THỦ TƯỚNG CHÍNH PHỦ	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 18/CT-TTg	*Hà Nội, ngày 13 tháng 10 năm 2022*

CHỈ THỊ
Về đẩy mạnh triển khai các hoạt động ứng cứu sự cố an toàn thông tin mạng Việt Nam

An toàn thông tin mạng là trụ cột quan trọng, xuyên suốt để tạo lập niềm tin số và bảo vệ sự phát triển thịnh vượng của đất nước trong kỷ nguyên số nhằm thực hiện thành công chuyển đổi số quốc gia, một trong những nhiệm vụ trọng tâm và đột phá chiến lược được đề ra tại Đại hội đại biểu toàn quốc Đảng Cộng sản Việt Nam lần thứ XIII. Ứng cứu sự cố an toàn thông tin mạng là hoạt động then chốt, có tính cấp thiết giúp các cơ quan, tổ chức giảm thiểu thiệt hại, ngay cả khi xảy ra sự cố nghiêm trọng. Tuy nhiên, hiện nay công tác ứng cứu sự cố an toàn thông tin mạng trong các cơ quan, tổ chức, doanh nghiệp tại Việt Nam chưa đáp ứng được yêu cầu ứng phó chủ động từ sớm, xử lý kịp thời, hiệu quả các cuộc tấn công mạng có quy mô ngày càng lớn, phức tạp, có thể gây hậu quả khó lường đối với sự phát triển và ổn định kinh tế - xã hội.

Để khắc phục các hạn chế, tồn tại và tăng cường hiệu lực, hiệu quả hoạt động ứng cứu sự cố an toàn thông tin mạng quốc gia, 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, tập đoàn, tổng công ty nhà nước và các tổ chức, doanh nghiệp là thành viên (hoặc có đơn vị trực thuộc là thành viên) của Mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia khẩn trương triển khai một số nội dung sau:

a) Bộ trưởng, Thủ trưởng cơ quan ngang Bộ, cơ quan thuộc Chính phủ, Chủ tịch Ủy ban nhân dân các tỉnh, thành phố trực thuộc trung ương, Chủ tịch, Tổng giám đốc tập đoàn, tổng công ty nhà nước và các tổ chức, doanh nghiệp là thành viên (hoặc có đơn vị trực thuộc là thành viên) của Mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia quán triệt tới tất cả các tổ chức, cá nhân thuộc phạm vi quản lý nguyên tắc "Ứng cứu sự cố an toàn thông tin mạng là hoạt động quan trọng nhằm phát hiện, ngăn chặn, xử lý và khắc phục kịp thời sự cố an toàn thông tin mạng"; chỉ đạo triển khai nghiêm túc các nội dung của Chỉ thị này và chịu trách nhiệm trước Thủ tướng Chính phủ nếu lơ là trong công tác ứng cứu sự cố an toàn thông tin mạng, để xảy ra hậu quả, thiệt hại nghiêm trọng tại cơ quan, đơn vị thuộc phạm vi quản lý.

b) Hoạt động ứng cứu sự cố an toàn thông tin mạng phải chuyển từ bị động sang chủ động, bao gồm: chủ động thực hiện săn lùng mối nguy hại và rà quét lỗ hổng trên các hệ thống thông tin trong phạm vi quản lý tối thiểu 01 lần/6 tháng; ban hành phương án, kịch bản ứng cứu sự cố cho hệ thống thông tin trước ngày 31 tháng 12 năm 2022 và cập nhật kịp thời khi có thay đổi; tổ chức diễn tập thực chiến tối thiểu 01 lần/năm đối với hệ thống thông tin cấp độ 3 trở lên nhằm đánh giá khả năng phòng ngừa xâm nhập và khả năng phát hiện kịp thời các điểm yếu về quy trình, công nghệ, con người. Trường hợp phát hiện điểm yếu, lỗ hổng bảo mật cho phép xâm nhập và kiểm soát hệ thống thì thực hiện đồng thời khắc phục điểm yếu, lỗ hổng và săn lùng mối nguy hại.

c) Tổ chức, kiện toàn lại các Đội ứng cứu sự cố trước ngày 31 tháng 12 năm 2022 theo hướng chuyên nghiệp, cơ động, có tối thiểu 05 chuyên gia an toàn thông tin mạng (bao gồm cả chuyên gia thuê ngoài) đáp ứng chuẩn kỹ năng về an toàn thông tin do Bộ Thông tin và Truyền thông quy định.

d) Cơ quan chủ trì 11 lĩnh vực quan trọng cần ưu tiên bảo đảm an toàn thông tin mạng (theo Quyết định số 632/QĐ-TTg ngày 10 tháng 5 năm 2017 của Thủ tướng Chính phủ) chú trọng hoạt động chia sẻ thông tin về các nguy cơ, sự cố mất an toàn thông tin mạng cho các cơ quan, tổ chức, doanh nghiệp quản lý, vận hành hệ thống thông tin thuộc lĩnh vực và phục vụ kịp thời, hiệu quả cho Đội ứng cứu sự cố của lĩnh vực (CERT lĩnh vực).

