

KẾ HOẠCH

Triển khai thực hiện Chỉ thị số 14/CT-TTg ngày 25/5/2018 của Thủ tướng Chính phủ về nâng cao năng lực phòng, chống phần mềm độc hại bảo đảm an toàn, an ninh thông tin trên địa bàn tỉnh Đắk Nông giai đoạn 2018 – 2019

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

Căn cứ Quyết định số 63/QĐ-TTg ngày 13/01/2010 của Thủ tướng Chính phủ về phê duyệt Quy hoạch phát triển an toàn thông tin số quốc gia đến năm 2020;

Căn cứ Quyết định số 1622/QĐ-TTg ngày 25/10/2017 của Thủ tướng Chính phủ về 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 năm 2020, định hướng đến 2025;

Căn cứ Chỉ thị số 15/CT-TTg ngày 17/6/2014 của Thủ tướng Chính phủ về tăng cường công tác bảo đảm an ninh và an toàn thông tin mạng trong tình hình mới;

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 Thông tư số 03/2017/TT-BTTTT ngày 24/4/2017 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 86/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn thông tin theo cấp độ;

Căn cứ Quyết định số 20/2017/QĐ-UBND ngày 23/8/2017 của UBND tỉnh Đắk Nông ban hành Quy chế bảo đảm an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh Đắk Nông;

Nhằm tăng cường bảo đảm an toàn thông tin trong việc ứng dụng công nghệ thông tin trong các cơ quan nhà nước, nâng cao năng lực phòng, chống phần mềm độc hại, cải thiện độ tin cậy quốc gia trong hoạt động giao dịch điện tử, thúc đẩy phát triển kinh tế - xã hội, góp phần bảo đảm quốc phòng, an ninh trên địa bàn tỉnh Đắk Nông.

Ủy ban nhân dân tỉnh Đắk Nông xây dựng Kế hoạch triển khai thực hiện Chỉ thị số 14/CT-TTg ngày 25/5/2018 của Thủ tướng Chính phủ về nâng cao năng lực phòng, chống phần mềm độc hại bảo đảm an toàn, an ninh thông tin trên địa bàn tỉnh Đắk Nông giai đoạn 2018 - 2019.

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích

- Tạo chuyển biến mạnh mẽ trong nhận thức về an toàn thông tin, phòng chống phần mềm độc hại đối với lực lượng cán bộ, công chức, viên chức. Nâng cao trình độ, nhận thức kỹ năng xử lý các mối nguy hại của mã độc và trách nhiệm của các đơn vị, tổ chức, cá nhân trong công tác phòng, chống mã độc trong các cơ quan nhà nước tỉnh.

- Đảm bảo an ninh, an toàn hệ thống thông tin của tỉnh, đảm bảo phương châm phòng ngừa trong thế chủ động và xử lý kịp thời các sự cố. Trong đó tập trung đảm bảo an toàn thông tin cho các hệ thống thông tin quan trọng của tỉnh; có khả năng thích ứng một cách chủ động, linh hoạt và giảm thiểu các nguy cơ, đe dọa mất an toàn thông tin trên mạng; đề ra các giải pháp ứng phó khi gặp sự cố an toàn thông tin mạng.

2. Yêu cầu

- Cần khảo sát, đánh giá các nguy cơ, sự cố an toàn thông tin, phòng chống phần mềm độc hại của toàn hệ thống để đưa ra phương án đối phó, ứng cứu sự cố tương ứng, kịp thời, phù hợp.

- Phương án đối phó, ứng cứu sự cố an toàn thông tin, phần mềm độc hại phải đặt ra được các tiêu chí để có thể nhanh chóng xác định được tính chất, mức độ nghiêm trọng của sự cố khi xảy ra.

- Đảm bảo các nguồn lực và các điều kiện cần thiết để sẵn sàng triển khai kịp thời, hiệu quả phương án ứng cứu sự cố đảm bảo an toàn thông tin, phòng chống phần mềm độc hại lây lan trong hệ thống các cơ quan nhà nước tỉnh.

II. NỘI DUNG THỰC HIỆN

1. Nâng cao nhận thức về an toàn, an ninh thông tin, phòng chống phần mềm độc hại

- Quán triệt Chỉ thị số 14/CT-TTg ngày 25/5/2018 của Thủ tướng Chính phủ về nâng cao năng lực phòng, chống phần mềm độc hại bảo đảm an toàn, an ninh thông tin.

