vi quản lý.

2) Xây dựng Hồ sơ đề xuất cấp độ và thực hiện quy trình thủ tục thẩm định và phê duyệt theo quy định. Trong đó, phương án bảo đảm an toàn thông tin được thuyết minh trong Hồ sơ đề xuất phải đáp ứng các yêu cầu an toàn theo tiêu chuẩn quốc gia TCVN 11930:2017 về yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ trình cấp có thẩm quyền phê duyệt theo quy định tại 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.

Trường hợp hệ thống thông tin được đề xuất là cấp độ 4 hoặc cấp độ 5, đề nghị Quý cơ quan, tổ chức gửi Hồ sơ đề xuất cấp độ về Bộ Thông tin và Truyền thông để thẩm định theo quy định của pháp luật..

3) Tổ chức triển khai phương án bảo đảm an toàn thông tin theo phương án thuyết minh trong Hồ sơ đề xuất cấp độ sau khi được phê duyệt.

Bộ TT&TT gửi kèm theo tài liệu hướng dẫn xác định cấp độ và xây dựng Hồ sơ đề xuất cấp độ. Trong quá trình thực hiện, nếu gặp khó khăn, vướng mắc, cơ quan, tổ chức có thể gửi văn bản đề nghị Bộ TT&TT/Cục ATTT hướng dẫn, hỗ trợ.

Trân trọng./.

Nơi nhận:
- Như trên;
- Bộ trưởng (để b/c);
- Thứ trưởng Nguyễn Thành Hưng;
- Lưu: VT, CATTT.

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

Nguyễn Thành Hưng

TÀI LIỆU HƯỚNG DẪN CƠ BẢN XÂY DỰNG HỒ SƠ ĐỀ XUẤT CẤP ĐỘ

Hồ sơ đề xuất cấp độ bao gồm hai loại tài liệu bản cứng: Tài liệu thuyết minh Hồ sơ đề xuất cấp độ và Tài liệu thiết kế hệ thống.

Trong đó, tài liệu thuyết minh Hồ sơ đề xuất cấp độ bao gồm các nội dung sau: (1) Thuyết minh tổng quan về hệ thống thông tin; (2) Thuyết minh đề xuất cấp độ an toàn hệ thống thông tin; (3) Thuyết minh phương án bảo đảm an toàn thông tin.

Khi xây dựng Hồ sơ đề xuất cấp độ cần chú ý, đối với một hệ thống thông tin lớn có nhiều hệ thống thành phần. Trong đó, các hệ thống thành phần được quản lý, chia sẻ trên một hạ tầng dùng chung, có cùng đơn vị vận hành và có thể triển khai phương án bảo đảm an toàn thông tin chung cho toàn bộ hạ tầng đó, thì có thể xây dựng một Hồ sơ cấp độ chung cho các hệ thống thông tin thành phần. Chỉ xây dựng Hồ sơ cấp độ cho từng hệ thống riêng biệt trong trường hợp độc lập về hạ tầng, cơ chế quản lý và đơn vị vận hành.

Xây dựng Hồ sơ đề xuất cấp độ theo hướng dẫn sau:

I. Thuyết minh tổng quan về hệ thống thông tin

1. Thông tin Chủ quản hệ thống thông tin

Hướng dẫn: Cung cấp thông tin về Chủ quản hệ thống thông tin, bao gồm: Tên Tổ chức, Người đại diện, Số Quyết định thành lập/Quy định chức năng, nhiệm vụ và quyền hạn, Người đại diện, Địa chỉ,Thông tin liên hệ.

2. Thông tin Đơn vị vận hành

Hướng dẫn: Cung cấp thông tin về đơn vị vận hành hệ thống thông tin bao gồm các thông tin như đối với Chủ quản hệ thống thông tin. Trường hợp hệ thống thông tin lớn có nhiều đơn vị vận hành khác nhau thì cung cấp đầy đủ thông tin của các đơn vị vận hành.

3. Mô tả phạm vi, quy mô của hệ thống

Hướng dẫn: Mô tả thành phần các ứng dụng, dịch vụ và đối tượng cung cấp dịch vụ của Hệ thống. Chú ý là một hệ thống thông tin có thể bao gồm các hệ thống thông tin thành phần trong đó và mỗi thành phần đó cung cấp một ứng dụng/dịch vụ khác nhau.

4. Mô tả cấu trúc của hệ thống

Hướng dẫn: Mô tả cấu trúc hiện tại của Hệ thống, bao gồm các thông tin sau:

a) Cấu trúc vật lý mô tả các thiết bị mạng, các thiết bị đầu cuối có trong hệ thống và các kết nối vật lý giữa các thiết bị.

b) Cấu trúc logic mô tả thiết kế các vùng mạng chức năng có trong hệ thống; Hướng hết nối mạng; Các thiết bị đầu cuối; Các thiết bị mạng. Trường hợp các các thiết bị vật lý được cài đặt các thành phần ảo hóa hoặc logic, hoạt động như một thiết bị độc lập thì sơ đồ logic sẽ thể hiện thành phần ảo hóa hoặc logic thay cho thiết bị vật lý.

