BỘ THÔNG TIN VÀ TRUYỀN THÔNG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM **Độc lập - Tự do - Hạnh phúc**
Số: 652 /BTTTT-CATTT V/v hướng dẫn triển khai một số nhiệm vụ trọng tâm về an toàn thông tin mạng trong năm 2023	*Hà Nội, ngày 28 tháng 02 năm 2023*

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

Triển khai 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 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. 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 (Sở Thông tin và Truyền thông các tỉnh, thành phố trực thuộc Trung ương; đơn vị được giao chuyên trách về an toàn thông tin tại các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ) tham mưu tập trung triển khai một số nhiệm vụ trọng tâm về an toàn thông tin mạng trong năm 2023 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 2023

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 2023 thuộc phạm vi quản lý như sau:

1. Triển khai Chiến lược An toàn, An ninh mạng quốc gia

Chiến lược An toàn, An ninh mạng quốc gia đã đề ra các mục tiêu cụ thể và đưa ra nhiệm vụ, giải pháp tổng thể, rõ ràng về an toàn, an ninh mạng đến năm 2025, tầm nhìn năm 2030. Các hoạt động về an toàn thông tin mạng quy mô quốc gia do các bộ, ngành, địa phương triển khai trong năm 2023 cũng như các năm tới đây cần tập trung trọng tâm để triển khai các nhiệm vụ, giải pháp này nhằm đạt được mục tiêu của Chiến lược. Trân trọng đề nghị Quý Cơ quan quan tâm chỉ đạo:

1.1. Mục tiêu

- Ban hành Kế hoạch triển khai Chiến lược.

- Hoàn thành 100% mục tiêu cụ thể, nhiệm vụ được phân kỳ thực hiện trong năm 2023.

1.2. Giải pháp

- Ban hành Kế hoạch triển khai Chiến lược (đối với các bộ, ngành, địa phương chưa ban hành Kế hoạch).

Kế hoạch triển khai Chiến lược cần xác định rõ mục tiêu cụ thể đến năm 2025 và mục tiêu cụ thể đến năm 2030, phù hợp với mục tiêu cụ thể của Chiến lược. Từ mục tiêu này, cần phân kỳ mục tiêu cụ thể từng năm (từng Quý trong năm nếu có thể) trong giai đoạn để triển khai thực hiện và thuận tiện trong việc giám sát, quản lý thực thi. Đối với các cơ quan có điều kiện, nguồn lực triển khai tốt, khuyến nghị đặt mục tiêu cao hơn mục tiêu của Chiến lược để bù đắp cho kết quả của các cơ quan có điều kiện, nguồn lực khó khăn. Đảm bảo hoàn thành mục tiêu tổng thể trên cả nước.

Nhằm quản lý thực thi Chiến lược (đối với lĩnh vực An toàn thông tin mạng), Bộ Thông tin và Truyền thông sẽ xây dựng và lấy ý kiến các cơ quan liên quan dự thảo Bộ tiêu chí đánh giá kết quả triển khai Chiến lược An toàn, An ninh mạng trước khi ban hành. Từ năm 2023, Bộ Thông tin và Truyền thông sẽ tổ chức đánh giá, xếp hạng và công bố kết quả triển khai thực thi Chiến lược hàng năm (đối với lĩnh vực An toàn thông tin mạng).

- Bố trí nguồn lực để tập trung triển khai các nhiệm vụ được giao tại Chiến lược theo Kế hoạch đã ban hành, đảm bảo đạt mục tiêu cụ thể đã đề ra.

1.3. Đầu mối hướng dẫn, hỗ trợ

Ông Nguyễn Văn Trưởng, chuyên viên, Cục An toàn thông tin, Bộ Thông tin và Truyền thông; số điện thoại: 0349729092; thư điện tử: nv_truong@mic.gov.vn.

2. 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.

