THỦ TƯỚNG CHÍNH PHỦ	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 14/CT-TTg	*Hà Nội, ngày 25 tháng 5 năm 2018*

CHỈ THỊ
Về việc nâng cao năng lực phòng, chống phần mềm độc hại

Thời gian vừa qua, công nghệ thông tin đã và đang được ứng dụng vào mọi mặt đời sống, phục vụ phát triển kinh tế - xã hội, góp phần bảo đảm quốc phòng, an ninh của đất nước. Trong xu hướng của cuộc cách mạng công nghiệp lần thứ tư, sẽ ngày càng có nhiều thiết bị thông minh kết nối mạng. Những thiết bị này khi bị lây nhiễm các loại phần mềm độc hại (gọi tắt là mã độc) sẽ gây mất an toàn thông tin, tiềm ẩn nguy cơ khó lường. Trong năm 2016 và năm 2017, một số cuộc tấn công mạng sử dụng mã độc làm thiệt hại nghiêm trọng cho nhiều cơ quan, tổ chức ở Việt Nam.

Các cơ quan, tổ chức ở Việt Nam đã và đang thực hiện nhiều giải pháp khác nhau trong việc xử lý mã độc. Tuy nhiên, hiệu quả đạt được chưa cao, khả năng chia sẻ thông tin thấp. Thực trạng lây nhiễm mã độc tại Việt Nam hiện nay rất đáng báo động. Đặc biệt, nhiều trường hợp tấn công mã độc mà cơ quan chức năng không phản ứng kịp thời để phát hiện, phân tích và gỡ bỏ.

Để nâng cao năng lực phòng, chống phần mềm độc hại, cải thiện mức độ tin cậy của quốc gia trong hoạt động giao dịch điện tử, thúc đẩy phát triển kinh tế - xã hội, góp phần bảo đảm quốc phòng, an ninh của đất nước, Thủ tướng Chính phủ chỉ thị:

1. Các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân các tỉnh, thành phố trực thuộc trung ương thực hiện một số giải pháp sau:

a) Khẩn trương phân loại, xác định cấp độ an toàn hệ thống thông tin và xây dựng phương án bảo đảm an toàn hệ thống thông tin theo cấp độ phù hợp với quy định của pháp luật và tiêu chuẩn, quy chuẩn kỹ thuật. Thời hạn hoàn thành xác định hệ thống thông tin cấp độ 4, cấp độ 5: Tháng 11 năm 2018.

b) Tăng cường sử dụng chữ ký số cho văn bản điện tử tại các đơn vị, tổ chức trong phạm vi bộ, ngành, địa phương mình.

c) Bảo đảm có giải pháp phòng, chống mã độc bảo vệ cho 100% máy chủ, máy trạm, thiết bị đầu cuối liên quan và có cơ chế tự động cập nhật phiên bản hoặc dấu hiệu nhận dạng mã độc mới. Thời hạn hoàn thành: Tháng 12 năm 2018.

Giải pháp phòng, chống mã độc được đầu tư mới hoặc nâng cấp cần có chức năng cho phép quản trị tập trung; có dịch vụ, giải pháp hỗ trợ kỹ thuật 24/7, có khả năng phản ứng kịp thời trong việc phát hiện, phân tích và gỡ bỏ phần mềm độc hại; có thể chia sẻ thông tin, dữ liệu thống kê tình hình lây nhiễm mã độc với hệ thống kỹ thuật của cơ quan chức năng có thẩm quyền, tuân thủ theo tiêu chuẩn, quy chuẩn kỹ thuật, hướng dẫn nghiệp vụ của Bộ Thông tin và Truyền thông và quy định của pháp luật.

d) Trong các dự án đầu tư ứng dụng công nghệ thông tin phải có cấu phần phù hợp cho giải pháp bảo đảm an toàn thông tin, giải pháp phòng, chống mã độc.

