BỘ CÔNG AN	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 60/TB-BCA-A05	*Hà Nội, ngày 28 tháng 7 năm 2025*

UBND TỈNH KHÁNH HÒA
ĐẾN Số: 2808
Ngày: 09/9
Chuyển:
Số và ký hiệu HS:

THÔNG BÁO
Hướng dẫn triển khai một số nhiệm vụ trọng tâm về an toàn thông tin mạng 06 tháng cuối năm 2025

Kính gửi:
- Các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ;
- Ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương.

(Khánh Hoà)

Thực hiện Nghị quyết số 190/2025/QH15 ngày 19/02/2025 của Quốc hội quy định về xử lý một số vấn đề liên quan đến sắp xếp tổ chức bộ máy nhà nước, từ ngày 01/3/2025, Bộ Công an tiếp nhận nhiệm vụ quản lý nhà nước về an toàn thông tin mạng từ Bộ Thông tin và Truyền thông. Căn cứ Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015; Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ; Quyết định số 964/QĐ-TTg ngày 10 tháng 8 năm 2022 của Thủ tướng Chính phủ phê duyệt Chiến lược An toàn, An ninh mạng quốc gia, chủ động ứng phó với các thách thức từ không gian mạng đến năm 2025, tầm nhìn 2030; Chỉ thị số 09/CT-TTg ngày 23 tháng 02 năm 2024 của Thủ tướng Chính phủ về tuân thủ quy định pháp luật và tăng cường bảo đảm an toàn hệ thống thông tin theo cấp độ; Thực hiện Công điện số 33/CĐ-TTg ngày 07 tháng 4 tháng 2024 của Thủ tướng Chính phủ về tăng cường bảo đảm an toàn thông tin mạng. Hiện nay, nguy cơ mất an toàn thông tin trong nước vẫn phổ biến, phức tạp. Việc bảo đảm an toàn thông tin trên không gian mạng không chỉ là trách nhiệm của cơ quan quản lý nhà nước mà còn là trách nhiệm chung của toàn xã hội. Theo thống kê, năm 2024 toàn quốc ghi nhận khoảng 5000 cuộc tấn công mạng, phát hiện gần 500.000 địa chỉ IP tham gia mạng botnet, gây thiệt hại đáng kể cho xã hội. Các cuộc tấn công chủ yếu nhằm vào các hệ thống thông tin có cấp độ an toàn thông tin mức 1, 2.

Thực hiện chức năng quản lý nhà nước về an toàn thông tin mạng, nhằm đẩy mạnh triển khai các hoạt động tuân thủ, bảo đảm an toàn thông tin mạng theo quy định tại các văn bản quy phạm pháp luật và chỉ đạo, điều hành của Thủ tướng Chính phủ tại các Chiến lược, Đề án, Quyết định, Chỉ thị nói chung và phòng chống tấn công mạng nói riêng; Bộ Công an đề nghị các Bộ, cơ quan ngang Bộ,

ban, ngành, tỉnh/thành phố trực thuộc Trung ương chỉ đạo tập trung triển khai một số nhiệm vụ trọng tâm về an toàn thông tin mạng trong 06 tháng cuối năm 2025 thuộc phạm vi quản lý như sau:

I. VĂN BẢN QUY PHẠM PHÁP LUẬT VÀ CHỈ ĐẠO, ĐIỀU HÀNH

Hiện nay, hành lang pháp lý về an toàn thông tin mạng đã cơ bản hoàn thiện ở mức chi tiết, đầy đủ để các cơ quan, tổ chức có căn cứ và hướng dẫn, tham chiếu để triển khai. Bộ Công an đề nghị các bộ, ngành, địa phương chỉ đạo rà soát tổng thể và tổ chức thực hiện để đảm bảo hoàn thành các nhiệm vụ được cấp có thẩm quyền giao tại các quy định pháp luật như: (1) Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015; (2) Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ; (3) Quyết định số 964/QĐ-TTg ngày 10 tháng 8 năm 2022 của Thủ tướng Chính phủ phê duyệt Chiến lược An toàn, An ninh mạng quốc gia, chủ động ứng phó với các thách thức từ không gian mạng đến năm 2025, tầm nhìn 2030.

