

Số: 1607/BTTTT-CATTT

Hà Nội, ngày 26 tháng 04 năm 2024

V/v hướng dẫn triển khai
một số nhiệm vụ trọng tâm về
an toàn thông tin mạng trong năm 2024

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.

Căn cứ Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015;

Căn cứ 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;

Thực hiện 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;

Thực hiện 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 năm 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 nói chung và vấn nạn lừa đảo trên không gian mạng đang trở nên ngày càng phổ biến, phức tạp và gây hậu quả ngày càng lớn. Việc bảo đảm an toàn thông tin, phòng chống lừa đảo 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. Chủ đề năm 2024 trong lĩnh vực an toàn thông tin được Bộ Thông tin và Truyền thông lựa chọn là **“Năm phòng chống lừa đảo trực tuyến”**.

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 lừa đảo trực tuyến nói riêng; Bộ Thông tin và Truyền thông hướng dẫn và trân trọng đề nghị Quý Cơ quan chỉ đạo đơn vị chuyên trách về an toàn thông tin (đơn vị được giao chuyên trách về an toàn thông tin tại các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ; Sở Thông tin và Truyền thông các tỉnh, thành phố trực thuộc Trung ương) tham mưu tập trung triển khai một số nhiệm vụ trọng tâm về

an toàn thông tin mạng trong năm 2024 thuộc phạm vi quản lý như sau:

I. CÁC 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 Thông tin và Truyền thông trân trọng đề nghị Quý Cơ quan 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.

Chi tiết danh sách văn bản cần rà soát, tổ chức thực hiện và hướng dẫn tổ chức thực hiện xem tại Phụ lục kèm theo.

II. CÁC NHIỆM VỤ TRỌNG TÂM NĂM 2024

Để đảm bảo sự đồng bộ, thống nhất từ Trung ương tới địa phương trong việc nhận thức và triển khai thiết thực, hiệu quả công tác bảo đảm an toàn thông tin mạng trong hoạt động của cơ quan, tổ chức nhà nước, góp phần tăng cường bảo đảm an toàn không gian mạng quốc gia, Bộ Thông tin và Truyền thông trân trọng đề nghị Quý Cơ quan chỉ đạo tập trung triển khai một số nhiệm vụ trọng tâm về an toàn thông tin mạng trong năm 2024 thuộc phạm vi quản lý như sau:

1. Bảo đảm an toàn hệ thống thông tin theo cấp độ

Bảo đảm an toàn hệ thống thông tin theo cấp độ là tinh thần cốt lõi của Luật An toàn thông tin mạng và hành lang pháp lý về an toàn thông tin mạng. Đồng thời, là đặc điểm, đặc trưng riêng của Việt Nam trong công tác bảo đảm an toàn thông tin mạng nhằm tập trung nguồn lực, giải pháp để bảo đảm an toàn theo mức độ quan trọng của thông tin, hệ thống thông tin trong bối cảnh nguồn lực dành cho an toàn thông tin còn nhiều khó khăn, hạn chế.

Dù Luật đã quy định, Thủ tướng Chính phủ đã chỉ đạo, Bộ TT&TT đôn đốc quyết liệt nhưng đến nay, theo thống kê của Cục An toàn thông tin trên cả nước mới chỉ có 2.265 trong 3.418 hệ thống thông tin của cơ quan, tổ chức nhà nước được phê duyệt hồ sơ đề xuất cấp độ (đạt 69,2%). Tỷ lệ phê duyệt của các bộ, ngành đạt 56%. Tỷ lệ phê duyệt của các địa phương đạt 70%. Tỷ lệ hệ thống thông tin triển khai đầy đủ phương án bảo đảm an toàn hệ thống thông tin theo cấp độ trên cả nước chỉ đạt khoảng 20,9%.

Chính phủ, Thủ tướng Chính phủ rất quan tâm và chỉ đạo quyết liệt công tác bảo đảm an toàn hệ thống thông tin theo cấp độ. Thủ tướng Chính phủ đã ban hành 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 và Công điện số 33/CD-TTg ngày 07 tháng 4 tháng 2024 về tăng cường bảo đảm an toàn thông

tin mạng. Để triển khai Chỉ thị, Công điện của Thủ tướng, Bộ Thông tin và Truyền thông trân trọng đề nghị Quý Cơ quan quan tâm chỉ đạo:

1.1. Mục tiêu

- 100% hệ thống thông tin thuộc phạm vi quản lý được phê duyệt Hồ sơ đề xuất cấp độ chậm nhất trong tháng 9 năm 2024.
- 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 được phê duyệt, chậm nhất trong tháng 12 năm 2024.