Tại Chỉ thị số 02/CT-TTg ngày 26 tháng 4 năm 2022 về phát triển Chính phủ điện tử hướng tới Chính phủ số, thúc đẩy chuyển đổi số quốc gia, Thủ tướng Chính phủ đã yêu cầu các bộ, ngành, địa phương: hoàn thành phân loại, xác định và phê duyệt hồ sơ đề xuất cấp độ hệ thống thông tin trước tháng 12 năm 2022; triển khai đầy đủ phương án bảo đảm an toàn hệ thống thông tin theo cấp độ các hệ thống thông tin đang vận hành trước tháng 6 năm 2023. Tuy nhiên, đến nay, theo thống kê của Cục An toàn thông tin trên cả nước mới chỉ có 1.846 trong 3.078 hệ thống thông tin của cơ quan, tổ chức nhà nước được phê duyệt hồ sơ đề xuất cấp độ (đạt 60%). Tỷ lệ phê duyệt của các bộ, ngành đạt 51,6%. Tỷ lệ phê duyệt của các địa phương đạt 62,6%. 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 6,5%. 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 thuộc phạm vi quản lý được phê duyệt Hồ sơ đề xuất cấp độ.

- 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.

2.2. Giải pháp

- Tập trung rà soát, hoàn thành việc phân loại, xác định và phê duyệt đề xuất cấp độ an toàn đối với 100% hệ thống thông tin đang vận hành trước ngày 31/3/2023.

Để các cơ quan thuận tiện trong quá trình xây dựng, thẩm định và phê duyệt, Hồ sơ mẫu của Hồ sơ đề xuất cấp độ đã được Bộ Thông tin và Truyền thông (Cục An toàn thông tin) hướng dẫn, cung cấp cho Quý Cơ quan trước đây tại địa chỉ: https://ais.gov.vn/thong-tin-tham-khao/mau-hsdxcd.htm.

Bộ Thông tin và Truyền thông sẽ công bố Nền tảng hỗ trợ bảo đảm an toàn hệ thống thông tin theo cấp độ để các cơ quan có thể sử dụng, phục vụ hoạt động này tại các cơ quan.

- Triển khai đầy đủ phương án bảo đảm an toàn hệ thống thông tin theo cấp độ cho 100% hệ thống thông tin đang vận hành trước ngày 30/9/2023.

Căn cứ Hồ sơ đề xuất cấp độ và phương án bảo đảm an toàn hệ thống thông tin đã được phê duyệt, đề nghị tổ chức rà soát, đánh giá và triển khai đầy đủ phương án bảo đảm an toàn thông tin, bảo đảm tất cả yêu cầu quản lý, yêu cầu kỹ thuật đều được đáp ứng, đặc biệt là các yêu cầu chưa đáp ứng tại thời điểm phê duyệt Hồ sơ đề xuất cấp độ.

- Đối với các hệ thống thông tin đầu tư mới hoặc mở rộng, nâng cấp, khuyến nghị xây dựng và phê duyệt Hồ sơ đề xuất cấp độ trước khi phê duyệt Báo cáo nghiên cứu khả thi (hoặc hồ sơ tương đương) và triển khai đầy đủ phương án bảo đảm an toàn thông tin đã được phê duyệt tại Hồ sơ đề xuất cấp độ trước khi đưa vào vận hành, khai thác theo quy định tại khoản 6 điều 9 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 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ.

- Định kỳ trước 25 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) để tổng hợp, báo cáo Thủ tướng Chính phủ qua thư điện tử của đầu mối dưới đây. Sau khi Nền tảng hỗ trợ bảo đảm an toàn hệ thống thông tin theo cấp độ được khai trương đưa vào sử dụng, thông tin và số liệu sẽ được Bộ Thông tin và Truyền thông giám sát, truy xuất trực tiếp từ Nền tảng.

2.3. Đầu mối hướng dẫn, hỗ trợ

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

3. 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, theo đánh giá của Bộ Thông tin và Truyền thông, công tác bảo đảm an toàn thông tin theo mô hình "4 lớp" của các cơ quan vẫn ở mức cơ bản, chưa đáp ứng được đầy đủ yêu cầu để bảo đảm an toàn thông tin. Cụ thể: lực lượng tại chỗ còn thiếu về số lượng, chưa có nhiều kinh nghiệm thực tiễn; tỷ lệ hệ thống thông tin được thực hiện giám sát, bảo vệ chuyên nghiệp của cả nước mới đạt 28,7%; tỷ lệ hệ thống thông tin được kiểm tra, đánh giá định kỳ đúng theo

quy định của cả nước mới đạt 35,3%; hoạt động kết nối, chia sẻ dữ liệu giám sát với hệ thống giám sát quốc gia của một số cơ quan còn chưa đầy đủ, dữ liệu chia sẻ chưa nhiều, còn xảy ra hiện tượng mất kết nối (hiện chỉ có khoảng 28% cơ quan duy trì kết nối thường xuyên, ổn định). Bộ Thông tin và Truyền thông trân trọng đề nghị Quý Cơ quan quan tâm chỉ đạo:

3.1. Mục tiêu

Duy trì và nâng cao hiệu quả của mô hình bảo đảm an toàn thông tin "4 lớp", đặc biệt là 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.

