ỦY BAN NHÂN DÂN
THÀNH PHỐ HỒ CHÍ MINH
TIỂU BAN AN TOÀN, AN NINH MẠNG

Số: 2748 /UBND-TBATANM

V/v tăng cường công tác bảo đảm an toàn thông tin mạng trong thời gian diễn ra đại lễ kỷ niệm 50 năm Ngày giải phóng miền Nam, thống nhất đất nước

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

TP. Hồ Chí Minh, ngày 21 tháng 4 năm 2025

Kính gửi:
- Các sở, ban, ngành Thành phố;
- Ủy ban nhân dân các quận, huyện và thành phố Thủ Đức;
- Các Tổng công ty, Công ty trực thuộc Ủy ban nhân dân Thành phố.

Từ đầu năm 2024 đến nay, tình trạng các hệ thống thông tin của các cơ quan Đảng, Nhà nước trên cả nước bị tấn công, chiếm quyền điều khiển diễn biến hết sức phức tạp; trong đó, lực lượng An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao Bộ Công an đã ghi nhận một số hoạt động tấn công có chủ đích vào các hệ thống thông tin của các cơ quan Đảng, Nhà nước nhằm thu thập, đánh cắp thông tin, dữ liệu. Đặc điểm của các cuộc tấn công có chủ đích này tập trung nhắm vào các mạng công nghệ thông tin (CNTT) có nhiều dữ liệu mật, dữ liệu quan trọng; sử dụng mã độc tấn công được thiết kế riêng với đặc thù từng mạng CNTT mà các chương trình phòng, chống mã độc khó phát hiện; phần lớn không xác định được thời gian thực hiện chiến dịch tấn công mạng, có những mạng CNTT khi điều tra, phân tích, đã phát hiện mã độc nằm vùng trước đó *(từ vài tháng đến vài năm)* gây khó khăn trong việc đánh giá được các dữ liệu đã bị thất thoát.

Trên địa bàn Thành phố từ đầu năm 2024 đến nay, Tiểu ban An toàn, An ninh mạng Thành phố đã ghi nhận **07** vụ việc tấn công mạng vào hệ thống thông tin của các cơ quan, đơn vị trực thuộc Thành ủy, Ủy ban nhân dân Thành phố và **15** vụ việc lộ tài liệu bí mật nhà nước trên không gian mạng; trong đó một số vụ việc có phương thức tấn công mạng phổ biến như: tấn công xâm nhập hệ thống (04 vụ), tấn công mã hóa dữ liệu (03 vụ). Hầu hết các vụ việc có nguồn gốc tấn công từ nước ngoài, chưa xác định được chủ thể thực hiện hành vi cũng như động cơ, mục đích tấn công mạng; không loại trừ khả năng các vụ việc hệ thống

thông tin của các cơ quan, đơn vị trực thuộc Thành ủy, Hội đồng nhân dân Thành phố, Ủy ban nhân dân Thành phố bị tấn công mạng có liên quan đến các cá nhân, tổ chức phản động nhằm chiếm đoạt bí mật nhà nước, phá hoại hệ thống, làm gián đoạn công tác của cơ quan, đơn vị.

Để bảo đảm an toàn đối với các hệ thống thông tin của Thành phố, phòng ngừa các sự cố an toàn thông tin mạng, các hoạt động tấn công mạng của cá nhân, tổ chức phản động nhắm đến phá hoại công tác chuẩn bị, tổ chức các chương trình, hoạt động chào mừng đại lễ kỷ niệm 50 năm Ngày giải phóng miền Nam, thống nhất đất nước (30/4/1975-30/4/2025) *(Lễ kỷ niệm)*; xét đề nghị của Công an Thành phố - Cơ quan Thường trực Tiểu ban An toàn, An ninh mạng Thành phố tại Tờ trình số 2074/TTr-CATP-PA05 ngày 11 tháng 4 năm 2025, Tiểu ban An toàn, An ninh mạng Thành phố đề nghị các cơ quan, đơn vị tập trung triển khai thực hiện một số công tác sau:

1. Quán triệt đến toàn thể cán bộ, đảng viên, công chức, viên chức, người lao động thực hiện nghiêm túc các quy định về công tác bảo đảm an ninh mạng, bảo vệ bí mật nhà nước, bảo vệ dữ liệu cá nhân như: Luật An ninh mạng, Luật Bảo vệ bí mật nhà nước, Nghị định quy định về bảo vệ dữ liệu cá nhân và các văn bản hướng dẫn thi hành; Chỉ thị số 01/CT-TTg ngày 18 tháng 02 năm 2021 của Thủ tướng Chính phủ về tăng cường công tác bảo vệ an ninh mạng trong tình hình hiện nay… Xây dựng và hoàn thiện quy định quản lý, sử dụng và bảo đảm an ninh mạng máy tính nội bộ, mạng máy tính có kết nối Internet, trong đó nghiêm cấm thực hiện các nội dung sau:

- Không sử dụng máy tính kết nối Internet để soạn thảo, lưu trữ tài liệu nội bộ, tài liệu có nội dung bí mật nhà nước;

- Không sử dụng chung thiết bị lưu trữ ngoại vi (USB, ổ cứng di động...) giữa máy tính kết nối Internet và máy tính nội bộ lưu trữ, soạn thảo tài liệu bí mật nhà nước;

- Không cài đặt các phần mềm, ứng dụng không có bản quyền, phần mềm bẻ khóa trên máy tính của cơ quan, đơn vị;

- Không sử dụng tài khoản hộp thư điện tử công vụ, phần mềm quản lý văn bản và hồ sơ công việc, các ứng dụng mạng xã hội (Zalo, Viber, Telegram...) trên môi trường mạng Internet để gửi/nhận văn bản, tài liệu nội bộ, tài liệu bí mật nhà nước;

- Ban hành và tuân thủ quy trình quản lý, cấp phát, thu hồi, sử dụng tài khoản công vụ, tài khoản truy cập hệ thống thông tin phục vụ hành chính công, Dịch vụ công, một cửa;

- Xây dựng và ban hành phương án đảm bảo an ninh mạng, ứng phó, khắc phục sự cố an ninh mạng các hệ thống thông tin thuộc phạm vi quản lý theo quy định.