1.2. Giải pháp

- 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.
- Sử dụng thường xuyên, hiệu quả Nền tảng Hỗ trợ quản lý bảo đảm an toàn hệ thống thông tin theo cấp độ đã được Bộ Thông tin và Truyền thông cung cấp cấp miễn phí, hướng dẫn sử dụng tại Công văn số 2046/BTTTT-CATTT ngày 01 tháng 6 năm 2023 và Công văn số 387/CATTT-ATHTTT ngày 18 tháng 3 năm 2024.
- Phổ biến và áp dụng hiệu quả Sổ tay Hướng dẫn bảo đảm an toàn hệ thống thông tin theo cấp độ được ban hành tại Công văn số 478/CATTT-ATHTTT ngày 30 tháng 3 năm 2024.
- Trong năm 2024, Bộ Thông tin và Truyền thông sẽ triển khai: (1) Xây dựng Hướng dẫn bảo đảm an toàn thông tin cấp bộ, tỉnh; (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 sau khi năm 2023 đã triển khai cho hơn 1.200 cán bộ trên cả nước.
- Định kỳ trước 20 hàng tháng, cung cấp thông tin về tình hình, kết quả triển khai về Bộ Thông tin và Truyền thông (Cục An toàn thông tin) thông qua Nền tảng hỗ trợ bảo đảm an toàn hệ thống thông tin theo cấp độ.

1.3. Đầu mối hướng dẫn, hỗ trợ

Bà Lê Thị Quỳnh Trang, Phòng An toàn hệ thống thông tin, Cục An toàn thông tin, Bộ Thông tin và Truyền thông; số điện thoại: 0919247397; thư điện tử: lqtrang@mic.gov.vn.

2. Duy trì và nâng cao hiệu quả công tác bảo đảm an toàn thông tin theo mô hình “4 lớp”

Bảo đảm an toàn thông tin theo mô hình “4 lớp” (Lực lượng tại chỗ; Tổ chức

hoặc doanh nghiệp giám sát, bảo vệ chuyên nghiệp; Tổ chức hoặc doanh nghiệp độc lập kiểm tra, đánh giá định kỳ; Kết nối, chia sẻ thông tin với hệ thống giám sát quốc gia) được Thủ tướng Chính phủ chỉ đạo thực hiện tại Chỉ thị số 14/CT-TTg ngày 07 tháng 6 năm 2019 của Thủ tướng Chính phủ về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam. Bộ Thông tin và Truyền thông hướng dẫn thực hiện tại: công văn số 1552/BTTTT-CATTT ngày 28 tháng 4 năm 2020 về việc đôn đốc tổ chức triển khai bảo đảm an toàn thông tin cho hệ thống thông tin theo mô hình “4 lớp”; Công văn số 1598/BTTTT-CATTT ngày 28 tháng 4 năm 2022 về việc tăng cường bảo đảm an toàn thông tin theo cấp độ và nâng cao năng lực bảo đảm an toàn thông tin theo mô hình “4 lớp”; Công văn số 235/CATTT-ATHTTT ngày 08 tháng 4 năm 2020 của Cục An toàn thông tin về việc hướng dẫn mô hình đảm bảo an toàn thông tin cấp bộ, tỉnh.

Hiện nay, thống kê theo báo cáo của các cơ quan, 100% bộ, cơ quan ngang bộ, địa phương đã triển khai bảo đảm an toàn thông tin theo mô hình “4 lớp”. Tuy nhiên, Bộ Thông tin và Truyền thông thấy rằng việc tổ chức bảo đảm an toàn thông tin theo mô hình “4 lớp” của các cơ quan vẫn ở mức cơ bản, mang tính hình thức chưa thực chất và đầy đủ yêu cầu để bảo đảm an toàn thông tin. Bộ Thông tin và Truyền thông trân trọng đề nghị Quý Cơ quan quan tâm chỉ đạo:

2.1. Mục tiêu

100% hệ thống thông tin của cơ quan, tổ chức được tổ chức bảo đảm an toàn thông tin thực chất, toàn diện theo hướng dẫn của Bộ Thông tin và Truyền thông; nâng cao năng lực của lớp giám sát, bảo vệ chuyên nghiệp và kết nối, chia sẻ thông tin với hệ thống giám sát quốc gia.

2.2. Giải pháp

- 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 chậm nhất trong tháng 11 năm 2024. 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 webiste (.gov.vn) bao gồm cả các sub domain để tiến hành đánh giá an toàn thông tin định kỳ và triển khai gán nhãn tín nhiệm mạng cho các webiste.

- Duy trì kết nối ổn định, chia sẻ đầy đủ dữ liệu giám sát theo thời gian thực

về Hệ thống giám sát 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.

