VĂN PHÒNG CHÍNH PHỦ	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 1634/CT-VPCP	*Hà Nội, ngày 20 tháng 4 năm 2024*

CHỈ THỊ
Về việc tăng cường bảo đảm an toàn thông tin mạng, an ninh mạng cho các hệ thống thông tin của Văn phòng Chính phủ

Thời gian vừa qua, các hoạt động tấn công mạng, gián điệp mạng nhắm vào các hệ thống thông tin của cơ quan, tổ chức và doanh nghiệp diễn biến hết sức phức tạp và tinh vi, trên nhiều lĩnh vực. Thủ tướng Chính phủ đã có nhiều văn bản[1] chỉ đạo các bộ, ngành, địa phương về tăng cường bảo đảm an toàn thông tin mạng, an ninh mạng (viết tắt là an toàn, an ninh mạng), tuy nhiên vẫn còn xảy ra một số sự cố gây mất an toàn, an ninh mạng tại một số ngành, lĩnh vực. Trước các nguy cơ bị tấn công mạng, khai thác lỗ hổng bảo mật, các hệ thống thông tin phục vụ hoạt động chỉ đạo, điều hành của Chính phủ, Thủ tướng Chính phủ do Văn phòng Chính phủ làm chủ quản cần phải được ưu tiên triển khai bảo đảm an toàn, an ninh mạng ở mức độ cao nhất.

Trên cơ sở đó, để khắc phục các tồn tại, hạn chế rủi ro tiềm ẩn, tăng cường hiệu lực, hiệu quả hoạt động bảo vệ, giám sát, phát hiện và ứng cứu sự cố an toàn, an ninh mạng cho các hệ thống thông tin của Văn phòng Chính phủ, Bộ trưởng, Chủ nhiệm yêu cầu:

1. Trưởng các Vụ, Cục, đơn vị sự nghiệp công lập, Cổng Thông tin điện tử Chính phủ tập trung chỉ đạo thực hiện đồng bộ các nhiệm vụ sau:

a) Trực tiếp chỉ đạo và phụ trách công tác bảo đảm an toàn, an ninh mạng trong hoạt động của đơn vị mình; chịu trách nhiệm trước pháp luật và Bộ trưởng, Chủ nhiệm nếu đơn vị mình quản lý xảy ra tình trạng mất an toàn, an ninh mạng, lộ lọt thông tin, bí mật nhà nước, dữ liệu công vụ do không tuân thủ quy định của pháp luật về an toàn, an ninh mạng.

b) Tiếp tục quán triệt cán bộ, công chức, viên chức, người lao động thực hiện nghiêm túc, hiệu quả chủ trương chỉ đạo của Đảng, pháp luật của nhà nước về bảo đảm an toàn, an ninh mạng và bảo vệ bí mật nhà nước trên không gian mạng.

---

[1] Chỉ thị số 14/CT-TTg ngày 07 tháng 6 năm 2019 về tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam; Chỉ thị số 18/CT-TTg ngày 13 tháng 10 năm 2022 về đẩy mạnh triển khai các hoạt động ứng cứu sự cố an toàn thông tin mạng Việt Nam; Chỉ thị số 09/CT-TTg ngày 23 tháng 02 năm 2024 về tuân thủ quy định pháp luật và tăng cường bảo đảm an toàn hệ thống thông tin theo cấp độ; Công điện số 33/CĐ-TTg ngày 07 tháng 4 năm 2024 về tăng cường bảo đảm an toàn thông tin mạng; Công văn số 1257/VPCP-KSTT ngày 10 tháng 4 năm 2024 của Văn phòng Chính phủ thông báo ý kiến chỉ đạo của Thủ tướng Chính phủ về việc rà soát nguy cơ tấn công, gián điệp mạng.

c) Tổ chức rà soát, thống kê, cập nhật danh mục hệ thống thông tin thuộc phạm vi quản lý; bảo đảm 100% hệ thống thông tin từ cấp độ 1 đến cấp độ 5 (nếu có) đang vận hành hoàn thành việc phê duyệt hồ sơ đề xuất cấp độ an toàn hệ thống thông tin chậm nhất trong tháng 9 năm 2024 và triển khai đầy đủ phương án bảo đảm an toàn thông tin theo hồ sơ đề xuất cấp độ được phê duyệt trong tháng 12 năm 2024.

d) Phối hợp với đơn vị chuyên trách về công nghệ thông tin của Văn phòng Chính phủ (Cục Kiểm soát thủ tục hành chính) và các đơn vị liên quan kiểm tra, rà soát an toàn, an ninh mạng đối với các hệ thống thông tin được giao quản trị, vận hành; kịp thời cập nhật các bản vá lỗ hổng bảo mật khi phát hiện hoặc được cảnh báo.

