UBND TỈNH BÌNH ĐỊNH
SỞ NGOẠI VỤ

Số: 676/KH-SNgV

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

Bình Định, ngày 10 tháng 6 năm 2024

KẾ HOẠCH
Xây dựng phương án ứng cứu, xử lý sự cố tấn công mạng

Triển khai thực hiện Quyết định số 107/QĐ-STTTT ngày 05/6/2024 của Sở Thông tin và Truyền thông phê duyệt cấp độ an toàn Hệ thống thông tin đối với hệ thống thông tin của Sở Ngoại vụ (cấp độ 2); theo đó, Sở Ngoại vụ xây dựng phương án ứng cứu, xử lý sự cố tấn công mạng, với các nội dung cụ thể như sau:

I. MỤC TIÊU, NGUYÊN TẮC ĐẢM BẢO AN TOÀN THÔNG TIN

1. Mục tiêu, nguyên tắc bảo đảm an toàn thông tin

***1.1. Mục tiêu*:** Đảm bảo an toàn thông tin là làm cho hệ thống hoạt động thông suốt và không bị tấn công bởi virus và hacker làm mất dữ liệu cũng như gián đoạn quá trình hoạt động của hệ thống.

1.2. Nguyên tắc:

- Cài đặt và cập nhật các phần mềm diệt virus cho máy chủ và các máy con.

- Định kỳ kiểm tra thông tin truy cập của hệ thống, kiểm soát băng thông đường truyền.

- Rà soát và thay đổi các tài khoản, các ứng dụng.

- Hạn chế truy cập vào các website không rõ nguồn gốc.

- Trang bị cho các máy tính để bàn, máy tính xách tay và máy chủ phần mềm diệt virus.

- Tăng cường trao đổi thông tin qua hệ thống hộp thư điện tử công vụ và văn phòng điện tử (hạn chế sử dụng USB, thẻ nhớ, các thiết bị gắn trực tiếp vào máy tính).

II. NỘI DUNG XÂY DỰNG PHƯƠNG ÁN AN TOÀN THÔNG TIN

1. Nội dung, trách nhiệm bảo đảm an toàn thông tin

- Các cán bộ làm về an toàn thông tin, người sử dụng đầu cuối, các đối tượng thuộc phạm vi điều chỉnh của chính sách an toàn thông tin.

- Người đứng đầu cơ quan chỉ đạo thực hiện việc kiểm tra về vấn đề an toàn thông tin.

- Cán bộ chuyên trách công nghệ thông tin thường xuyên kiểm tra mức độ an toàn của hệ thống.

- Người sử dụng các dịch vụ do máy chủ cung cấp có trách nhiệm bảo mật thông tin của mình.

2. Phạm vi chính sách an toàn thông tin

Các văn bản, chính sách quản lý hệ thống thông tin trong phạm vi cơ quan

- Quyết định số 16/QĐ-SNgV ngày 05/9/2013 về Quy chế hoạt động Trang thông tin điện tử của Sở Ngoại vụ tỉnh Bình Định;

- Quy chế hoạt động của Ban Biên tập Website Sở Ngoại vụ tỉnh Bình Định; - Quyết định số 29/QĐ-SNgV ngày 09/12/2013 về Quy chế hoạt động của Ban Biên tập Website Sở Ngoại vụ tỉnh Bình Định;

- Quyết định số 1368/QĐ-SNgV ngày 04/12/2023 của Sở Ngoại vụ Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng CNTT theo Quy định hướng dẫn tại Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 Quy định chi tiết và hướng dẫn một số điều của 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;

- Quyết định số 817/QĐ-SNgV ngày 24/10/2014 về Quy chế quản lý, sử dụng thư điện tử công vụ trong hoạt động của Sở Ngoại vụ tỉnh Bình Định;

- Quyết định số 1048/QĐ-SNgV ngày 22/11/2016 về Quy chế quản lý, sử dụng Phần mềm chuyển, nhận văn bản hành chính giữa Bộ Ngoại giao và Sở Ngoại vụ tỉnh Bình Định;

- Quyết định số 1279/QĐ-SNgV ngày 28/12/2018 về Quy chế quản lý và sử dụng Văn phòng điện tử liên thông của Sở Ngoại vụ tỉnh Bình Định.

3. Tổ chức bảo đảm an toàn thông tin

- Thường xuyên kiểm tra mức độ an toàn thông tin.

- Cập nhật các phần mềm diệt virus.

- Kiểm tra và cập nhật các bản vá lỗi để sửa chữa các lỗ hổng bảo mật.

4. Bảo đảm nguồn nhân lực

Nguồn nhân lực đảm bảo an toàn thông tin phải được thường xuyên tập huấn và đào tạo kiến thức an toàn thông tin.