- Thay đổi tư duy từ phát triển các hệ thống thông tin, phần mềm riêng lẻ sang đầu tư các nền tảng số hoặc thuê mua các dịch vụ do các doanh nghiệp cung cấp hạ tầng đã triển khai đầy đủ giải pháp bảo đảm an toàn hệ thống thông tin theo cấp độ và mô hình “4 lớp”.

2.3. Đầu mối hướng dẫn, hỗ trợ

Ông Phạm Tuấn An, Phòng An toàn hệ thống thông tin, Cục An toàn thông tin, Bộ Thông tin và Truyền thông; số điện thoại: 0984545179; thư điện tử: anpt@mic.gov.vn.

3. 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. Nếu không tuân thủ, tổ chức sẽ phải đối mặt với rủi ro và chịu trách nhiệm trước pháp luật khi xảy ra sự cố. Theo Luật, an toàn thông tin mạng là yêu cầu “bắt buộc”, không phải là yếu tố để “lựa chọn”. 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 Thông tin và Truyền thông trân trọng đề nghị Quý Cơ quan quan tâm chỉ đạo:

3.1. Mục tiêu

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

3.2. Giải pháp

Trong năm 2024, 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. Từ đó đưa hoạt động bảo đảm an toàn thông tin trở nên quy củ, hiệu quả. Trong đó:

Ưu tiên, tập trung 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) và bảo vệ thông tin, dữ liệu cá nhân (theo quy định tại Mục 2 Chương II Luật An toàn thông tin mạng).

Ưu tiên kiểm tra, đánh giá đối với 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.

3.3. Đầu mối hướng dẫn, hỗ trợ

Ông Vũ Ngọc Hưng, chuyên viên, Phòng Pháp chế và Kiểm tra, Cục An toàn thông tin, Bộ Thông tin và Truyền thông; số điện thoại: 0948977677; thư điện tử: vnhung@mic.gov.vn.

4. Sử dụng hiệu quả các nền tảng số

Theo đánh giá của Bộ Thông tin và Truyền thông, hiện trạng hiện nay của nhiều các cơ quan là: thiếu nhân sự, thiếu công cụ, thiếu kinh phí, thiếu năng lực và kinh nghiệm an toàn thông tin để đáp ứng được yêu cầu thực tế. Vì vậy, việc tận dụng tối đa năng lực của các nền tảng số, công cụ sẽ là phương án để các tổ chức bù đắp cho những thiếu hụt trên. Năm 2023, Bộ Thông tin và Truyền thông đã giao Cục An toàn thông tin nghiên cứu, phát triển và cung cấp 03 nền tảng, các khóa học nâng cao kiến thức kỹ năng, các tài liệu truyền truyền để hỗ trợ công tác quản lý nhà nước và thực thi pháp luật về an toàn thông tin hoàn toàn miễn phí cho các cơ quan, tổ chức. Các nền tảng, tài liệu đều được thường xuyên nghiên cứu, cải tiến, cập nhật tính năng và hiệu năng để có thể hỗ trợ tốt nhất cho các bộ, ngành, địa phương. Tuy nhiên, nhiều tổ chức vẫn chưa sử dụng hoặc sử dụng chưa hiệu quả.

Bộ Thông tin và Truyền thông trân trọng đề nghị Quý Cơ quan quan tâm chỉ đạo:

4.1. Mục tiêu

100% các bộ, ngành, địa phương triển khai áp dụng hiệu quả các nền tảng được cung cấp để thực hiện quản lý nhà nước và thực thi pháp luật trong phạm vi quản lý, giúp chuyển đổi số và giám sát, đo lường hoạt động bảo đảm an toàn thông tin mạng.

4.2. Giải pháp

Chỉ đạo các đơn vị tìm hiểu kỹ lưỡng, áp dụng hiệu quả các nền tảng được cung cấp để thực hiện quản lý nhà nước và thực thi pháp luật trong phạm vi quản lý, bao gồm: (1) Nền tảng Hỗ trợ quản lý bảo đảm an toàn hệ thống thông tin theo cấp độ; (2) Nền tảng Hỗ trợ điều phối, ứng cứu sự cố; (3) Nền tảng Hỗ trợ điều tra số. Bộ Thông tin và Truyền thông sẽ thường xuyên nghiên cứu, cải tiến, cập nhật tính năng và hiệu năng các nền tảng để có thể hỗ trợ tốt nhất cho các bộ, ngành, địa phương.

