BỘ THÔNG TIN VÀ TRUYỀN THÔNG
CỤC AN TOÀN THÔNG TIN

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Số: 476 /CATTT-ATHTTT
V/v Tăng cường bảo đảm an toàn thông tin mạng đối với hệ thống thông tin

Hà Nội, ngày tháng năm 2024

Kính gửi:

- Đơn vị chuyên trách về công nghệ thông tin/an toàn thông tin của 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;
- Các Tập đoàn, Tổng công ty nhà nước;
- Các Tổ chức tài chính, Ngân hàng thương mại nhà nước;
- Các Ngân hàng: Chính sách xã hội; Phát triển Việt Nam; Hợp tác xã Việt Nam;
- Các Tổ chức, doanh nghiệp hoạt động trong lĩnh vực bưu chính;
- Các Tổ chức, doanh nghiệp hoạt động trong lĩnh vực thương mại điện tử.

Căn cứ Luật An toàn thông tin mạng;

Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Quyết định số 05/2017/QĐ-TTg ngày 16/03/2017 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;

Thực hiện Chỉ thị số 09/CT-TTg ngày 23/02/2024 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.

Qua theo dõi, giám sát không gian mạng, Cục An toàn thông tin (Bộ Thông tin và Truyền thông) phát hiện xu hướng tấn công mạng, đặc biệt là mã hóa tấn công tống tiền (ransomware) tăng cao. Trong thời gian gần đây, đã có một số hệ thống thông tin của cơ quan, tổ chức, doanh nghiệp tại Việt Nam bị sự cố tấn công, gây gián đoạn hoạt động và thiệt hại về vật chất, hình ảnh của các cơ quan, tổ chức, doanh nghiệp, cũng như hoạt động bảo đảm an toàn không gian mạng quốc gia.

Thực hiện chức năng quản lý nhà nước về an toàn thông tin mạng, Cục An toàn thông tin đề nghị các cơ quan, tổ chức, doanh nghiệp rà soát và triển khai

bảo đảm an toàn thông tin mạng cho các hệ thống thông tin thuộc phạm vi quản lý, với các nhiệm vụ chính như sau:

1. Tổ chức rà soát, tăng cường các giải pháp bảo đảm an toàn thông tin mạng cho các hệ thống thông tin, ưu tiên các giải pháp giám sát, cảnh báo sớm; Thực hiện kiểm tra, đánh giá đảm bảo an toàn thông tin các hệ thống thông tin thuộc phạm vi quản lý, trong trường hợp phát hiện các nguy cơ, lỗ hổng, điểm yếu, cần lập tức triển khai các biện pháp khắc phục, đặc biệt là các hệ thống thông tin lưu trữ, xử lý thông tin cá nhân, dữ liệu cá nhân. Hoàn thành trước ngày 15/4/2024.

2. Rà soát, tổ chức triển khai bảo đảm an toàn thông tin theo cấp độ[i].

Tổ chức triển khai các nhiệm vụ liên quan theo Chỉ thị số 09/CT-TTg ngày 23/02/2024 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, đặc biệt là tổ chức thống kê, phân loại các hệ thống thông tin thuộc phạm vi quản lý; xây dựng kế hoạch triển khai hoàn thành quy định bảo đảm an toàn hệ thống thông tin theo cấp độ (theo tiến độ tháng), bảo đảm 100% hệ thống thông tin đang vận hành phải được phê duyệt 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 chậm nhất trong tháng 12 năm 2024 theo.

3. Tổ chức thực thi hiệu quả, thực chất, thường xuyên, liên tục công tác bảo đảm an toàn thông tin theo mô hình 4 lớp, đặc biệt là nâng cao năng lực của lớp giám sát, bảo vệ chuyên nghiệp và duy trì liên tục, ổn định kết nối, chia sẻ thông tin với Trung tâm Giám sát an toàn không gian mạng quốc gia trực thuộc Cục An toàn thông tin, Bộ Thông tin và Truyền thông; ưu tiên sử dụng các sản phẩm, giải pháp, dịch vụ an toàn thông tin mạng do doanh nghiệp Việt Nam sản xuất hoặc làm chủ công nghệ.

4. Xây dựng kế hoạch ứng phó sự cố đối với hệ thống thông tin thuộc phạm vi quản lý theo quy định tại Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc. Triển khai phương án sao lưu định kỳ hệ thống và dữ liệu quan trọng để kịp thời khôi phục khi bị tấn công mã hóa dữ liệu và báo cáo sự cố về Cục An toàn thông tin theo quy định. Tham gia mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia theo quy định tại Điều 7 Quyết định số 05/2017/QĐ-TTg ngày 16/03/2017 của Thủ tướng Chính phủ.