2. Tổ chức rà soát, khắc phục sơ hở, thiếu sót trong công tác quản lý, quản trị, vận hành hệ thống mạng máy tính tại cơ quan, đơn vị; định kỳ, đột xuất kiểm tra máy tính, triển khai công tác giám sát an toàn thông tin mạng, kiểm soát truy cập mạng đối với các hệ thống thông tin thuộc phạm vi quản lý; rà soát, gỡ bỏ phần mềm độc hại và cập nhật đầy đủ các bản vá lỗ hổng bảo mật cho toàn bộ máy chủ, máy trạm trong hệ thống thông tin; phân công nhân sự theo dõi thường xuyên, liên tục để đảm bảo phát hiện sớm các nguy cơ tấn công mạng *(đặc biệt là tấn công mã hóa dữ liệu, thay đổi giao diện)* để kịp thời xử lý, khắc phục nhanh sự cố tấn công mạng.

3. Quan tâm đầu tư cơ sở vật chất, trang thiết bị, giải pháp kỹ thuật nhằm bảo đảm an ninh mạng, an toàn thông tin các hệ thống thông tin. Rà soát, đánh giá lại toàn bộ hệ thống thông tin tại cơ quan, đơn vị, thay thế các mô hình mạng, giải pháp đảm bảo an ninh mạng đã lỗi thời bằng các biện pháp, thiết bị mới. Rà soát, trang bị thêm các giải pháp phòng, chống mã độc, quản lý thiết bị đầu cuối tập trung; hệ thống tự động quản lý, cập nhật bản vá lỗ hổng bảo mật; hệ thống giám sát, phát hiện, cảnh báo hoạt động tấn công mạng (SEIM/SOC); không mua sắm mới thiết bị đã bị cảnh báo tồn tại lỗ hổng bảo mật, có nguy cơ mất an ninh mạng, an toàn thông tin.

4. Chú trọng các hoạt động tuyên truyền, đào tạo, tập huấn, nâng cao nhận thức cho lãnh đạo, cán bộ, công chức, viên chức về đảm bảo an toàn thông tin, an ninh mạng, bảo vệ bí mật nhà nước, bảo vệ dữ liệu cá nhân; Tập huấn chuyên sâu về an ninh mạng cho bộ phận chuyên trách về công nghệ thông tin, quản trị hệ thống; Nhận biết, cảnh giác trước thông tin xấu độc, tin giả, thông tin xuyên tạc, chống phá, chính sách của Đảng, Nhà nước; Phòng, chống lừa đảo trên không gian mạng, cho toàn thể cán bộ, công chức, viên chức, người lao động của cơ quan và người dân trên địa bàn.

5. Giao Sở Văn hóa và Thể thao, Sở Khoa học và Công nghệ theo chức năng, nhiệm vụ, lĩnh vực phụ trách chủ trì, phối hợp với Công an Thành phố thực hiện các nội dung sau:

- Rà soát các phương tiện có kết nối mạng, các bảng điện tử, màn hình led tại nơi tổ chức sự kiện và các địa điểm liên quan khác có trình chiếu thông tin, hình ảnh về sự kiện để kiểm tra, hướng dẫn và có biện pháp chống xâm nhập, phá hoại;

- Tăng cường triển khai các biện pháp, giải pháp nhằm nâng cao hiệu lực quản lý nhà nước về an toàn thông tin; yêu cầu các doanh nghiệp cung cấp dịch vụ thông tin viễn thông, Internet ngăn chặn, gỡ bỏ các thông tin xấu, độc, chống phá gây tác động xấu đến tình hình an ninh chính trị, trật tự an toàn xã hội, ảnh hưởng đến hoạt động đối ngoại của Đảng, Nhà nước và các hoạt động của Lễ kỷ niệm trên địa bàn Thành phố.

Quá trình thực hiện, nếu gặp khó khăn, vướng mắc hoặc phát hiện có sự cố an ninh mạng, nhất là trong thời gian diễn ra đại lễ kỷ niệm 50 năm Ngày giải phóng miền Nam, thống nhất đất nước, đề nghị các đơn vị trao đổi nhanh về Công an Thành phố *(Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Đ/c Đại tá Nguyễn Hồng Doanh - Trưởng phòng, SĐT: 090.977.3838*) để được hỗ trợ, phối hợp xử lý./.

Nơi nhận:
- Như trên;
- Thường trực Thành ủy;
- Thường trực HĐND Thành phố;
- TTUB: CT, PCT/NC;
- Văn phòng Thành ủy;
- Văn phòng Đảng ủy;
- Công an Thành phố;
- VPUB: CVP, PCVP/NC;
- Phòng NCPC;
- Lưu: VT (NCPC/NH). 4

KT. TRƯỞNG TIỂU BAN
PHÓ TRƯỞNG TIỂU BAN

PHÓ CHỦ TỊCH ỦY BAN NHÂN DÂN
THÀNH PHỐ HỒ CHÍ MINH
Dương Ngọc Hải