II. CÁC NHIỆM VỤ TRỌNG TÂM CÁC THÁNG CUỐI NĂM 2025

1. Bảo đảm an toàn thông tin theo cấp độ

- Lãnh đạo các bộ, ngành, địa phương chỉ đạo các cơ quan, đơn vị trực thuộc hoàn thành mục tiêu 100% hệ thống thông tin cấp độ 1, 2, 3 thuộc phạm vi quản lý được phê duyệt Hồ sơ đề xuất cấp độ chậm nhất trong tháng 10 năm 2025; hệ thống thông tin cấp độ 4, 5 được lập hồ sơ gửi đề nghị về Bộ Công an thẩm định đúng quy định của pháp luật.

- 100% hệ thống thông tin thuộc phạm vi quản lý được triển khai đầy đủ phương án bảo đảm an toàn hệ thống thông tin theo cấp độ phê duyệt. Việc triển khai phương án bảo đảm an toàn thông tin cần đảm bảo hiệu quả, tiết kiệm. Ưu tiên lựa chọn giải pháp, sản phẩm an ninh mạng, an toàn thông tin do Việt Nam phát triển để chủ động về công nghệ, các giải pháp cần hỗ trợ quản lý tập trung để dễ vận hành, tiết kiệm chi phí, các hệ thống quản lý yêu cầu đặt máy chủ tại Việt Nam, tuân thủ với Nghị quyết số 57-NQ/TW ngày 22/12/2024 của Bộ Chính trị về đột phá phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia; Luật An ninh mạng, pháp luật về bảo vệ dữ liệu cá nhân và Quyết định số 1131/QĐ-TTg ngày 12/6/2025 của Thủ tướng Chính phủ ban hành danh mục công nghệ chiến lược và sản phẩm công nghệ chiến lược.

- Người đứng đầu cơ quan tổ chức trực tiếp chỉ đạo và ưu tiên nguồn lực để tổ chức thực thi và triển khai công tác bảo đảm an toàn hệ thống thông tin theo

cấp độ theo chỉ đạo của Thủ tướng Chính phủ tại Chỉ thị số 09/CT-TTg và Công điện số 33/CĐ-TTg.

- Trong 06 tháng cuối năm 2025, các bộ, ban, ngành, tỉnh/thành phố trực thuộc trung ương triển khai: (1) Xây dựng Hướng dẫn bảo đảm an toàn thông tin cấp bộ, ban, ngành, tỉnh/thành phố trực thuộc trung ương. (2) Tiếp tục tập huấn cho cán bộ phụ trách công tác bảo đảm an toàn hệ thống thông tin của đơn vị vận hành hệ thống thông tin.

2. Mô hình bảo đảm an toàn thông tin 04 lớp

- Phấn đấu 100% hệ thống thông tin của cơ quan, tổ chức được tổ chức bảo đảm an toàn thông tin thực chất, toàn diện; nâng cao năng lực của lớp giám sát, bảo vệ chuyên nghiệp và kết nối, chia sẻ thông tin với Trung tâm An ninh mạng quốc gia thuộc Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao.

- Nâng cao năng lực lực lượng tại chỗ đáp ứng yêu cầu mới thông qua đào tạo, tuyển dụng hoặc thuê chuyên gia, bảo đảm mỗi đơn vị chuyên trách an toàn thông tin có tối thiểu 05 chuyên gia an toàn thông tin mạng.

- Hoàn thành mở rộng phạm vi giám sát, bảo vệ cho 100% hệ thống thông tin thuộc phạm vi quản lý. Đối với các hệ thống thông tin cấp độ 3 trở lên, khuyến nghị tổ chức giám sát, bảo vệ đầy đủ các lớp: lớp mạng, lớp ứng dụng, lớp cơ sở dữ liệu, lớp thiết bị đầu cuối.

- Kiểm tra, đánh giá an toàn thông tin định kỳ theo quy định cho hệ thống thông tin thuộc phạm vi quản lý. Rà soát danh sách các trang web (.gov.vn) bao gồm cả các sub domain để kiểm tra, đánh giá an toàn thông tin định kỳ.

- Duy trì kết nối ổn định, chia sẻ đầy đủ dữ liệu giám sát theo thời gian thực về Trung tâm An ninh mạng quốc gia để được hỗ trợ giám sát, phân tích, cảnh báo sớm các nguy cơ về an toàn thông tin mạng và tấn công mạng.

