1. PHÒNG, CHỐNG HÀNH VI SỬ DỤNG KHÔNG GIAN MẠNG, CÔNG NGHỆ THÔNG TIN, PHƯƠNG TIỆN ĐIỆN TỬ ĐỂ VI PHẠM PHÁP LUẬT VỀ AN NINH QUỐC GIA, TRẬT TỰ, AN TOÀN XÃ HỘI

a) Hành vi sử dụng không gian mạng, công nghệ thông tin, phương tiện điện tử để vi phạm pháp luật về an ninh quốc gia, trật tự, an toàn xã hội bao gồm:

- Đăng tải, phát tán thông tin trên không gian mạng có nội dung quy định tại các khoản 1, 2, 3, 4 và 5 Điều 16 Luật an ninh mạng (gồm các nội dung tuyên truyền chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam; kích động gây bạo loạn, phá rối an ninh, gây rối trật tự công cộng; làm nhục, vu khống; xâm phạm trật tự quản lý kinh tế) và hành vi quy định tại khoản 1 Điều 17 Luật an ninh mạng (gồm các hành vi gián điệp mạng; xâm phạm bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên không gian mạng).

- Chiếm đoạt tài sản; tổ chức đánh bạc, đánh bạc qua mạng Internet; trộm cắp cước viễn thông quốc tế trên nền Internet; vi phạm bản quyền và sở hữu trí tuệ trên không gian mạng;

- Giả mạo trang thông tin điện tử của cơ quan, tổ chức, cá nhân; làm giả, lưu hành, trộm cắp, mua bán, thu thập, trao đổi trái phép thông tin thẻ tín dụng, tài khoản ngân hàng của người khác; phát hành, cung cấp, sử dụng trái phép các phương tiện thanh toán;

- Tuyên truyền, quảng cáo, mua bán hàng hóa, dịch vụ thuộc danh mục cấm theo quy định của pháp luật;

- Hướng dẫn người khác thực hiện hành vi vi phạm pháp luật;

- Hành vi khác sử dụng không gian mạng, công nghệ thông tin, phương tiện điện tử để vi phạm pháp luật về an ninh quốc gia, trật tự, an toàn xã hội.

b) Lực lượng chuyên trách bảo vệ an ninh mạng có trách nhiệm phòng, chống hành vi sử dụng không gian mạng, công nghệ thông tin, phương tiện điện tử để vi phạm pháp luật về an ninh quốc gia, trật tự, an toàn xã hội.

(Điều 18 Luật an ninh mạng)

2. PHÒNG, CHỐNG TẤN CÔNG MẠNG

a) Hành vi tấn công mạng và hành vi có liên quan đến tấn công mạng bao gồm:

- Phát tán chương trình tin học gây hại cho mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử;

- Gây cản trở, rối loạn, làm tê liệt, gián đoạn, ngưng trệ hoạt động, ngăn chặn trái phép việc truyền đưa dữ liệu của mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, phương tiện điện tử;

- Xâm nhập, làm tổn hại, chiếm đoạt dữ liệu được lưu trữ, truyền đưa qua mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử;

- Xâm nhập, tạo ra hoặc khai thác điểm yếu, lỗ hổng bảo mật và dịch vụ hệ thống để chiếm đoạt thông tin, thu lợi bất chính;

- Sản xuất, mua bán, trao đổi, tặng cho công cụ, thiết bị, phần mềm có tính năng tấn công mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử để sử dụng vào mục đích trái pháp luật;

- Hành vi khác gây ảnh hưởng đến hoạt động bình thường của mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử.

b) Chủ quản hệ thống thông tin có trách nhiệm áp dụng biện pháp kỹ thuật để phòng ngừa, ngăn chặn hành vi quy định ở trên đối với hệ thống thông tin thuộc phạm vi quản lý, trừ hành vi sản xuất, mua bán, trao đổi, tặng cho công cụ, thiết bị, phần mềm có tính năng tấn công mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử để sử dụng vào mục đích trái pháp luật.

c) Khi xảy ra tấn công mạng xâm phạm hoặc đe dọa xâm phạm chủ quyền, lợi ích, an ninh quốc gia, gây tổn hại nghiêm trọng trật tự, an toàn xã hội, lực lượng chuyên trách bảo vệ an ninh mạng chủ trì, phối hợp với chủ quản hệ thống thông tin và tổ chức, cá nhân có liên quan áp dụng biện pháp xác định nguồn gốc tấn công mạng, thu thập chứng cứ; yêu cầu doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng chặn lọc thông tin để ngăn chặn, loại trừ hành vi tấn công mạng và cung cấp đầy đủ, kịp thời thông tin, tài liệu liên quan.