Trong năm 2024, Cục sẽ cung cấp thêm một số nền tảng để các bộ, ngành, địa phương triển khai công tác bảo đảm an toàn thông tin thống nhất, đồng bộ và thuận lợi, hiệu quả hơn nữa: (1) Nền tảng Quản lý và phát hiện, cảnh báo sớm rủi ro an toàn thông tin; (2) Nền tảng Hỗ trợ diễn tập thực chiến; (3) Nền tảng Đánh giá mức độ trưởng thành đội ứng cứu sự cố.

4.3. Đầu mối hướng dẫn, hỗ trợ

Ông Trần Mạnh Thắng, Phó Trưởng phòng, Phòng An toàn hệ thống thông tin, Cục An toàn thông tin, Bộ Thông tin và Truyền thông; số điện thoại: 0963791366; thư điện tử: tmthang@mic.gov.vn.

5. Phòng chống lừa đảo trực tuyến

Thời gian qua, người dân Việt Nam thường xuyên phải đối mặt với vấn nạn lừa đảo qua mạng (lừa đảo trực tuyến), các đối tượng xấu (đối tượng lừa đảo) tìm mọi cách để lợi dụng, khai thác đánh vào điểm yếu nhất là con người. Chúng áp dụng nhiều biện pháp tác động tâm lý để lấy lòng tin và dẫn dắt theo kịch bản. Các hình thức lừa đảo trên mạng liên tục gia tăng không ngừng, từ lừa đảo đánh cắp thông tin cá nhân, lừa đảo tình cảm, lừa đảo đầu tư,...

Các kỹ thuật tấn công lừa đảo phát triển ngày càng cao do kết hợp nhiều công nghệ mới, từ việc đơn giản là lừa đảo mật khẩu tài khoản qua email đến kết hợp với trí tuệ nhân tạo (AI) và giả mạo sâu (DeepFake), thông qua mạng xã hội, thiết bị di động, thiết bị IoT (Internet of Things) để thực hiện các cuộc tấn công lừa đảo tinh vi hơn. Lừa đảo trực tuyến đã trở thành một trong những mối đe dọa lớn nhất trong thế giới số. Bộ Thông tin và Truyền thông trân trọng đề nghị Quý Cơ quan quan tâm chỉ đạo:

5.1. Mục tiêu

100% người dân trên địa bàn được tuyên truyền thường xuyên, liên tục thông qua các tổ chức mạng lưới, phương tiện thông tin đại chúng, hệ thống thông tin cơ sở, mạng xã hội,...

5.2. Giải pháp

- Bộ Thông tin và Truyền thông thành lập Liên minh Phòng chống lừa đảo trực tuyến trên không gian mạng để hướng dẫn, kết nối, cung cấp thông tin, tài liệu và triển khai các giải pháp kỹ thuật phòng chống lừa đảo trực tuyến thông qua 04 hướng tiếp cận chính: (1) thông qua mạng viễn thông; (2) thông qua mạng xã hội; (3) thông qua tuyên truyền, giáo dục; (4) thông qua công nghệ.

- Các bộ, ngành, địa phương triển khai các hoạt động theo hướng dẫn của Bộ Thông tin và Truyền thông và Liên minh. Cơ quan, tổ chức liên hệ Cục An toàn thông tin hoặc truy cập Cổng không gian mạng quốc gia (khonggianmang.vn),

website của Cục An toàn thông tin (ais.gov.vn) để kịp thời nhận được cảnh báo, cung cấp miễn phí nội dung tuyên truyền (video, tài liệu, poster, bài viết,...). Tận dụng tối đa tất cả các kênh tuyên truyền như: sự kiện, mạng xã hội, website, hệ thống thư điện tử, tin nhắn SMS, các ứng dụng thông minh,...Tuyên truyền thường xuyên, liên tục tới toàn thể cán bộ, công chức, viên chức, người lao động của cơ quan và người dân trên địa bàn thông qua các hệ thống thông tin cơ sở (đài truyền thanh, đài truyền hình), các Tổ công nghệ số cộng đồng để tuyên truyền nhận thức, kỹ năng cho người dân, nhất là người vùng nông thôn, vùng xa để tránh bị lừa đảo trên không gian mạng. Khuyến nghị việc tuyên truyền qua các kênh nêu trên cần được thực hiện định kỳ hàng tuần, tháng, Quý tùy theo nội dung để đảm bảo tính thường xuyên, liên tục.

- Chỉ đạo các cơ quan chức năng thường xuyên cập nhật thông tin, tiếp nhận cảnh báo của Bộ Thông tin và Truyền thông (Cục An toàn thông tin) để kịp thời triển khai tuyên truyền tới người sử dụng khi có những vấn đề an toàn thông tin, hình thức tấn công mạng mới phát sinh.