đ) Kịp thời báo cáo khi xảy ra sự cố tấn công mạng cho đơn vị chuyên trách về công nghệ thông tin của Văn phòng Chính phủ và tuân thủ quy trình điều phối, ứng cứu sự cố an toàn thông tin mạng của Văn phòng Chính phủ (ban hành theo Quyết định số 968/QĐ-VPCP ngày 18 tháng 10 năm 2018 của Bộ trưởng, Chủ nhiệm Văn phòng Chính phủ).

e) Thực hiện chế độ báo cáo định kỳ được quy định tại Quy chế quản lý công tác bảo đảm an toàn thông tin, an ninh mạng của Văn phòng Chính phủ ban hành theo Quyết định số 08/QĐ-VPCP ngày 07 tháng 01 năm 2020 của Bộ trưởng, Chủ nhiệm Văn phòng Chính phủ.

2. Cục Kiểm soát thủ tục hành chính có trách nhiệm:

a) Chủ động theo dõi, giám sát, phát hiện sớm các nguy cơ tấn công, ứng phó kịp thời các lỗ hổng bảo mật, điểm yếu đối với hệ thống thông tin đã được các đơn vị chức năng của Bộ Công an, Bộ Quốc phòng, Bộ Thông tin và Truyền thông và Ban Cơ yếu Chính phủ cảnh báo; định kỳ dò quét lỗ hổng bảo mật, kiểm thử xâm nhập các hệ thống thông tin, ứng dụng để phát hiện và khắc phục ngay các điểm yếu, tồn tại; tăng cường tổ chức diễn tập bảo đảm an toàn, an ninh mạng đối với các hệ thống thông tin được giao quản lý.

b) Chủ động phối hợp các đơn vị chức năng của các cơ quan, tổ chức liên quan đến lĩnh vực an toàn, an ninh mạng nhận diện các mối nguy hại về an toàn, an ninh mạng và rà quét lỗ hổng trên các hệ thống thông tin trong phạm vi quản lý tối thiểu 01 lần/năm; 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.

c) Kịp thời cảnh báo tới các đơn vị quản lý, vận hành các hệ thống CNTT tại VPCP về các nguy cơ, điểm yếu, lỗ hổng bảo mật đã được các đơn vị chức năng, tổ chức bảo mật cảnh báo hoặc qua rà quét, giám sát phát hiện được.

d) Rà soát, hoàn thiện, trình cấp có thẩm quyền ban hành quy định về bảo đảm an toàn, an ninh mạng cho các hệ thống thông tin, cơ sở dữ liệu phục vụ công tác chỉ đạo, điều hành của Chính phủ, Thủ tướng Chính phủ do Văn phòng Chính phủ làm chủ quản; chủ động rà soát các quy định, quy trình về an toàn, an ninh mạng của Văn phòng Chính phủ để kịp thời sửa đổi, bổ sung theo thẩm quyền hoặc đề xuất sửa đổi, bổ sung cho phù hợp với thực tiễn.

đ) Chủ trì, phối hợp với Vụ Quan hệ quốc tế, Vụ Tổ chức cán bộ tăng cường, thúc đẩy hợp tác quốc tế về an toàn, an ninh mạng theo chức năng, nhiệm vụ được giao nhằm nâng cao trình độ, kiến thức và biện pháp kỹ thuật, kinh nghiệm trong đảm bảo an toàn, an ninh mạng.

e) Phối hợp với các đơn vị chức năng của Bộ Công an, Bộ Quốc phòng, Bộ Thông tin và Truyền thông và Ban Cơ yếu Chính phủ kiểm tra, đánh giá an toàn, an ninh mạng đối với các hệ thống thông tin, cơ sở dữ liệu phục vụ công tác chỉ đạo, điều hành của Chính phủ, Thủ tướng Chính phủ do Văn phòng Chính phủ làm chủ quản.

g) Phối hợp với Vụ Tổ chức cán bộ tổ chức tập huấn, bồi dưỡng, nâng cao kiến thức, kỹ năng và đánh giá việc chấp hành quy định, bảo đảm an toàn, an ninh mạng cho cán bộ, công chức, viên chức, người lao động thuộc Văn phòng Chính phủ.