đ) Chỉ đạo các cơ quan, đơn vị trực thuộc khi mua sắm các thiết bị điện tử có kết nối Internet (như camera giám sát, router, modem DSL v.v...) cần thực hiện rà soát, kiểm tra, đánh giá về an toàn thông tin; trước khi đưa vào sử dụng cần thiết lập cấu hình an toàn thông tin phù hợp với quy định, tuyệt đối không sử dụng cấu hình mặc định.

e) Định kỳ thực hiện kiểm tra, đánh giá tổng thể về an toàn thông tin theo quy định tại Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ và hướng dẫn tại Thông tư số 03/2017/TT-BTTTT ngày 24 tháng 4 năm 2017 của Bộ Thông tin và Truyền thông; tổ chức theo dõi, thống kê chỉ số lây nhiễm mã độc trên các thiết bị đầu cuối, các hệ thống thông tin trong phạm vi bộ, ngành, địa phương mình, định kỳ hàng quý báo cáo về Bộ Thông tin và Truyền thông trước ngày 20 của tháng cuối cùng trong quý.

g) Thường xuyên tổ chức tuyên truyền, phổ biến, tập huấn nâng cao nhận thức, kỹ năng xử lý các mối nguy hại của mã độc và trách nhiệm của các đơn vị, tổ chức, cá nhân trong công tác phòng, chống mã độc trong phạm vi bộ, ngành, địa phương mình.

2. Bộ Thông tin và Truyền thông có trách nhiệm:

a) Phê duyệt các nội dung theo thẩm quyền và tổ chức triển khai thực hiện Đề án nâng cao năng lực phòng, chống phần mềm độc hại, cải thiện mức độ tin cậy quốc gia trong hoạt động giao dịch điện tử.

b) Tận dụng cơ sở hạ tầng, trang thiết bị hiện có để thiết lập hệ thống kỹ thuật chủ động theo dõi, rà quét phát hiện mã độc trên không gian mạng Việt Nam; kịp thời cảnh báo, yêu cầu xử lý, bóc gỡ. Thời hạn hoàn thành: Tháng 6 năm 2018.

c) Xây dựng, ban hành văn bản hướng dẫn kết nối, trao đổi, chia sẻ thông tin, dữ liệu về mã độc giữa hệ thống kỹ thuật của cơ quan chức năng liên quan với giải pháp phòng, chống mã độc ở các bộ, ngành, địa phương, tuân thủ theo tiêu chuẩn, quy chuẩn kỹ thuật. Thời hạn hoàn thành: Tháng 6 năm 2018.

d) Thành lập và duy trì hoạt động Nhóm chuyên gia để phối hợp phân tích, xác định, phát hiện ra các mã độc đặc biệt nguy hiểm, các mạng máy tính nhiễm mã độc lớn; tư vấn giải pháp xử lý, bóc gỡ.

đ) Tổ chức phát động và chỉ đạo các chiến dịch bóc gỡ mã độc, mạng máy tính nhiễm mã độc trên diện rộng với sự tham gia của các doanh nghiệp cung cấp dịch vụ viễn thông, Internet (ISP) và các tổ chức, doanh nghiệp hoạt động trong lĩnh vực công nghệ thông tin và an toàn thông tin.

e) Xây dựng và vận hành hệ thống phân tích mã độc trên cơ sở hệ thống máy chủ tên miền DNS quốc gia từ nguồn kinh phí được phép trích lại trong hoạt động thu phí duy trì sử dụng tên miền quốc gia ".vn" và địa chỉ Internet (IP) ở Việt Nam theo quy định của pháp luật. Sử dụng hiệu quả hệ thống này để tham gia xử lý mã độc lây nhiễm trên không gian mạng Việt Nam, phối hợp xử lý sự cố, triển khai việc giám sát về mặt kỹ thuật quá trình thực thi xử lý sự cố của các doanh nghiệp ISP, đảm bảo tài nguyên Internet Việt Nam, mạng Internet Việt Nam phát triển, an toàn, tin cậy.

g) Chỉ đạo tăng cường tuyên truyền, phổ biến, tập huấn nâng cao nhận thức về tác hại và kỹ năng, phương thức phòng, chống mã độc, lồng ghép vào các Đề án về đào tạo, tuyên truyền đã được phê duyệt.

