Phụ lục 02

PHƯƠNG ÁN PHÒNG NGỪA SỰ CỐ TẤN CÔNG MẠNG

(Kèm theo công văn số 193/CATTT-VNCERTCC ngày 25/6/2021 của Cục An toàn thông tin)

1. Triển khai mô hình 04 lớp về đảm bảo an toàn thông

1.1. Lớp 1: Lực lượng tại chỗ

a) Người đứng đầu cơ quan báo chí trực tiếp quan tâm, chỉ đạo công tác an toàn, an ninh mạng hoặc có thể phân công một Lãnh đạo cấp phó giúp theo dõi, điều hành;

b) Thành lập Bộ phận (Đội) ứng cứu sự cố tại chỗ gồm cán bộ kỹ thuật đủ năng lực, đại diện của đơn vị vận hành hệ thống, đại diện đơn vị cung cấp dịch vụ đảm bảo an toàn thông tin mạng (nếu có). Bộ phận ứng cứu sự cố phải am hiểu hạ tầng kỹ thuật của hệ thống, tối thiểu có đủ năng lực ứng cứu, xử lý sự cố an toàn thông tin cơ bản;

c) Đăng ký tham gia Mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia theo quy định tại Điều 5, Thông tư 20/2017/TT-BTTTT quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc.

1.2. Lớp 2: Lực lượng giám sát, bảo vệ chuyên nghiệp

Bên cạnh bộ phận ứng cứu sự cố tại chỗ, trong trường hợp chưa đủ năng lực để tự giám sát, bảo vệ, cơ quan báo chí cần phối hợp, lựa chọn các lực lượng chuyên nghiệp để giám sát, bảo vệ hệ thống thông tin.

Lực lượng chuyên nghiệp có thể là doanh nghiệp đã được Bộ Thông tin và Truyền thông cấp phép hoặc đơn vị chuyên trách của Bộ Quốc phòng (Bộ Tư lệnh 86, Ban Cơ yếu Chính phủ), Bộ Công an (Cục An ninh mạng và phòng chống tội phạm công nghệ cao), Bộ Thông tin và Truyền thông (Cục An toàn thông tin).

1.3. Lớp 3: Lực lượng độc lập kiểm tra, đánh giá định kỳ

Lựa chọn tổ chức, doanh nghiệp thực hiện kiểm tra, đánh giá định kỳ, lực lượng này độc lập với lực lượng giám sát, bảo vệ.

Định kỳ tối thiểu 1 năm một lần thực hiện kiểm tra, đánh giá, rà quét, phát hiện lỗ hổng, điểm yếu, kiểm thử xâm nhập hệ thống để từ đó có biện pháp phòng ngừa, khắc phục phù hợp.

1.4. Lớp 4: Kết nối, chia sẻ thông tin với hệ thống giám sát quốc gia

Thực hiện kết nối, chia sẻ thông tin kỹ thuật với hệ thống giám sát quốc gia của Cục An toàn thông tin, Bộ Thông tin và Truyền thông để được theo dõi, cảnh báo kịp thời các kết nối bất thường, độc hại. Để kết nối, chia sẻ đề nghị liên hệ với Cục An toàn thông tin qua số điện thoại 02432091616 và email ais@mic.gov.vn.

2. Xây dựng phương án ứng cứu khẩn cấp sự cố tấn công mạng bao gồm tối thiểu các nội dung sau:

2.1. Xác định các hệ thống thông tin cần bảo vệ, hệ thống thông tin càng quan trọng thì công tác giám sát, mức độ sẵn sàng ứng cứu, hệ thống bảo vệ và nguồn lực đảm bảo an toàn thông tin càng phải cao.

2.2. Quy định trách nhiệm và quy trình phối hợp giữa các lực lượng tham gia ứng cứu sự cố gồm: chủ quản hệ thống thông tin; đơn vị vận hành hệ thống thông tin; đơn vị cung cấp dịch vụ, giải pháp an toàn thông tin mạng (nếu có); bộ phận an toàn thông tin/bộ phận ứng cứu sự cố; các đơn vị liên quan khác (nếu có).

2.3. Đánh giá các nguy cơ, sự cố mất an toàn thông tin mạng đối với các hệ thống gồm:

- Các nguy cơ, sự cố có thể xảy ra với các hệ thống thông tin.
- Đánh giá, dự báo các thiệt hại, tác động có thể nếu xảy ra sự cố.
- Khả năng đáp ứng về năng lực ứng cứu sự cố bao gồm công cụ hỗ trợ, và đội ngũ nhân lực.

2.4. Xây dựng sẵn kịch bản, quy trình ứng cứu sự cố cho một số sự cố tấn công mạng tiêu biểu, tối thiểu bao gồm các loại sự cố sau: Tấn công từ chối dịch vụ (DDoS); Tấn công giả mạo; Tấn công sử dụng mã độc; Tấn công truy cập trái phép, chiếm quyền điều khiển; Tấn công thay đổi giao diện; Tấn công mã hóa phần mềm, dữ liệu, thiết bị; Tấn công nghe trộm, gián điệp, lấy cắp thông tin, dữ liệu; Tấn công tổng hợp sử dụng kết hợp nhiều hình thức.

2.5. Các kịch bản, quy trình ứng cứu sự cố phải thể hiện rõ vai trò các lực lượng, các bước cụ thể, công việc cần làm, thời gian thực hiện, kết quả cần thiết.

2.6. Thường xuyên tổ chức huấn luyện, diễn tập ứng cứu sự cố đối với các hệ thống thông tin, ưu tiên đối với các hệ thống hiện diện trên Internet.

Chi tiết tham khảo Phụ lục III đề cương kế hoạch ứng phó sự cố an toàn thông tin mạng tại thông tư 20/2017/TT-BTTTT