3. Cổng Thông tin điện tử Chính phủ có trách nhiệm:

a) Chủ động rà soát, hoàn thiện, ban hành theo thẩm quyền hoặc trình cấp có thẩm quyền ban hành quy định liên quan quản lý, vận hành và sử dụng các hệ thống thông tin do Cổng Thông tin điện tử Chính phủ làm chủ quản.

b) Chủ trì, phối hợp với các đơn vị liên quan triển khai các biện pháp, giải pháp bảo đảm an toàn, an ninh mạng cho các hệ thống thông tin do Cổng Thông tin điện tử làm chủ quản.

c) Tham gia hỗ trợ, phối hợp với đơn vị chuyên trách về công nghệ thông tin của Văn phòng Chính phủ triển khai biện pháp bảo đảm an toàn, an ninh mạng, diễn tập thực chiến bảo đảm an toàn thông tin mạng cho các hệ thống thông tin quan trọng.

d) Định kỳ gửi thư điện tử cho người dùng hệ thống thư điện tử công vụ Chính phủ để phổ biến, hướng dẫn, nhắc nhở, cảnh báo nguy cơ mã độc chiếm quyền điều khiển và mã hóa dữ liệu, thông tin trên máy tính người dùng.

4. Vụ Kế hoạch tài chính có trách nhiệm: Bảo đảm nguồn lực đầu tư, ưu tiên kinh phí cho việc triển khai các hoạt động, giải pháp bảo đảm an toàn, an ninh mạng đối với các hệ thống thông tin của VPCP theo quy định của pháp luật.

5. Các đơn vị cung cấp dịch vụ, vận hành các hệ thống thông tin có trách nhiệm:

a) Hoàn thành xây dựng hồ sơ đề xuất cấp độ an toàn cho 100% hệ thống thông tin trong tháng 6 năm 2024 và triển khai đầy đủ phương án bảo đảm an toàn thông tin theo hồ sơ đề xuất cấp độ được phê duyệt trong tháng 12 năm 2024.

b) Tăng cường quản lý, giám sát việc truy cập, can thiệp dữ liệu của các nhân sự tham gia các hoạt động quản trị, vận hành để bảo đảm quyền sở hữu dữ liệu của các hệ thống thông tin, cơ sở dữ liệu; chịu trách nhiệm trước pháp luật và cơ quan chủ quản hệ thống thông tin trong trường hợp xảy ra lộ, mất thông tin, dữ liệu từ phía nhân sự quản trị, vận hành.

c) Thường xuyên kiểm tra, đánh giá an toàn thông tin đối với các hệ thống thông tin được thuê quản trị, vận hành; kịp thời cập nhật các bản vá lỗ hổng bảo mật và báo cáo kết quả thực hiện cho cơ quan chủ quản (Văn phòng Chính phủ) qua đầu mối Cục Kiểm soát thủ tục hành chính.

6. Cục Kiểm soát thủ tục hành chính giúp Bộ trưởng, Chủ nhiệm theo dõi, đôn đốc việc thực hiện Chỉ thị này. Định kỳ hàng quý tổng hợp, báo cáo Bộ trưởng, Chủ nhiệm tình hình, kết quả thực hiện./.

Nơi nhận:
- Thủ tướng Chính phủ (để b/c);
- Phó Thủ tướng Trần Lưu Quang (để b/c);
- Các Bộ: Công an, Quốc phòng, Thông tin và Truyền thông;
- Ban Cơ yếu Chính phủ;
- Các Tập đoàn: Công nghiệp - Viễn thông Quân đội (Viettel), Bưu chính Viễn thông Việt Nam (VNPT);
- VPCP: BTCN, các PCN, Trợ lý TTg, TGĐ Cổng TTĐT, các Vụ, Cục, đơn vị trực thuộc, Công báo;
- Lưu: VT, KSTT (2). 12

BỘ TRƯỞNG, CHỦ NHIỆM

VĂN PHÒNG CHÍNH PHỦ

Trần Văn Sơn