h) Chỉ đạo các đơn vị trực thuộc phối hợp chặt chẽ với các đơn vị chức năng của Bộ Công an trong các chiến dịch bóc gỡ mã độc đối với các hệ thống thông tin chứa bí mật nhà nước, phục vụ công tác bảo đảm an ninh quốc gia.

i) Chỉ đạo, đôn đốc các doanh nghiệp cung cấp dịch vụ viễn thông, Internet (các ISP):

- Xây dựng và công bố quy trình thông báo, hướng dẫn, khuyến nghị xử lý mã độc, trong đó, xác định rõ đầu mối, quy trình, trách nhiệm xử lý khi phát hiện ra mã độc thông thường, mã độc nguy hiểm hoặc khi có yêu cầu của cơ quan chức năng. Thời hạn hoàn thành: Tháng 6 năm 2018;

- Thiết lập hệ thống kỹ thuật cho phép theo dõi tình hình lây nhiễm mã độc trên phạm vi mạng lưới của mình; có khả năng kết nối, chia sẻ thông tin, dữ liệu với hệ thống kỹ thuật của cơ quan chức năng. Thời hạn hoàn thành: Tháng 7 năm 2018;

- Thường xuyên tổ chức tuyên truyền, phổ biến nâng cao nhận thức cho cán bộ và khách hàng của mình về các mối nguy hại của mã độc và phương thức phòng, chống;

- Phối hợp với cơ quan chức năng của Bộ Thông tin và Truyền thông trong việc phân tích nhật ký phân giải tên miền (DNS) để xử lý mã độc. Chủ động rà quét, xử lý, bóc gỡ mã độc đã theo dõi, phát hiện được; chủ trì bóc gỡ, ngăn chặn mã độc có nguồn gốc từ các hệ thống của người dùng trong mạng lưới của mình có dấu hiệu tấn công tới các hệ thống khác.

k) Chỉ đạo, đôn đốc các doanh nghiệp cung cấp dịch vụ lưu trữ web (hosting), dịch vụ trung tâm dữ liệu (data center):

- Xây dựng và công bố quy trình thông báo, hướng dẫn, khuyến nghị xử lý mã độc, trong đó, xác định rõ đầu mối, quy trình, trách nhiệm xử lý khi phát hiện ra mã độc thông thường, mã độc nguy hiểm hoặc khi có yêu cầu của cơ quan chức năng. Thời hạn hoàn thành: Tháng 6 năm 2018.

- Phối hợp với ISP và chủ quản hệ thống thông tin hoặc đơn vị vận hành hệ thống thông tin để bóc gỡ mã độc ra khỏi hệ thống thông tin trong phạm vi quản lý của mình;

- Thực hiện bóc gỡ mã độc ra khỏi hệ thống thông tin trong phạm vi quản lý của mình hoặc thực hiện cách ly hệ thống bị lẫy nhiễm mã độc nếu tổ chức, cá nhân thuê dịch vụ không đủ năng lực thực hiện.

l) Chỉ đạo, đôn đốc các doanh nghiệp sản xuất phần mềm phòng, chống mã độc:

- Công bố quy trình phản ứng và cập nhật dấu hiệu nhận dạng cho các mẫu mã độc mới vào sản phẩm chống mã độc đang cung cấp trên thị trường Việt Nam;

- Phối hợp với cơ quan chức năng trong việc xây dựng và cung cấp các công cụ, giải pháp để loại bỏ mã độc trên diện rộng;

- Thiết lập các hệ thống kỹ thuật cho phép chia sẻ thông tin về tình hình lây nhiễm mã độc tuân thủ theo tiêu chuẩn, quy chuẩn kỹ thuật và hướng dẫn nghiệp vụ của Bộ Thông tin và Truyền thông với cơ quan chức năng có thẩm quyền và các ISP.

m) Hướng dẫn, điều phối, đôn đốc thực hiện Chỉ thị này. Theo dõi, tổng hợp, đánh giá chỉ số lây nhiễm phần mềm độc hại ở các bộ, ngành, địa phương, coi đây là một trong những tiêu chí đánh giá mức độ bảo đảm an toàn thông tin của các bộ, ngành, địa phương. Định kỳ hàng quý tổng hợp tình hình báo cáo Thủ tướng Chính phủ.