- Tổ chức xây dựng một số nội dung tuyên truyền ấn tượng, phù hợp với đặc điểm, đặc trưng, bản sắc văn hóa của ngành, địa phương để tạo hiệu quả cao và phạm vi tuyên truyền rộng đến mọi đối tượng của cộng đồng.

- Tham gia hưởng ứng mạnh mẽ Chiến dịch Tuyên truyền nâng cao nhận thức về an toàn thông tin do Bộ Thông tin và Truyền thông phát động.

5.3. Đầu mối hướng dẫn, hỗ trợ

Ông Nguyễn Phú Lương, Trung tâm Giám sát an toàn không gian mạng quốc gia, Cục An toàn thông tin, Bộ Thông tin và Truyền thông; số điện thoại: 0886682266; thư điện tử: npluong@mic.gov.vn.

6. Diễn tập thực chiến an toàn thông tin mạng

Thủ tướng Chính phủ đã ban hành Chỉ thị số 18/CT-TTg ngày 13 tháng 10 năm 2022 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.”*

Năm 2022, đã tổ chức 03 diễn tập thực chiến quy mô quốc gia và hướng dẫn 36% bộ ngành, 54% địa phương diễn tập thực chiến. Có gần 2.500 lượt chuyên gia tham gia. Phát hiện hơn 340 lỗ hổng, điểm yếu.

Năm 2023, đã tổ chức 03 diễn tập thực chiến quốc gia, phát hiện 488 lỗ hổng,

điểm yếu. Đã có 55% bộ ngành, 83% địa phương diễn tập thực chiến trong năm. Theo báo cáo của các cơ quan, đến thời điểm hiện tại có khoảng 4.500 lượt chuyên gia tham gia, phát hiện 1.150 lỗ hổng, điểm yếu.

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 báo cáo về Bộ Thông tin và Truyền thông năm 2023 cũng được cải thiện nhiều, hầu như địa phương nào cũng phát hiện ra lỗ hổng nghiêm trọng. Việc phát hiện và xử lý kịp thời này đóng vai trò quan trọng trong việc bảo vệ hệ thống cũng như cơ quan, tổ chức, doanh nghiệp, người dân sử dụng các hệ thống này. Điểm đáng lưu ý là còn khoảng cách rất lớn về hiệu quả, chất lượng giữa diễn tập thực chiến quốc gia và diễn tập thực chiến ở địa phương. Riêng số lỗ hổng nghiêm trọng/cao trong 03 diễn tập thực chiến quốc gia đã lớn hơn 50 cuộc diễn tập của các cơ quan, tổ chức (09 bộ, ngành, 33 tỉnh thành, và 08 tổ chức, doanh nghiệp) trên toàn quốc cộng lại. Vì vậy, hoạt động này cần được thực hiện định kỳ, thường xuyên.

Bộ Thông tin và Truyền thông trân trọng đề nghị Quý Cơ quan quan tâm chỉ đạo:

6.1. Mục tiêu

100% bộ, ngành, địa phương tổ chức diễn tập thực chiến trong năm 2024.

6.2. Giải pháp

- Mỗi bộ, ngành, địa phương tổ chức tối thiểu 01 cuộc diễn tập thực chiến an toàn thông tin mạng trong năm 2024. Trong đó, đảm bảo có tổ chức diễn tập thực chiến cho các hệ thống thông tin cấp độ 3 trở lên. Đây cũng sẽ là một trong các tiêu chí được Cục An toàn thông tin sử dụng để đánh giá mức độ trưởng đội ứng cứu sự cố của cơ quan.

Quy trình, cách thức diễn tập thực chiến đã được Bộ Thông tin và Truyền thông hướng dẫn cụ thể tại Quyết định số 1429/QĐ-BTTTT ngày 26 tháng 7 năm 2022 của Bộ trưởng Bộ Thông tin và Truyền thông và Hướng dẫn số 01/HD-CATTT ngày 24 tháng 2 năm 2022 của Cục An toàn thông tin.

Đối với các hệ thống thông tin được sử dụng để diễn tập thực chiến, khi phát hiện ra lỗ hổng, điểm yếu hoặc sự cố tấn công mạng, ngoài việc cập nhật bản vá, cần thực hiện sẵn lòng mỗi nguy hại để phát hiện và xử lý hành vi xâm nhập, phá hoại đã được thực hiện trước khi lỗ hổng, điểm yếu được phát hiện. Từ đó, loại bỏ nguy cơ tiềm ẩn dẫn đến mất an toàn hệ thống thông tin.