3.2. Giải pháp

- Về lực lượng tại chỗ: tổ chức, kiện toàn lực lượng tại chỗ theo hướng chuyên nghiệp, cơ động, có tối thiểu 05 chuyên gia an toàn thông tin mạng (bao gồm cả chuyên gia thuê ngoài) thông qua hoạt động đào tạo, tuyển dụng hoặc thuê ngoài chuyên gia.

Tích cực khai thác, sử dụng Nền tảng điều phối xử lý sự cố an toàn thông tin mạng quốc gia do Cục An toàn thông tin triển khai tại địa chỉ irlab.vn trong công tác báo cáo sự cố, ứng cứu sự cố, huấn luyện, diễn tập để nâng cao năng lực cán bộ và được hỗ trợ khi xảy ra sự cố an toàn thông tin mạng.

- Về giám sát, bảo vệ chuyên nghiệp: hoàn thành mở rộng phạm vi giám sát, bảo vệ cho 100% hệ thống thông tin thuộc phạm vi quản lý trước ngày 30/11/2023. 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.

- Về kiểm tra, đánh giá: kiểm tra, đánh giá an toàn thông tin định kỳ theo quy định tại Điều 20 Nghị định số 85/2016/NĐ-CP cho tối thiểu 80% hệ thống thông tin thuộc phạm vi quản lý. 100% hệ thống thông tin cấp độ 3 trở lên được kiểm tra, đánh giá an toàn thông tin định kỳ theo quy định (hàng năm đối với hệ thống thông tin cấp độ 3 và cấp độ 4; 6 tháng đối với hệ thống thông tin cấp độ 5). 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.

- Về kết nối, chia sẻ thông tin với hệ thống giám sát quốc gia: 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.

3.3. Đầu mối hướng dẫn, hỗ trợ

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

4. Kiểm tra tuân thủ quy định của pháp luật về an toàn thông tin mạng

Thống kê theo báo cáo của các cơ quan, năm 2022 chỉ có khoảng 5% cơ quan tổ chức đoàn kiểm tra, đánh giá tuân thủ quy định của pháp luật về an toàn thông tin đối với các đơn vị, tổ chức, doanh nghiệp thuộc phạm vi quản lý. Điều này dẫn đến 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. Bộ Thông tin và Truyền thông trân trọng đề nghị Quý Cơ quan quan tâm chỉ đạo:

4.1. 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.

4.2. Giải pháp

Trong năm 2023, 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.

4.3. Đầu mối hướng dẫn, hỗ trợ

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

5. 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."*

Bộ trưởng Bộ Thông tin và Truyền thông đã ban hành Chỉ thị số 60/CT-BTTTT ngày 16 tháng 9 năm 2021 về việc tổ chức triển khai diễn tập thực chiến bảo đảm an toàn thông tin mạng, trong đó nêu rõ đơn vị chuyên trách về an toàn

thông tin: *"Tham mưu cho các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương về kế hoạch, bố trí kinh phí hàng năm để tổ chức ít nhất 01 cuộc diễn tập thực chiến chuyên đề an toàn thông tin, ứng cứu sự cố mạng trong phạm vi của bộ, ngành, địa phương".*

Năm 2022, Bộ Thông tin và Truyền thông đã tổ chức 03 cuộc diễn tập thực chiến quy mô quốc gia. Khoảng 50% bộ, ngành, địa phương đã tổ chức diễn tập thực chiến ở các quy mô khác nhau trong phạm vi quản lý. Kết quả và hiệu quả của các cuộc diễn tập thực chiến bước đầu cho chúng ta thấy sự đúng đắn và cần thiết của mô hình diễn tập này, đối với cả hệ thống thông tin lẫn năng lực của cán bộ an toàn thông tin. Diễn tập thực chiến không chỉ đánh giá khả năng ứng phó trước các cuộc tấn công mạng, tăng cường năng lực và kinh nghiệm của cán bộ làm về an toàn thông tin, cải tiến quy trình ứng cứu sự cố mà còn giúp phát hiện ra nhiều điểm yếu, lỗ hổng nghiêm trọng đang tồn tại trên hệ thống thông tin, có khả năng dẫn đến hậu quả khó lường nếu bị tấn công mạng. 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:

5.1. Mục tiêu

100% bộ, ngành, địa phương tổ chức diễn tập thực chiến trong năm 2023.