3. Bộ Công an chủ trì thực hiện điều tra, xác minh, đấu tranh, xử lý tội phạm phát tán hoặc thực hiện các cuộc tấn công mạng bằng mã độc.

4. Đề nghị Trung ương Đoàn Thanh niên Cộng sản Hồ Chí Minh phát động đoàn viên thanh niên, đặc biệt là đoàn viên thanh niên các cơ sở đào tạo về công nghệ thông tin, an toàn thông tin tham gia tuyên truyền, phổ biến về tác hại, hướng dẫn cách thức phòng, chống, xử lý khi bị lây nhiễm mã độc dưới các hình thức lồng ghép tuyên truyền, các đợt sinh hoạt của Đoàn, các chương trình tình nguyện vì cộng đồng.

5. Các cơ quan thông tấn báo chí Trung ương và địa phương, các cổng/trang thông tin điện tử của bộ, ngành, địa phương có trách nhiệm tăng cường các bài viết, chương trình, dành thời lượng thích hợp để tuyên truyền, phổ biến về tác hại và phương thức phòng, chống mã độc.

6. Hiệp hội An toàn thông tin Việt Nam (VNISA) có trách nhiệm:

a) Định kỳ hàng năm thực hiện chương trình khảo sát, đánh giá chỉ số lây nhiễm mã độc tại Việt Nam. Tổ chức khảo sát, đánh giá mức độ hài lòng của người sử dụng đối với các giải pháp phòng, chống mã độc; bình chọn, tôn vinh giải pháp phòng, chống mã độc tiêu biểu.

b) Tổ chức nghiên cứu, phân tích phương pháp thống kê về tình hình lây nhiễm phần mềm độc hại trong báo cáo do các doanh nghiệp trong và ngoài nước công bố; thúc đẩy việc hợp tác, chia sẻ thông tin, dữ liệu về mã độc giữa các cơ quan, tổ chức và doanh nghiệp.

c) Phát động hội viên tham gia các chiến dịch bóc gỡ mã độc, mạng máy tính nhiễm mã độc trên diện rộng. Chủ động kết hợp tuyên truyền, phổ biến, nâng cao nhận thức về tác hại và phương thức phòng, chống mã độc tại sự kiện Ngày An toàn thông tin Việt Nam và cuộc thi Sinh viên với An toàn thông tin hàng năm.

7. Các Bộ trưởng, Thủ trưởng cơ quan ngang bộ, Thủ trưởng cơ quan thuộc Chính phủ, Chủ tịch Ủy ban nhân dân tỉnh, thành phố trực thuộc trung ương, Thủ trưởng các cơ quan, đơn vị và các tổ chức, cá nhân liên quan có trách nhiệm thi hành nghiêm túc Chỉ thị này./.

Nơi nhận:
- Ban Bí thư Trung ương Đảng;
- Thủ tướng, các Phó Thủ tướng Chính phủ;
- Các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ;
- HĐND, UBND các tỉnh, thành phố trực thuộc trung ương;
- Văn phòng trung ương và các Ban của Đảng;
- Văn phòng Tổng Bí thư;
- Văn phòng Chủ tịch nước;
- Hội đồng dân tộc và các Ủy ban của Quốc hội;
- Văn phòng Quốc hội;
- Tòa án nhân dân tối cao;
- Viện kiểm sát nhân dân tối cao;
- Kiểm toán nhà nước;
- Ủy ban trung ương Mặt trận Tổ quốc Việt Nam;
- Cơ quan trung ương của các đoàn thể;
- Các Tập đoàn kinh tế và Tổng công ty nhà nước;
- VPCP: BTCN, các PCN, Trợ lý TTg, TGĐ Cổng TTĐT, các Vụ, đơn vị: KTTH, CN, NC, TTTH;
- Lưu: VT, KSTT (2).xh 320

THỦ TƯỚNG

THỦ TƯỚNG CHÍNH PHỦ

Nguyễn Xuân Phúc