- Tổ chức tuyên truyền, phổ biến, nâng cao nhận thức các mối nguy hại của virus, mã độc đối với hệ thống máy vi tính bằng nhiều hình thức khác nhau như: cập nhật các cơ chế, chính sách (văn bản không mật) và văn bản chỉ đạo, hướng dẫn nghiệp vụ, bản tin trên Cổng thông tin điện tử của tỉnh, Trang thông

điện tử các Sở, ban, ngành và UBND các huyện thị xã; tổ chức hội nghị phổ biến để cán bộ Lãnh đạo các Sở, ban, ngành và UBND các huyện thị xã và cán bộ chuyên trách CNTT.

- Tập huấn kỹ năng xử lý các mối nguy hại của virus, mã độc đối với hệ thống máy vi tính cho công chức, viên chức tại cơ quan, đơn vị, địa phương (lồng ghép trong kế hoạch thực hiện Quyết định số 914/QĐ-UBND ngày 01/6/2017 của Ủy ban nhân dân tỉnh về việc đào tạo, phát triển nguồn nhân lực đảm bảo an toàn thông tin tỉnh Đắk Nông đến năm 2020 (giai đoạn 1).

Thời gian thực hiện: Quý IV/2018 và năm 2019.

Đơn vị thực hiện: Sở Thông tin và Truyền thông chủ trì, phối hợp với các cơ quan, đơn vị liên quan.

2. Khảo sát hiện trạng hạ tầng công nghệ thông tin

- Khảo sát, đánh giá hạ tầng công nghệ thông tin tại các cơ quan nhà nước theo Quyết định số 20/2017/QĐ-UBND ngày 23/8/2017 của UBND tỉnh Đắk Nông. Thống kê, rà soát, đánh giá về an toàn thông tin mạng máy tính các cơ quan nhà nước về các thiết bị mạng như: bộ chuyên mạch (switch), router, modem DSL, camera giám sát, v.v...; các hệ điều hành, các ứng dụng, tình hình sử dụng bản quyền.

- Ghi nhận những tồn tại, hạn chế để kiến nghị, đề xuất đơn vị chủ quản biện pháp xử lý, khắc phục và báo cáo UBND tỉnh theo quy định.

Thời gian thực hiện: Quý I/2019.

Đơn vị thực hiện: Sở Thông tin và Truyền thông chủ trì, phối hợp với các cơ quan, đơn vị liên quan.

3. Kiểm tra phân loại, xác định cấp độ an toàn hệ thống thông tin

- Đánh giá xác định cấp độ an toàn hệ thống thông tin và xây dựng phương án bảo đảm an toàn hệ thống thông tin theo cấp độ phù hợp với quy định của pháp luật và tiêu chuẩn, quy chuẩn kỹ thuật trong hệ thống thông tin của các cơ quan nhà nước trên địa bàn tỉnh.

- Thực hiện trình tự, thủ tục xác định cấp độ đối với hệ thống thông tin theo Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ và Thông tư số 03/2017/TT-BTTTT ngày 24/4/2017 của Bộ Thông tin và Truyền thông và thời gian hoàn thành theo Chỉ thị số 14/CT-TTg ngày 25/5/2018 của Thủ tướng Chính phủ.

Thời gian thực hiện: Quý IV/2018.

Đơn vị thực hiện: Sở Thông tin và Truyền thông chủ trì, phối hợp với các Sở, ban, ngành, UBND các huyện, thị xã và các cơ quan, đơn vị liên quan.

4. Giải pháp phòng, chống mã độc

a) Đầu tư phần mềm bản quyền tập trung phòng chống mã độc bảo vệ cho 100% máy chủ, máy trạm, thiết bị đầu cuối liên quan và đảm bảo cơ chế tự động cập nhật phiên bản hoặc dấu hiệu nhận diện mã độc mới. Có chức năng cho phép quản trị tập trung; có dịch vụ, giải pháp hỗ trợ kỹ thuật 24/7 có khả năng phản ứng kịp thời trong việc phát hiện, phân tích và gỡ bỏ phần mềm độc hại; có thể chia sẻ thông tin, dữ liệu thống kê tình hình lây nhiễm mã độc với hệ thống kỹ thuật của cơ quan chức năng có thẩm quyền, tuân thủ theo tiêu chuẩn, quy chuẩn kỹ thuật, hướng dẫn nghiệp vụ của Bộ Thông tin và Truyền thông.