5. Quản lý vận hành hệ thống

- Việc quản lý vận hành hệ thống như: Quản lý an toàn máy chủ, an toàn ứng dụng, an toàn dữ liệu, an toàn mạng, sự cố an toàn thông tin, an toàn người sử dụng đầu cuối của các hệ thống thông tin thành phần tại Sở đều được kiểm tra đảm bảo các hệ thống thông tin hoạt động ổn định 24/24, có đầy đủ các thiết bị bảo mật, an toàn và lưu trữ dữ liệu thường xuyên.

- Các quy định như xây dựng kế hoạch, chính sách, quy trình thực hiện quản lý an toàn hạ tầng mạng được đơn vị cho thuê dịch vụ thực hiện.

- Hệ thống mạng nội bộ- LAN của cơ quan luôn được theo dõi, quản lý đảm bảo hoạt động thông suốt, các máy tính được trang bị phần mềm diệt virus.

6. Yêu cầu kỹ thuật

6.1. Bảo đảm an toàn mạng **(**cấp độ 2 trở lên**)**

- Thường xuyên phối hợp với đơn vị cho thuê dịch vụ để vận hành hệ thống ổn định;

- Công chức phụ trách công nghệ thông tin tại cơ quan phải thường xuyên nghiên cứu, cập nhật các kiến thức về an toàn, an ninh thông tin, nguy cơ tiềm ẩn có thể gây mất thông tin và các biện pháp phòng tránh khi tiến hành các hoạt động quản lý hay kỹ thuật nghiệp vụ;

- Thường xuyên thực hiện việc theo dõi bảng ghi nhật ký hệ thống (logfile) và các sự kiện khác có liên quan để đánh giá, báo cáo các rủi ro và mức độ nghiêm trọng các rủi ro đó. Các rủi ro đó có thể xảy ra do sự truy cập trái phép, sử dụng trái phép, mất, thay đổi hoặc phá hủy thông tin và hệ thống thông tin;

- Khi thiết lập các dịch vụ trên môi trường mạng Internet, chỉ cung cấp những chức năng thiết yếu bảo đảm duy trì hoạt động của hệ thống thông tin; hạn chế sử dụng chức năng, cổng giao tiếp mạng, giao thức và các dịch vụ không cần thiết.

6.2. Bảo đảm an toàn ứng dụng

- Thực hiện cấp phát, thu hồi, cập nhật và quản lý tất cả các tài khoản truy cập vào hệ thống thông tin của sở; hướng dẫn người dùng thay đổi mật khẩu cá nhân theo quy định.

- Nghiêm chỉnh chấp hành các quy định nội bộ về an toàn thông tin của cơ quan, đơn vị và các quy định khác của pháp luật.

- Thường xuyên cài đặt và cập nhật các phần mềm diệt virus,.. cho tất cả các máy tính cá nhân, máy tính xách tay.

- Phối hợp với Sở Thông tin và Truyền thông kiểm tra và cập nhật các bản vá lỗi và để sửa chữa các lỗ hổng bảo mật.

- Thiết lập chính sách lưu dự phòng dữ liệu định kỳ.

7. Bảo đảm an toàn dữ liệu

- Hệ thống mạng nội bộ của Sở được thiết kế, xây dựng theo mô hình nhóm (Group) cho từng phòng và cấp địa chỉ mạng cố định cho từng cá nhân, cho từng máy tính của cơ quan và giao các đơn vị, phòng chuyên môn quản lý, theo dõi nhằm mục đích quản lý hệ thống chặt chẽ, an toàn và bảo mật.

- Định kỳ lưu trữ dữ liệu vào các thiết bị lưu trữ như Qnap, các server.

8. Thời gian, địa điểm

- Thời gian tổ chức: Quý III năm 2024.

- Địa điểm: Sở Ngoại vụ.

III. KINH PHÍ TỔ CHỨC

Từ nguồn kinh phí được phân bổ cho Sở Ngoại vụ theo Quyết định số 4568/QĐ-UBND ngày 10/12/2024 của UBND tỉnh về việc giao dự toán ngân sách nhà nước năm 2024.

IV. TỔ CHỨC THỰC HIỆN

1. Văn phòng Sở chuẩn bị các nội dung có liên quan để có phương án ứng cứu, xử lý sự cố tấn công mạng theo định kỳ.

2. Các Phòng thuộc Sở chủ động, phối hợp với Văn phòng Sở triển khai thực hiện các nội dung liên quan theo Kế hoạch này.

Trên đây là Kế hoạch xây dựng phương án ứng cứu, xử lý sự cố tấn công mạng của Sở Ngoại vụ năm 2024, đề nghị các Phòng thuộc Sở và các đơn vị có liên quan triển khai thực hiện./.

GIÁM ĐỐC

Nguyễn Thái Bình

Nơi nhận:
- Lãnh đạo Sở;
- Các Phòng thuộc Sở;
- Lưu: VT,VP.