Trường hợp các hệ thống thông tin có cấu trúc đặt thù theo chức năng và không có những vùng mạng được đưa ra như trong Thông tư số 03/2017/TT-BTTTT của Bộ TT&TT về quy định chi tiết và hướng dẫn một số điều của Nghị định 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ (Thông tư 03) thì việc mô tả cấu trúc của hệ thống thông tin đó được mô tả theo cấu trúc thực tế của hệ thống.

c) Cung cấp danh mục thiết bị sử dụng trong hệ thống:Cung cấp thông tin về các thiết bị mạng và các thiết bị đầu cuối có trong hệ thống. Bao gồm các thông tin Tên thiết bị/Chủng loại; Vị trí triển khai, trường hợp thiết bị vật lý được chia thành các thiết bị logic thì vị trí triển khai là các vị trí của thiết bị logic.

d) Danh mục các ứng dụng/dịch vụ cung cấp bởi hệ thống (bao gồm các ứng dụng nghiệp vụ như quản lý văn bản, thư điện tử... và các dịch vụ hệ thống như DNS, DHCP, NTP....) : Cung cấp thông tin các ứng dụng/dịch vụ có trên hệ thống bao gồm Tên dịch vụ; Máy chủ triển khai/Vị trí triển khai/Hệ điều hành máy chủ; Mục đích sử dụng dịch vụ.

II. Thuyết minh đề xuất cấp độ an toàn hệ thống thông tin

1. Danh mục hệ thống thông tin và cấp độ đề xuất tương ứng

Hướng dẫn: Việc xác định cấp độ của hệ thống thông tin căn cứ vào loại thông tin hệ thống đó xử lý và loại hình hệ thống thông tin đó.

Khi xác định cấp độ, ta không cần thiết phải liệt kê ra hết các tiêu chí, mà chỉ đưa ra duy nhất một tiêu chí và tiêu chí đó đủ để xác định cấp độ cao nhất.

Trường hợp một hệ thống thông tin lớn, bao gồm nhiều thành phần khác nhau, thì cần xác định loại thông tin và loại hình của từng thành phần tương ứng.

Thành phần nào có tiêu chí để đề xuất cấp độ cao nhất sẽ quyết định cấp độ an toàn thông tin của hệ thống đó. Do đó, khi xác định cấp độ của Hệ thống thông tin cần xác định thành phần nào trong hệ thống thông tin tổng thể khớp với tiêu chí xác định cấp độ ở cấp cao nhất.

Thành phần của hệ thống thông tin có thể phân chia bằng nhiều hình thức khác nhau, miễn là ta có thể phân biệt được thành phần đó với các thành phần khác trong hệ thống theo cách phân chia được thực hiện.

Thành phần của hệ thống có thể phân theo các ứng dụng/dịch vụ cụ thể (Thư điện tử, Cổng thông tin điện tử...) hoặc phân theo vùng mạng (Vùng DMZ, Vùng máy chủ nội bộ,...) hay chức năng (Hệ thống chăm sóc khác hàng, hệ thống truyền hình trực tuyến...) của thành phần đó.

Chú ý: việc phân chia hệ thống thông tin thành các thành phần cần phải đảm bảo số lượng các thành phần là nhỏ, đơn giản nhất và đủ để áp dụng các tiêu chí để xác định cấp độ cho hệ thống thông tin đó.

2. Thuyết minh chi tiết đối với hệ thống thông tin

Hướng dẫn: Nội dung này chỉ yêu cầu đối với hệ thống được đề xuất là cấp độ 4 hoặc cấp độ 5, theo khoản 4, Điều 7 Thông tư 03. Bao gồm các nội dung:

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 và mức độ quan trọng;

c) Thuyết minh về các nguy cơ tấn công mạng, mất an toàn thông tin đối với hệ thống và các ảnh hưởng;

d) 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;

đ) Thuyết minh yêu cầu cần phải vận hành 24/7 và không chấp nhận ngừng vận hành mà không có kế hoạch trước.

III. Thuyết minh phương án bảo đảm an toàn thông tin

Đối với các hệ thống thông tin/hệ thống thành phần độc lập về hạ tầng, đơn vị vận hành và chính sách quản lý thì xây dựng phương án bảo đảm an toàn thông tin riêng cho từng hệ thống đó.