- Dự kiến Quý III/2024, Bộ Thông tin và Truyền thông sẽ thiết lập Nền tảng Hỗ trợ diễn tập thực chiến để hỗ trợ các bộ ngành địa phương tri thức, tình huống, phương pháp xử lý các vấn đề và quản lý diễn tập thực chiến. Với nền tảng này, việc triển khai diễn tập thực chiến tại các cơ quan, tổ chức sẽ dễ dàng và đạt chất

lượng cao hơn, đồng bộ và thu hẹp dần khoảng cách giữa các cơ quan cũng như với diễn tập thực chiến quốc gia.

6.3. Đầu mối hướng dẫn, hỗ trợ

Ông Lê Công Phú, Phó Giám đốc, Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT/CC), Cục An toàn thông tin, Bộ Thông tin và Truyền thông; số điện thoại: 0977717759; thư điện tử: phulc@mic.gov.vn.

Để bảo đảm an toàn thông tin mạng trong hoạt động của các bộ, ngành, địa phương, góp phần nâng cao năng lực bảo đảm an toàn không gian mạng quốc gia, Bộ Thông tin và Truyền thông trân trọng đề nghị Quý Cơ quan chỉ đạo đơn vị chuyên trách về an toàn thông tin tập trung tham mưu và tổ chức triển khai một số nhiệm vụ trọng tâm nêu trên.

Trong quá trình thực hiện, nếu có khó khăn, vướng mắc, trân trọng đề nghị Quý Cơ quan liên hệ với Bộ Thông tin và Truyền thông (Cục An toàn thông tin) để được hướng dẫn, hỗ trợ triển khai.

- Đầu mối hỗ trợ, hướng dẫn tổng thể các nội dung tại văn bản này: Ông Nguyễn Văn Trường, Phòng Quy hoạch và Phát triển, Cục An toàn thông tin, Bộ Thông tin và Truyền thông. Số điện thoại: 0349729092. Thư điện tử: nv_truong@mic.gov.vn.

- Đầu mối hướng dẫn, hỗ trợ chi tiết đối với từng nhiệm vụ: chi tiết tại từng nhiệm vụ nêu trên.

Trân trọng./.

Nơi nhận:

- Như trên;
- Bộ trưởng (để b/c);
- Thứ trưởng Phạm Đức Long;
- Đơn vị chuyên trách CNTT/ATTT của: các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ; Văn phòng Trung ương Đảng; Văn phòng Quốc hội; Văn phòng Chủ tịch nước; Tòa án nhân dân tối cao; Viện Kiểm sát nhân dân tối cao; Ủy ban Trung ương Mặt trận Tổ quốc Việt Nam;
- Sở TT&TT các tỉnh, thành phố trực thuộc TW;
- Lưu: VT, CATT. QHPT.NVT

**KT. BỘ TRƯỞNG
THỨ TRƯỞNG**



Phạm Đức Long

Phụ lục

DANH SÁCH VĂN BẢN QUY PHẠM PHÁP LUẬT VÀ CHỈ ĐẠO, ĐIỀU HÀNH LĨNH VỰC AN TOÀN THÔNG TIN

(Kèm theo Công văn số /BT-TT-CATT
ngày / /2024 của Bộ Thông tin và Truyền thông)

1. Danh sách văn bản quy phạm pháp luật

- 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 05/2017/QĐ-TTg ngày 16 tháng 3 năm 2017 của Thủ tướng Chính phủ ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia;
- Thông tư số 20/2017/TT-BTTTT ngày 12 tháng 9 năm 2017 của Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc;
- Thông tư số 31/2017/TT-BTTTT ngày 15 tháng 11 năm 2017 quy định hoạt động giám sát an toàn hệ thống thông tin;
- Thông tư số 12/2022/TT-BTTTT ngày 12 tháng 8 năm 2022 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 về bảo đảm an toàn hệ thống thông tin theo cấp độ.

2. Danh sách văn bản chỉ đạo, điều hành của Thủ tướng Chính phủ

- Quyết định số 632/QĐ-TTg ngày 10 tháng 5 năm 2017 của Thủ tướng Chính phủ ban hành Danh mục lĩnh vực quan trọng cần ưu tiên bảo đảm an toàn thông tin mạng và hệ thống thông tin quan trọng quốc gia;
- Quyết định số 1622/QĐ-TTg ngày 25 tháng 10 năm 2017 của Thủ tướng Chính phủ phê duyệt Đề án đẩy mạnh hoạt động của mạng lưới ứng cứu sự cố, tăng cường năng lực cho các cán bộ, bộ phận chuyên trách ứng cứu sự cố an toàn thông tin mạng trên toàn quốc đến 2020, định hướng đến 2025;
- Quyết định số 1017/QĐ-TTg ngày 14 tháng 8 năm 2018 của Thủ tướng Chính phủ Phê duyệt Đề án giám sát an toàn thông tin mạng đối với hệ thống, dịch vụ công nghệ thông tin phục vụ Chính phủ điện tử đến năm 2020, định hướng đến 2025;
- Quyết định số 1907/QĐ-TTg ngày 23 tháng 11 năm 2020 của Thủ tướng Chính phủ phê duyệt Đề án “Tuyên truyền, nâng cao nhận thức và phổ biến kiến thức về an toàn thông tin giai đoạn 2021 - 2025”;