- Ban hành quy trình báo cáo, phối hợp ứng phó sự cố theo sự điều phối của Trung tâm An ninh mạng quốc gia.

3. Kiểm tra tuân thủ

Kiểm tra tuân thủ quy định của pháp luật về an toàn thông tin mạng bảo đảm an toàn thông tin mạng vừa là bảo vệ tổ chức, nhưng cũng là trách nhiệm của tổ chức. Tuy nhiên, nhiều cơ quan chưa nhận thức hoặc nhận thức chưa đầy đủ vấn đề này. Vì vậy, nhận thức và mức độ tuân thủ các quy định về bảo đảm an toàn thông tin của các đơn vị trực thuộc các bộ, ngành, địa phương còn lỏng lẻo, hạn chế, chưa được quan tâm thực hiện đầy đủ. Đây là một trong những

nguyên nhân cơ bản khiến cho nguy cơ mất an toàn thông tin trong hoạt động của cơ quan, tổ chức còn nhiều vấn đề đáng lo ngại. Theo quy định của Nghị định số 85/2016/NĐ-CP và Thông tư số 12/2022/TT-BTTTT, chủ quản hệ thống thông tin và đơn vị chuyên trách có trách nhiệm định kỳ tổ chức kiểm tra, đánh giá an toàn thông tin đối với các cơ quan, tổ chức thuộc phạm vi quản lý. Bộ Công an đề nghị:

- Phấn đấu 100% bộ, ngành, địa phương tổ chức kiểm tra, đánh giá tuân thủ quy định của pháp luật về an toàn thông tin.

- Trong 06 tháng cuối năm 2025, tổ chức tối thiểu 01 đoàn kiểm tra, đánh giá tuân thủ các quy định pháp luật về an toàn thông tin đối với các đơn vị, tổ chức, doanh nghiệp thuộc phạm vi quản lý.

Nội dung: Kiểm tra tuân thủ quy định pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ (theo Luật An toàn thông tin mạng, Nghị định số 85/2016/NĐ-CP và các văn bản hướng dẫn).

Đối tượng: Trọng tâm là các đơn vị, tổ chức, doanh nghiệp đang được giao quản lý, vận hành nhiều hệ thống thông tin hoặc hệ thống thông tin quan trọng, dùng chung.

4. Diễn tập thực chiến

Ngày 13 tháng 10 năm 2022, Thủ tướng Chính phủ đã ban hành Chỉ thị số 18/CT-TTg về việc đẩy mạnh ứng cứu sự cố an toàn thông tin mạng Việt Nam, trong đó nêu rõ các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương: "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". Diễn tập thực chiến đã thực sự đã tạo ra hiệu ứng tích cực và đạt được hiệu quả rõ ràng. Chất lượng diễn tập thực chiến cũng được cải thiện. Việc phát hiện và xử lý kịp thời này đóng vai trò quan trọng trong việc bảo vệ hệ thống thông tin cũng như cơ quan, tổ chức, doanh nghiệp, người dân sử dụng các hệ thống thông tin. Bộ Công an đề nghị 100% bộ, ngành, địa phương tổ chức diễn tập thực chiến trong năm 2025. Mỗi bộ, ngành, địa phương tổ chức tối thiểu 01 cuộc diễn tập thực chiến an toàn thông tin mạng trong năm 2025. Trong đó, đảm bảo có tổ chức diễn tập thực chiến cho các hệ thống thông tin cấp độ 3 trở lên.

Bộ Công an đề nghị các bộ, ban, ngành, ủy ban nhân dân các tỉnh/thành phố trực thuộc trung ương tiến hành xây dựng phương hướng thực hiện nhiệm vụ 06

tháng cuối năm 2025. Kết quả tổng kết về công tác bảo đảm an toàn thông tin mạng gửi về Bộ Công an (qua Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao - Địa chỉ: Lô E2 khu đô thị Cầu Giấy mới, phường Cầu Giấy, thành phố Hà Nội) trước ngày **15/11/2025** để tập hợp, báo cáo Chính phủ theo quy định tại Điều 52 Luật An toàn thông tin mạng./.

Bộ Công an trân trọng thông báo./.

Nơi nhận:
- Như trên;
- Đ/c Bộ trưởng (để báo cáo);
- Lưu: VT, A05(P7).PNH.56b

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

Thượng tướng Phạm Thế Tùng