5. Rà soát, triển khai các nhiệm vụ liên quan theo Chỉ thị số 18/CT-TTg ngày 13/10/2022 của Thủ tướng Chính phủ về đẩy mạnh triển khai các hoạt động ứng cứu sự cố an toàn thông tin mạng Việt Nam. Thực hiện định kỳ săn lùng mối nguy hại để phát hiện kịp thời các dấu hiệu hệ thống bị xâm nhập. Đối với hệ thống đã phát hiện lỗ hổng bảo mật nghiêm trọng, sau khi khắc phục lỗ hổng, cần thực hiện ngay việc săn lùng mối nguy hại nhằm xác định khả năng bị xâm nhập trước đó.

6. Kiểm tra, cập nhật các bản vá an toàn thông tin cho các hệ thống quan trọng theo cảnh báo của Cục An toàn thông tin và các cơ quan, tổ chức liên quan;

định kỳ kiểm tra, đánh giá, rà soát để phát hiện kịp thời các lỗ hổng an toàn thông tin, các điểm yếu đang tồn tại trên hệ thống.

7. Thường xuyên, liên tục sử dụng các Nền tảng về an toàn thông tin do Cục An toàn thông tin (Bộ Thông tin và Truyền thông) phát triển, cung cấp để hỗ trợ các cơ quan, tổ chức, doanh nghiệp: Sử dụng Nền tảng Điều phối xử lý sự cố an toàn thông tin mạng quốc gia (IRLab) để được hướng dẫn, nhận các cảnh báo sớm và hỗ trợ xử lý sớm nguy cơ, sự cố; Sử dụng Nền tảng Hỗ trợ điều tra số (DFLab) trong trường hợp phù hợp để tổ chức ứng cứu sự cố và được sự hỗ trợ từ cơ quan nhà nước, các chuyên gia đầu ngành về an toàn thông tin.

Đề nghị các tổ chức, doanh nghiệp rà soát, cử đầu mối trao đổi chuyên môn và báo cáo kết quả thực hiện về Cục An toàn thông tin **trước ngày 20/4/2024** để tổng hợp và báo cáo cấp có thẩm quyền.

Trong quá trình thực hiện, nếu có khó khăn vướng mắc hoặc trường hợp cần hỗ trợ giám sát, xử lý, ứng cứu sự cố đề nghị liên hệ với Cục An toàn thông tin, Bộ Thông tin và Truyền thông thông qua các đầu mối:

- Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT/CC), điện thoại 024.3640.4421 hoặc số điện thoại trực đường dây nóng ứng cứu sự cố 086.9100.317, thư điện tử: ir@vncert.vn;

- Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), điện thoại: 024.32091.616 hoặc số điện thoại trực đường dây nóng hỗ trợ giám sát, cảnh báo sớm 038.9942.878, thư điện tử: ais@mic.gov.vn.

- Phòng An toàn hệ thống thông tin, Cục An toàn thông tin (hướng dẫn công tác bảo đảm an toàn hệ thống thông tin theo cấp độ), điện thoại: 0369596886, thư điện tử: athttt@mic.gov.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- Bộ trưởng (để b/c);
- Thứ trưởng Phạm Đức Long (để b/c);
- Cục trưởng (để b/c);
- Các Phó Cục trưởng;
- Lưu: VT, ATHTTT.PQM, PTA.

KT. CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG

CỘNG HÒA X.H.C.N VIỆT NAM
CỤC AN TOÀN THÔNG TIN
BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Trần Đăng Khoa

---

[i] Lưu ý: *Căn cứ quy định tại Phụ lục IV Luật đầu tư năm 2020 và điểm b khoản 2 Điều 9 Nghị định 85/2016/NĐ-CP, các hệ thống thông tin cung cấp dịch vụ trực tuyến thuộc danh mục kinh doanh có điều kiện cần triển khai bảo đảm an toàn hệ thống thông tin theo cấp độ quy định tại Nghị định số 85/2016/NĐ-CP*

ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ và Thông tư 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ trưởng Bộ Thông tin và Truyền thông. Việc không triển khai bảo đảm an toàn hệ thống thông tin theo cấp độ là vi phạm quy định pháp luật và bị xử phạt hành chính theo Điều 88 và Điều 89 Nghị định số 15/2020/NĐ-CP ngày 03/02/2020 của Chính phủ quy định xử phạt vi phạm hành chính trong lĩnh vực bưu chính, viễn thông, tần số vô tuyến điện, công nghệ thông tin và giao dịch điện tử.