5.2. Giải pháp

- Mỗi bộ, ngành, địa phương tổ chức tối thiểu 01 cuộc diễn tập thực chiến an toàn thông tin mạng trong năm 2023. Trong đó, đảm bảo có tổ chức diễn tập thực chiến cho các hệ thống thông tin cấp độ 3 trở lên.

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 săn lùng mối 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 II/2023, Bộ Thông tin và Truyền thông sẽ công bố Nền tảng hỗ trợ điều tra số để các đơn vị chuyên trách về an toàn thông tin, Sở Thông tin và Truyền thông và các thành viên Mạng lưới Ứng cứu sự cố an toàn thông tin mạng quốc gia có thể sử dụng, nâng cao năng lực cho nhân lực và tăng hiệu quả công tác bảo đảm an toàn thông tin mạng, ứng cứu sự cố cũng như hoạt động huấn luyện, diễn tập thực chiến, săn lùng mối nguy hại.

5.3. Đầu mối hướng dẫn, hỗ trợ

Ông Lê Công Phú, Phó Giám đốc, Trung tâm Ứng cứu khẩn cấp không gina mạng Việt Nam (VNCERT/CC), Cục An toàn thông tin, Bộ Thông tin và

Truyền thông; số điện thoại: 0977717759; thư điện thử: phulc@mic.gov.vn.

6. Đẩy mạnh tuyên truyền nâng cao nhận thức và phổ biến kỹ năng

Đối với các cuộc tấn công mạng qua hình thức lây nhiễm mã độc, nhất là tấn công mạng có chủ đích, đối tượng tấn công thông thường sẽ tấn công người làm trong tổ chức để từ đó tấn công leo thang sang hệ thống thông tin của tổ chức. Vì vậy, để bảo đảm an toàn thông tin cho cơ quan, tổ chức nhà nước thì việc nâng cao nhận thức và trang bị kỹ năng an toàn thông tin cho cán bộ, công chức, viên chức và người lao động là rất quan trọng. Theo đánh giá, hơn 80% sự cố mất an toàn thông tin là do người sử dụng không có nhận thức và kỹ năng tự bảo vệ.

Đối với người dùng Internet, vấn đề gốc, cốt lõi nhất là làm sao để người dân có thể chủ động bảo vệ mình trên không gian mạng. Vì vậy, cần nâng cao nhận thức và trang bị kỹ năng an toàn thông tin cho đông đảo người dân. An toàn thông tin là lĩnh vực khó, chuyên sâu kỹ thuật. Để người sử dụng ý thức, quan tâm đến vấn đề này thì hoạt động tuyên truyền nâng cao nhận thức và phổ biến kỹ năng cần đáp ứng các tiêu chí: "Rộng", "Thường xuyên", "Dễ hiểu" và "Ấn tượng". Công tác này bước đầu đã được các cơ quan, tổ chức quan tâm nhưng chưa chú trọng thực hiện, chưa có giải pháp đáp ứng được các tiêu chí trên.

Cuối năm 2022, Bộ Thông tin và Truyền thông đã thành lập Liên minh Tuyên truyền nâng cao nhận thức, kỹ năng bảo đảm an toàn thông tin cho người dân trên không gian mạng. Liên minh sẽ xây dựng và chia sẻ miễn phí nội dung tuyên truyền và phổ biến kỹ năng dưới nhiều hình thức: video, tài liệu, poster, bài viết,… để tất cả các cơ quan, tổ chức, doanh nghiệp sử dụng phục vụ cho hoạt động tuyên truyền, phổ biến kỹ năng cho người sử dụng thuộc phạm vi quản lý của mình. Bộ Thông tin và Truyền thông trân trọng đề nghị Quý Cơ quan quan tâm chỉ đạo:

6.1. Mục tiêu

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.

6.2. Giải pháp

- Cơ quan, tổ chức liên hệ Cục An toàn thông tin để được cung cấp miễn phí nội dung (video, tài liệu, poster, bài viết,…) và tổ chức triển khai tuyên truyền nâng cao nhận thức, phổ biến kỹ năng cho cán bộ, công chức, viên chức, người lao động của cơ quan cũng như người dân trên địa bàn do cơ quan quản lý. 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,…

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.