đ) Giao Đội ứng cứu sự cố thực hiện các nhiệm vụ thường xuyên sau: làm đầu mối tiếp nhận, quản lý sự cố; ứng cứu, xử lý sự cố và săn lùng mối nguy hại; nghiên cứu, theo dõi các nguy cơ tấn công mạng, thông tin về lỗ hổng, điểm yếu; luyện tập các kỹ năng bảo vệ hệ thống thông tin và tham gia các chương trình huấn luyện, diễn tập do Cơ quan điều phối quốc gia chủ trì.

e) Bố trí đủ kinh phí bảo đảm hoạt động của Đội ứng cứu sự cố; thu hút nhân lực chất lượng cao vào làm công tác ứng cứu sự cố an toàn thông tin mạng.

g) Nghiêm túc thực hiện rà soát, phát hiện và khắc phục các lỗ hổng, điểm yếu theo cảnh báo của cơ quan chức năng; chủ động theo dõi, phát hiện sớm các nguy cơ mất an toàn thông tin mạng để kịp thời xử lý, khắc phục.

h) Có biện pháp kiểm soát nguy cơ mất an toàn thông tin mạng gây ra bởi bên thứ ba và các chuỗi cung ứng công nghệ thông tin và truyền thông.

i) Nghiêm túc thực hiện các quy định về báo cáo sự cố an toàn thông tin mạng; đẩy mạnh tuyên truyền cho người dân về việc báo cáo, cung cấp thông tin về sự cố.

k) Khuyến khích triển khai các chiến dịch nâng cao ý thức cảnh giác của người dùng cuối đối với các cuộc tấn công mạng.

l) Công bố thông tin đầu mối (số điện thoại, thư điện tử hoặc các kênh liên lạc khác) tiếp nhận thông báo sự cố trên cổng thông tin điện tử của cơ quan trước ngày 31 tháng 10 năm 2022.

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

a) Hướng dẫn phát triển Đội ứng cứu sự cố cho 11 lĩnh vực quan trọng cần ưu tiên bảo đảm an toàn thông tin mạng theo Quyết định số 632/QĐ-TTg ngày 10 tháng 5 năm 2017 của Thủ tướng Chính phủ.

b) Hướng dẫn triển khai các hoạt động thường xuyên của Đội ứng cứu sự cố và xây dựng khung năng lực Đội ứng cứu sự cố trước ngày 30 tháng 11 năm 2022.

c) Thúc đẩy hoạt động diễn tập thực chiến an toàn thông tin mạng tại các cơ quan, tổ chức, doanh nghiệp; sử dụng kết quả diễn tập làm tiêu chí để đánh giá mức độ trưởng thành, chuyên nghiệp các Đội ứng cứu sự cố hàng năm.

d) Chủ trì tổ chức triển khai, hướng dẫn, theo dõi, đôn đốc, kiểm tra và đánh giá việc thực hiện Chỉ thị này; tổng hợp, báo cáo Thủ tướng Chính phủ kết quả thực hiện.

3. Bộ Công an, Bộ Quốc phòng có trách nhiệm:

a) Triển khai các hoạt động ứng cứu sự cố theo chức năng, nhiệm vụ được giao.

b) Phối hợp chặt chẽ với Bộ Thông tin và Truyền thông trong hoạt động ứng cứu sự cố an toàn thông tin mạng quốc gia.

4. Bộ Tài chính có trách nhiệm hướng dẫn phân bổ và ưu tiên ngân sách cho hoạt động ứng cứu sự cố an toàn thông tin mạng.

5. Các doanh nghiệp cung cấp dịch vụ viễn thông, Internet:

a) Công bố thông tin đầu mối (số điện thoại, thư điện tử hoặc các kênh liên lạc khác) tiếp nhận thông báo sự cố trên cổng thông tin (website) trước ngày 31 tháng 10 năm 2022; tuyên truyền cho khách hàng về cách thức phản ánh sự cố mất an toàn thông tin mạng.

b) Nghiêm túc tuân thủ các yêu cầu điều phối của Cơ quan điều phối quốc gia trong các hoạt động ứng cứu, xử lý sự cố.

c) Cảnh báo cho khách hàng các nguy cơ, sự cố an toàn thông tin mạng trên diện rộng hoặc khi phát hiện nguy cơ, sự cố an toàn thông tin mạng liên quan tới khách hàng; hỗ trợ khách hàng ứng cứu, xử lý sự cố an toàn thông tin mạng liên quan tới dịch vụ do doanh nghiệp cung cấp.

6. Các doanh nghiệp an toàn thông tin mạng:

a) Cung cấp, chia sẻ thông tin về sự cố mất an toàn thông tin mạng về Bộ Thông tin và Truyền thông (Cục An toàn thông tin).

b) Phối hợp chặt chẽ với Cơ quan điều phối quốc gia trong các hoạt động ứng cứu, xử lý sự cố.

c) Chú trọng việc tham gia các tổ chức quốc tế về ứng cứu sự cố để đẩy mạnh hoạt động chia sẻ thông tin.

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, Cục, đơn vị trực thuộc, Công báo;
- Lưu: VT, KSTT (2).

KT. THỦ TƯỚNG
PHÓ THỦ TƯỚNG

Vũ Đức Đam