

Số: 77 /KH-SYT

Bắc Giang, ngày 11 tháng 7 năm 2018

KẾ HOẠCH
Nâng cao năng lực phòng, chống phần mềm độc hại
của Sở Y tế năm 2018

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

Căn cứ Công văn số 1929/UBND-KT ngày 15/6/2018 của UBND tỉnh Bắc Giang về nâng cao năng lực phòng, chống phần mềm độc hại;

Sở Y tế xây dựng Kế hoạch nâng cao năng lực phòng, chống phần mềm độc hại của Sở Y tế năm 2018 như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích

Nâng cao năng lực phòng, chống phần mềm độc hại, đảm bảo an toàn, an ninh hệ thống công nghệ thông tin của Sở, chủ động phòng ngừa và xử lý kịp thời các sự cố.

Đảm bảo an toàn thông tin cho hệ thống công nghệ thông tin, trang thông tin điện tử, các phần mềm chuyên ngành thuộc thẩm quyền quản lý của Sở, giảm thiểu các nguy cơ đe dọa mất an toàn thông tin trên mạng; đề ra các giải pháp khi gặp sự cố an toàn thông tin mạng.

Tạo chuyển biến trong nhận thức về an toàn thông tin đối với cán bộ, công chức trong cơ quan.

2. Yêu cầu

Thường xuyên đánh giá các nguy cơ, sự cố an toàn thông tin của toàn hệ thống công nghệ thông tin của Sở Y tế để đưa ra phương án xử lý, kịp thời, phù hợp.

II. NHIỆM VỤ

1. Tổ chức tuyên truyền, phổ biến nâng cao nhận thức và kỹ năng xử lý các mối nguy hại của mã độc cho cán bộ, công chức trong cơ quan thông qua các cuộc họp giao ban hoặc thường xuyên tuyên truyền, nhắc nhở bằng văn bản, Email như: không mở những Email có nội dung đáng ngờ, không truy cập vào

những trang web không có chứng chỉ bảo mật, kém an toàn, không dùng phần mềm crack và những phần mềm không rõ nguồn gốc, phần mềm miễn phí...

Thời gian thực hiện: Cả năm.

Đơn vị thực hiện: Văn phòng Sở chủ trì phối hợp với các phòng thuộc Sở.

2. 100% văn bản phát hành trên môi trường mạng sử dụng chữ ký số để gửi, nhận văn bản giữa Sở Y tế với các cơ quan hành chính nhà nước ở địa phương và UBND tỉnh. Từng bước sử dụng chữ ký số của lãnh đạo để ký văn bản điện tử.

Thời gian thực hiện: Cả năm.

Đơn vị chủ trì: Văn phòng Sở chủ trì phối hợp với các phòng thuộc Sở.

3. Thường xuyên thực hiện rà quét mã độc cho hệ thống công nghệ thông tin, trang thông tin điện tử, các phần mềm ứng dụng chuyên ngành: Giám sát, phát hiện sớm nguy cơ sự cố; kiểm tra đánh giá an toàn thông tin mạng và rà quét, phân tích, xử lý mã độc; phòng ngừa sự cố, quản lý rủi ro; nghiên cứu, phân tích, xác minh, cảnh báo sự cố, rủi ro an toàn thông tin mạng, phần mềm độc hại.

Thời gian thực hiện: Cả năm.

Đơn vị thực hiện: Văn phòng Sở.

4. Thường xuyên tiến hành vá lỗi, cập nhật các phiên bản mới của phần mềm. Nếu phát hiện mã độc thì tiến hành các giải pháp kỹ thuật để khắc phục trường hợp vượt ngoài khả năng của cơ quan thì phối hợp với Sở Thông tin và Truyền thông để khắc phục sự cố, xử lý lỗi kịp thời.

Thời gian thực hiện: Khi xảy ra sự cố, lỗi.

Đơn vị thực hiện: Văn phòng Sở.

5. Định kỳ hàng quý (trước ngày 15, tháng cuối quý) tổ chức kiểm tra, đánh giá về an toàn thông tin; theo dõi, tổng hợp và thống kê chỉ số lây nhiễm mã độc trên các thiết bị đầu cuối, các hệ thống thông tin của cơ quan, báo cáo kết quả thực hiện đến Sở Thông tin và Truyền thông để tổng hợp, báo cáo UBND tỉnh, Bộ Thông tin và Truyền thông theo quy định.

Thời gian thực hiện: Hàng quý.

Đơn vị thực hiện: Văn phòng Sở.

6. Bố trí cán bộ tham gia các lớp tập huấn nâng cao kỹ năng, phương thức phòng, chống mã độc do Bộ Y tế, Sở Thông tin và Truyền thông tổ chức.

Thời gian thực hiện: Cả năm.

Đơn vị thực hiện: Văn phòng Sở.

7. Định kỳ 3 tháng/lần thay đổi mật khẩu đăng nhập trên hệ thống Máy chủ, hệ thống thư điện tử công vụ, các phần mềm: Quản lý văn bản và điều hành tác nghiệp, Quản lý kế toán... Để tăng tính bảo mật, yêu cầu mật khẩu phải có từ 8 ký tự trở lên, trong đó có chữ hoa, chữ thường, số và ký tự đặc biệt.

Thời gian thực hiện: 3 tháng/lần.

Đơn vị thực hiện: Cán bộ Công chức Sở.

8. Bảo đảm có giải pháp phòng, chống mã độc bảo vệ cho Máy chủ, máy trạm, thiết bị đầu cuối liên quan và có cơ chế tự động cập nhật phiên bản hoặc dấu hiệu nhận dạng mã độc mới.

Thời gian thực hiện: Hàng năm.

Đơn vị thực hiện: Văn phòng Sở.

9. Thiết lập cấu hình an toàn thông tin cho các thiết bị điện tử có kết nối Internet (camera giám sát, router, modem ADSL...) phù hợp với quy định, tuyệt đối không sử dụng cấu hình mặc định.

Thời gian thực hiện: Sau khi mua sắm thiết bị.

Đơn vị thực hiện: Văn phòng Sở.

III. TỔ CHỨC THỰC HIỆN

1. Văn phòng Sở:

Chủ trì, phối hợp với các Phòng, đơn vị thuộc Sở tổ chức thực hiện có hiệu quả. Kịp thời báo cáo Lãnh đạo Sở về những thuận lợi, khó khăn và những đề xuất, giải pháp để đảm bảo điều chỉnh phù hợp và kịp thời.

2. Các phòng, ban thuộc Sở:

Căn cứ vào chức năng, nhiệm vụ được giao, các Phòng, ban thuộc Sở phối hợp với Văn phòng Sở triển khai thực hiện tốt Kế hoạch nâng cao năng lực phòng, chống phần mềm độc hại của Sở Y tế năm 2018.

Trên đây là kế hoạch nâng cao năng lực phòng, chống phần mềm độc hại của Sở Y tế năm 2018, yêu cầu Trưởng các phòng, ban triển khai thực hiện./.

Nơi nhận:

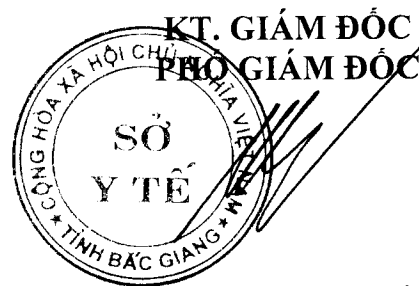
- Lưu VT, VP.

Bản điện tử:

- Sở TT&TT (b/c);

- Lãnh đạo Sở;

- Các phòng ban thuộc Sở.



Trương Quang Vinh