- Quyết định số 21/QĐ-TTg ngày 06 tháng 01 năm 2021 của Thủ tướng Chính phủ phê duyệt Đề án “Đào tạo và phát triển nguồn nhân lực an toàn thông tin giai đoạn 2021 - 2025”;

- Quyết định số 830/QĐ-TTg ngày 01 tháng 06 năm 2021 của Thủ tướng Chính phủ phê duyệt Chương trình “Bảo vệ và hỗ trợ trẻ em tương tác lành mạnh, sáng tạo trên môi trường mạng giai đoạn 2021 - 2025”;

- 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 (gọi tắt là Chiến lược An toàn, An ninh mạng quốc gia);

- Chỉ thị số 14/CT-TTg ngày 25 tháng 5 năm 2018 của Thủ tướng Chính phủ về việc nâng cao năng lực phòng, chống phần mềm độc hại;

- Chỉ thị số 14/CT-TTg ngày 07 tháng 6 năm 2019 của Thủ tướng Chính phủ về việc 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 của Thủ tướng Chính phủ về đẩy mạnh triển khai các hoạt động ứng cứu sự cố an toàn thông tin mạng Việt Nam;

- Chỉ thị số 23/CT-TTg ngày 26 tháng 12 năm 2022 của Thủ tướng Chính phủ về tăng cường công tác bảo đảm an toàn thông tin mạng, an ninh thông tin cho thiết bị camera giám sát.

- 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.

- Công điện số 33/CD-TTg ngày 07 tháng 4 năm 2024 của Thủ tướng Chính phủ về tăng cường bảo đảm an toàn thông tin mạng.

3. Danh sách các văn bản điều hành, hướng dẫn của Bộ Thông tin và Truyền thông

- Chỉ thị số 04/CT-BTTTT ngày 11 tháng 01 năm 2019 của Bộ trưởng Bộ Thông tin và Truyền thông về tăng cường phòng chống mã độc và bảo vệ thông tin cá nhân trên môi trường mạng;

- Chỉ thị số 49/CT-BTTTT ngày 18 tháng 8 năm 2021 của Bộ trưởng Bộ Thông tin và Truyền thông về thúc đẩy phát triển và sử dụng nền tảng số an toàn, lành mạnh;

- Chỉ thị số 60/CT-BTTTT ngày 16 tháng 9 năm 2021 của Bộ trưởng Bộ Thông tin và Truyền thông về việc tổ chức triển khai diễn tập thực chiến bảo đảm an toàn thông tin mạng;

- Chỉ thị số 01/BTTTT-CT ngày 20 tháng 01 năm 2023 của Bộ trưởng Bộ Thông tin và Truyền thông về định hướng phát triển ngành Thông tin và Truyền thông năm 2023 và giai đoạn 2024 - 2025;

- Công văn số 430/BTTTT-CATTTT ngày 09/02/2015 của Bộ Thông tin và Truyền thông hướng dẫn bảo đảm an toàn thông tin cho hệ thống thư điện tử của cơ quan, tổ chức nhà nước.

- Công văn số 2290/BTTTT-CATTTT ngày 17 tháng 7 năm 2018 của Bộ Thông tin và Truyền thông về việc hướng dẫn kết nối, chia sẻ thông tin về mã độc giữa các hệ thống kỹ thuật;

- Công văn số 1694/BTTTT-CATTTT ngày 31 tháng 5 năm 2019 của Bộ Thông tin và Truyền thông về việc hướng dẫn yêu cầu an toàn thông tin cơ bản đối với hệ thống thông tin kết nối vào mạng Truyền số liệu chuyên dùng;

- Công văn số 3001/BTTTT-CATTTT ngày 06 tháng 9 năm 2019 của Bộ Thông tin và Truyền thông về việc hướng dẫn bảo đảm an toàn thông tin cho hệ thống quản lý văn bản và điều hành;

- Công văn số 2973/BTTTT-CATTTT ngày 04 tháng 9 năm 2019 của Bộ Thông tin và Truyền thông về việc hướng dẫn triển khai hoạt động giám sát an toàn thông tin trong cơ quan, tổ chức nhà nước;