Phương án bảo đảm an toàn thông tin đối với hệ thống thông tin mới cần chỉ ra phương án triển khai cụ thể khi xây dựng và thiết lập hệ thống. Ví dụ để đáp ứng yêu cầu an toàn thông tin nào thì sử dụng giải pháp gì, phương án triển khai thế nào.

Phương án bảo đảm an toàn thông tin đối với hệ thống đã đưa vào quản lý vận hành, cần chỉ rõ các yêu cầu nào đã đáp ứng và mô tả ngắn gọn giải pháp và phương án đã triển khai. Đối với các yêu cầu chưa đáp ứng, cần mô tả phương án dự kiến sẽ sử dụng là gì, kế hoạch và lộ trình triển khai để đáp ứng yêu cầu an toàn.

Để thuyết minh chi tiết việc đáp ứng các yêu cầu an toàn quy định tại Thông tư số 03, có thể tham khảo các yêu cầu an toàn cụ thể tại Tiêu chuẩn quốc gia TCVN 11930:2017 về yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ.

I. Thuyết minh phương án bảo đảm an toàn thông tin

a) Yêu cầu Quản lý

Thuyết minh phương án đáp ứng yêu cầu quản lý theo cấu trúc sau:

1. Mục tiêu, nguyên tắc bảo đảm an toàn thông tin

2. Trách nhiệm của đơn vị chuyên trách về an toàn thông tin, các cán bộ làm về an toàn thông tin và các đối tượng thuộc phạm vi điều chỉnh của chính sách an toàn thông tin.

3. Phạm vi chính sách an toàn thông tin

4. Tổ chức bảo đảm an toàn thông tin

5. Bảo đảm nguồn nhân lực

6. Quản lý thiết kế, xây dựng hệ thống

7. Quản lý vận hành hệ thống

- Quản lý an toàn mạng

- Quản lý an toàn máy chủ và ứng dụng

- Quản lý an toàn dữ liệu

- Quản lý an toàn thiết bị đầu cuối

- Quản lý phòng chống phần mềm độc hại

- Quản lý giám sát an toàn hệ thống thông tin

- Quản lý điểm yếu an toàn thông tin

- Quản lý sự cố an toàn thông tin

- Quản lý an toàn người sử dụng đầu cuối.

b) Yêu cầu kỹ thuật

Tùy thuộc vào đặc trưng của từng hệ thống cụ thể, việc thuyết minh phương án bảo đảm an toàn thông tin có thể thuyết minh cho phù hợp với đặc thù của hệ thống đó.

Ví dụ, trường hợp có hệ thống thông tin có tính chất đặc thù như hệ thống điều khiển công nghiệp, không có kết nối Internet, thì không phải thuyết minh phương án phòng chống DDoS hay thiết kế vùng mạng DMZ...

Chú ý: Một yêu cầu kỹ thuật có thể thực hiện bằng nhiều phương án khác nhau. Đối với các hệ thống thông tin cấp độ 1,2 hoặc cấp độ 3 để giảm thiểu chi phí đầu tư thì để đáp ứng các yêu cầu kỹ thuật không nhất thiết phải đầu tư các thiết bị chuyên dụng mà có thể sử dụng chia sẻ hoặc đưa ra phương án tương đương khác.

Ví dụ, yêu cầu về phương án xử lý tấn công DDoS thì có thể thuê dịch vụ hoặc xây dựng phương án xử lý riêng của mình, dựa trên năng lực hệ thống hiện có, thay vì đầu tư thiết bị xử lý tấn công DDoS chuyên dụng.

Thuyết minh phương án đáp ứng yêu cầu kỹ thuật theo cấu trúc sau:

1. Bảo đảm an toàn mạng

1.1.Thiết kế hệ thống

1.2. Kiểm soát truy cập từ bên ngoài mạng

1.3. Kiểm soát truy cập từ bên trong mạng

1.4. Nhật ký hệ thống

1.5. Phòng chống xâm nhập

1.6. Phòng chống phần mềm độc hại trên môi trường mạng

1.7. Bảo vệ thiết bị hệ thống

2. Bảo đảm an toàn máy chủ

2.1. Xác thực

2.2. Kiểm soát truy cập

2.3. Nhật ký hệ thống

2.4. Phòng chống xâm nhập

2.5. Phòng chống phần mềm độc hại

2.6. Xử lý máy chủ khi chuyển giao

3. Bảo đảm an toàn ứng dụng

3.1. Xác thực

3.2. Kiểm soát truy cập

3.3. Nhật ký hệ thống

3.4. Bảo mật thông tin liên lạc

3.5. Chống chối bỏ

4. Bảo đảm an toàn dữ liệu

4.1. Nguyên vẹn dữ liệu

4.2. Bảo mật dữ liệu

4.3. Sao lưu dự phòng