- Đối với các địa phương, Bộ Thông tin và Truyền thông đề nghị tuyên truyền tối đa trên các hệ thống thông tin cơ sở (đài truyền thanh, đài truyền hình).

- 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, dự kiến diễn ra trong Quý II/2023.

6.3. Đầu mối hướng dẫn, hỗ trợ

Bà Phạm Phương Anh, chuyên viên, Cục An toàn thông tin, Bộ Thông tin và Truyền thông; số điện thoại: 0904755555; thư điện tử: ppanh@mic.gov.vn.

7. Bảo vệ thông tin, dữ liệu cá nhân

Thời gian qua, công tác bảo đảm an toàn dữ liệu, thông tin cá nhân vẫn chưa được các cơ quan, tổ chức thực sự quan tâm triển khai. Hiện tượng lộ lọt dữ liệu, thông tin cá nhân vẫn diễn ra với mức độ ngày càng phức tạp, nguy hiểm, ảnh hưởng không nhỏ đến quá trình kết nối, mở rộng, chia sẻ dữ liệu quốc gia, cũng như quá trình chuyển đổi số quốc gia.

Năm 2023 là Năm dữ liệu số quốc gia. Khi dữ liệu, thông tin cá nhân càng được tạo ra nhiều dẫn nguy cơ lộ lọt, mất an toàn thông tin ngày càng lớn, đặt ra vấn đề bảo vệ dữ liệu, thông tin cá nhân càng trở nên quan trọng.

7.1. Mục tiêu

Không để xảy ra lộ lọt thông tin, dữ liệu cá nhân nghiêm trọng trên các hệ thống thông tin thuộc phạm vi quản lý của cơ quan.

7.2. Giải pháp

- Chỉ đạo các đơn vị triển khai hoạt động thu thập, xử lý, sử dụng, lưu trữ thông tin cá nhân phải tuân thu quy định tại mục 2 Chương II Luật An toàn thông tin mạng và các văn bản hướng dẫn có liên quan.

- Phê duyệt Hồ sơ đề xuất cấp độ và triển khai đầy đủ phương án bảo đảm an toàn hệ thống thông tin theo cấp độ đối với các hệ thống thông tin có thu thập, xử lý, lưu trữ thông tin cá nhân. Đặc biệt là các hệ thống thông tin phục vụ chuyển đổi số, hệ thống thông tin dùng chung.

- Các phần mềm nội bộ do cơ quan, đơn vị xây dựng khuyến nghị áp dụng "Khung phát triển phần mềm an toàn (phiên bản 1.0)" theo hướng dẫn tại Công văn số 166/CATTT-ATHTTT ngày 10 tháng 02 năm 2022 của Cục An toàn thông tin.

- Hệ thống thông tin thử nghiệm có thu thập, xử lý, lưu trữ thông tin cá nhân cần phải được bảo đảm an toàn hệ thống thông tin như hệ thống thật đang vận hành.

- Tăng cường kiểm tra, đánh giá tuân thủ quy định của pháp luật về bảo vệ thông tin cá nhân theo mục 4 nêu trên, đặc biệt thực kiểm tra, đánh giá an toàn

thông tin mạng trước khi đưa vào sử dụng, khi nâng cấp, thay đổi, định kỳ theo quy định.

7.3. Đầu mối hướng dẫn, hỗ trợ

Ông Trần Nguyên Chung, Trưởng phòng, Cục An toàn thông tin, Bộ Thông tin và Truyền thông; số điện thoại: 0888609399; thư điện tử: tnchung@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 Trưởng, chuyên viên, 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 Nguyễn Huy Dũng (để b/c);
- Đơn vị chuyên trách CNTT/ATTT của các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ;
- Sở TT&TT các tỉnh, thành phố trực thuộc TƯ;
- Sở Văn hóa, Thông tin, Thể thao và Du lịch tỉnh Bạc Liêu;
- Lưu: VT, CATTT.QHPT.

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

Nguyễn Huy Dũng

Phụ lục

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

(Ban hành kèm theo Công văn số /BTTTT-CATTT ngày / /2023 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 Chỉnh 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.

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-CATTT ngày 17 tháng 7 năm 2018 của Bộ Thông tin và 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-CATTT ngày 31 tháng 5 năm 2019 của Bộ Thông tin và 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-CATTT 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-CATTT 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-CATTT 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-CATTT 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-CATTT 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-CATTT 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-CATTT 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 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 đôn 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.