- Công văn số 1145/BTTTT-CATTTT ngày 03 tháng 4 năm 2020 của Bộ Thông tin và Truyền thông về việc hướng dẫn bộ tiêu chí, chỉ tiêu kỹ thuật để đánh giá và lựa chọn giải pháp nền tảng điện toán đám mây phục vụ Chính phủ điện tử/Chính quyền điện tử;

- Công văn số 1552/BTTTT-CATTTT ngày 28 tháng 4 năm 2020 của Bộ Thông tin và Truyền thông về việc đôn đốc tổ chức triển khai bảo đảm an toàn thông tin cho hệ thống thông tin theo mô hình “4 lớp”;

- Công văn số 2612/BTTTT-CATTTT ngày 17 tháng 7 năm 2021 của Bộ Thông tin và Truyền thông về việc bổ sung bộ tiêu chí, chỉ tiêu để đánh giá và lựa chọn giải pháp nền tảng điện toán đám mây phục vụ Chính phủ điện tử/Chính quyền điện tử;

- Công văn số 4258/BTTTT-CATTTT ngày 26 tháng 10 năm 2021 của Bộ Thông tin và Truyền thông về việc hướng dẫn tổ chức, hoạt động của Đội ứng cứu sự cố an toàn thông tin mạng;

- Công văn số 964/BTTTT-CATTTT ngày 16 tháng 3 năm 2022 của Bộ Thông tin và Truyền thông về việc hướng dẫn áp dụng tiêu chuẩn an toàn thông tin cho các cơ quan nhà nước và hệ thống thông tin quan trọng quốc gia;

- Công văn số 1552/BTTTT-THH ngày 24 tháng 4 năm 2022 của Bộ Thông tin và Truyền thông về việc hướng dẫn triển khai Đề án 06 (phiên bản 1.0);

- Công văn số 708/BTTTT-CATTTT ngày 02 tháng 03 năm 2024 của Bộ

Thông tin và Truyền thông về sửa đổi, thay thế nội dung về an toàn, an ninh mạng tại Công văn số 1552/BTTTT-THH.

- Công văn số 1598/BTTTT-CATTT ngày 28 tháng 4 năm 2022 của Bộ Thông tin và Truyền thông về việc tăng cường bảo đảm an toàn thông tin theo cấp độ và nâng cao năng lực bảo đảm an toàn thông tin theo mô hình 4 lớp;

- Quyết định số 1439/QĐ-BTTTT 26/7/2022 của Bộ trưởng Bộ Thông tin và Truyền thông ban hành Ban hành quy trình hướng dẫn thực hiện diễn tập thực chiến.

4. Danh sách các văn bản hướng dẫn chuyên môn của Cục An toàn thông tin

- Công văn số 713/CATTT-TĐQLGS ngày 25 tháng 7 năm 2019 của Cục An toàn thông tin về việc hướng dẫn xác định và thực thi bảo vệ hệ thống thông tin theo cấp độ;

- Công văn số 235/CATTT-ATHTTT ngày 08 tháng 4 năm 2020 của Cục An toàn thông tin về việc Hướng dẫn mô hình đảm bảo an toàn thông tin cấp bộ, tỉnh.

- Công văn số 486/CATTT-ATHTTT ngày 19 tháng 6 năm 2020 của Cục An toàn thông tin về việc Hướng dẫn bảo đảm an toàn thông tin cho Trung tâm dữ liệu phục vụ Chính phủ điện tử;

- Công văn số 247/CATTT-ATHTTT ngày 26 tháng 3 năm 2021 của Cục An toàn thông tin về việc đơn đốc xác định cấp độ an toàn hệ thống thông tin và ban hành tài liệu hướng dẫn xác định cấp độ và xây dựng Hồ sơ đề xuất cấp độ 1, 2 và 3;

- Công văn số 793/CATTT-VNCERTCC ngày 25/6/2021 của Cục An toàn thông tin về việc hướng dẫn quy trình ứng cứu, xử lý sự cố tấn công mạng;

- Công văn số 166/CATTT-ATHTTT ngày 10 tháng 02 năm 2022 của Cục An toàn thông tin về việc ban hành hướng dẫn "Khung phát triển phần mềm an toàn (phiên bản 1.0)";

- Hướng dẫn số 01/HD-CATTT ngày 24 tháng 2 năm 2022 của Cục An toàn thông tin về việc hướng dẫn thực hiện hoạt động diễn tập thực chiến;

- Công văn số 5099/BTTTT-CATTT ngày 06/10/2023 của Bộ Thông tin và Truyền thông về việc Hướng dẫn phát triển Đội ứng cứu sự cố cho một số lĩnh vực quan trọng cần ưu tiên bảo đảm an toàn thông tin mạng./.