(Điều 19 Luật an ninh mạng)

3. PHÒNG NGỪA, XỬ LÝ TÌNH HUỐNG NGUY HIỂM VỀ AN NINH MẠNG

a) Tình huống nguy hiểm về an ninh mạng gồm:

- Xuất hiện thông tin kích động trên không gian mạng có nguy cơ xảy ra bạo loạn, phá rối an ninh, khủng bố;

- Tấn công vào hệ thống thông tin quan trọng về an ninh quốc gia;

- Tấn công nhiều hệ thống thông tin trên quy mô lớn, cường độ cao;

- Tấn công mạng nhằm phá hủy công trình quan trọng về an ninh quốc gia, mục tiêu quan trọng về an ninh quốc gia;

- Tấn công mạng xâm phạm nghiêm trọng chủ quyền, lợi ích, an ninh quốc gia; gây tổn hại đặc biệt nghiêm trọng trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

b) Trách nhiệm phòng ngừa tình huống nguy hiểm về an ninh mạng như sau:

- Lực lượng chuyên trách bảo vệ an ninh mạng phối hợp với chủ quản hệ thống thông tin quan trọng về an ninh quốc gia triển khai các giải pháp kỹ thuật, nghiệp vụ để phòng ngừa, phát hiện, xử lý tình huống nguy hiểm về an ninh mạng;

- Doanh nghiệp viễn thông, Internet, công nghệ thông tin, doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng và cơ quan, tổ chức, cá nhân có liên quan có trách nhiệm phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an trong phòng ngừa, phát hiện, xử lý tình huống nguy hiểm về an ninh mạng.

c) Biện pháp xử lý tình huống nguy hiểm về an ninh mạng bao gồm:

- Triển khai ngay phương án phòng ngừa, ứng phó khẩn cấp về an ninh mạng, ngăn chặn, loại trừ hoặc giảm nhẹ thiệt hại do tình huống nguy hiểm về an ninh mạng gây ra;

- Thông báo đến cơ quan, tổ chức, cá nhân có liên quan;

- Thu thập thông tin liên quan; theo dõi, giám sát liên tục đối với tình huống nguy hiểm về an ninh mạng;

- Phân tích, đánh giá thông tin, dự báo khả năng, phạm vi ảnh hưởng và mức độ thiệt hại do tình huống nguy hiểm về an ninh mạng gây ra;

- Ngừng cung cấp thông tin mạng tại khu vực cụ thể hoặc ngắt cổng kết nối mạng quốc tế;

- Bố trí lực lượng, phương tiện ngăn chặn, loại bỏ tình huống nguy hiểm về an ninh mạng;

- Biện pháp khác theo quy định của Luật An ninh quốc gia.

d) Việc xử lý tình huống nguy hiểm về an ninh mạng được quy định như sau:

- Khi phát hiện tình huống nguy hiểm về an ninh mạng, cơ quan, tổ chức, cá nhân kịp thời thông báo cho lực lượng chuyên trách bảo vệ an ninh mạng và áp dụng ngay các biện pháp, bao gồm: Triển khai ngay phương án phòng ngừa, ứng phó khẩn cấp về an ninh mạng, ngăn chặn, loại trừ hoặc giảm nhẹ thiệt hại do tình huống nguy hiểm về an ninh mạng gây ra và Thông báo đến cơ quan, tổ chức, cá nhân có liên quan;

- Thủ tướng Chính phủ xem xét, quyết định hoặc ủy quyền cho Bộ trưởng Bộ Công an xem xét, quyết định, xử lý tình huống nguy hiểm về an ninh mạng trong phạm vi cả nước hoặc từng địa phương hoặc đối với một mục tiêu cụ thể.

Thủ tướng Chính phủ xem xét, quyết định hoặc ủy quyền cho Bộ trưởng Bộ Quốc phòng xem xét, quyết định, xử lý tình huống nguy hiểm về an ninh mạng đối với hệ thống thông tin quân sự và hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ;

- Lực lượng chuyên trách bảo vệ an ninh mạng chủ trì, phối hợp với cơ quan, tổ chức, cá nhân có liên quan áp dụng các biện pháp xử lý tình huống nguy hiểm về an ninh mạng (nêu trên) để xử lý tình huống nguy hiểm về an ninh mạng;

- Cơ quan, tổ chức, cá nhân có liên quan có trách nhiệm phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng thực hiện biện pháp nhằm ngăn chặn, xử lý tình huống nguy hiểm về an ninh mạng.

(Điều 21 Luật an ninh mạng)

BỘ TƯ PHÁP

ĐỀ ÁN "TĂNG CƯỜNG CÔNG TÁC PHỔ BIẾN, GIÁO DỤC PHÁP LUẬT TẠI MỘT SỐ ĐỊA BÀN TRỌNG ĐIỂM VỀ VI PHẠM PHÁP LUẬT" ĐẾN NĂM 2021

TÌM HIỂU PHÁP LUẬT VỀ PHÒNG NGỪA, XỬ LÝ HÀNH VI XÂM PHẠM AN NINH MẠNG

(Theo Luật an ninh mạng năm 2018)

HÀ NỘI - 2018