Thời gian thực hiện: Quý IV/năm 2018 và năm 2019.

Đơn vị thực hiện: Sở Thông tin và Truyền thông chủ trì, phối hợp với các cơ quan, đơn vị liên quan.

b) Các dự án đầu tư, các hoạt động ứng dụng công nghệ thông tin hoặc thuê dịch vụ công nghệ thông tin phải có cấu phần phù hợp cho giải pháp bảo đảm an toàn thông tin, giải pháp phòng, chống mã độc. Khi đầu tư mới mua sắm, sử dụng phần mềm có bản quyền để đảm bảo an ninh thông tin.

c) Sử dụng triệt để chữ ký số, chứng thư số trong trao đổi văn bản điện tử trên Phần mềm văn phòng điện tử iOffice; đảm bảo 100% các văn bản phát hành trên môi trường mạng phải sử dụng chứng thư số, chữ ký số với các cơ quan, đơn vị, địa phương trên địa bàn tỉnh và các Bộ, Ngành, Trung ương. Thực hiện nghiêm Quyết định số 28/2018/QĐ-TTg ngày 12/7/2018 của Thủ tướng Chính phủ quy định về việc gửi, nhận văn bản điện tử giữa các cơ quan trong hệ thống nhà nước, Quyết định số 37/2016/QĐ-UBND ngày 28/11/2016 của UBND tỉnh, Quyết định số 35/2016/QĐ-UBND ngày 15/11/2016 của UBND tỉnh.

d) Rà soát, kiểm tra, nâng cấp, chuẩn hóa các thiết bị phần cứng, phần mềm khắc phục lỗ hổng an toàn thông tin mạng

- Rà soát, nâng cấp cấu hình máy chủ, máy trạm để mua sắm nâng cấp hệ điều hành và các ứng dụng bản quyền trên cài máy chủ, máy trạm phiên bản mới hoặc cập nhật các phiên bản mới do Bộ Thông tin và Truyền thông, Bộ Công an và Sở Thông tin và Truyền thông hướng dẫn, cảnh báo. Thiết lập, cấu hình chính sách bảo mật trên hệ điều hành máy chủ, máy trạm cho người sử dụng.

- Rà soát, mua sắm bổ sung các thiết bị chuyển mạch (Switch), router, thiết bị lưu trữ dự phòng qua mạng (Network-Attached Storage, viết tắt là NAS) để lưu trữ dữ liệu dự phòng quan trọng,... có tính năng bảo mật để cấu hình, thiết lập chính sách bảo mật kết nối mạng. Kiểm tra, đánh giá về an toàn thông tin đối với các thiết bị có kết nối Internet (như camera giám sát, router, modem DSL ...) trước khi đưa vào sử dụng; thiết lập cấu hình an toàn thông tin phù hợp với quy định, tuyệt đối không sử dụng cấu hình mặc định của các thiết bị.

đ) Phối hợp với các doanh nghiệp cung cấp dịch vụ viễn thông, Internet (ISP) hoặc các tổ chức, doanh nghiệp hoạt động trong lĩnh vực công nghệ thông tin và an toàn thông tin rà quét, gỡ mã độc, mạng máy tính nhiễm mã độc, trên Cổng/trang thông tin điện tử khắc phục các lỗ hổng bảo mật và điểm yếu có nguy cơ bị tin tặc (hacker) khai thác, tấn công đối với các Website của các cơ quan Đảng, Nhà nước, tổ chức chính trị - xã hội trên địa bàn tỉnh.

e) Hàng tháng tổ chức sao lưu dữ liệu quan trọng của cơ quan, đơn vị ra thiết bị thiết bị lưu trữ dự phòng qua mạng (Network-Attached Storage, viết tắt là NAS).

g) Định kỳ thực hiện kiểm tra, đánh giá tổng thể về an toàn thông tin theo quy định tại Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ và hướng dẫn tại Thông tư số 03/2017/TT-BTTTT ngày 24/4/2017 của Bộ Thông tin và Truyền thông; tổ chức theo dõi, thống kê chỉ số lây nhiễm mã độc trên các thiết bị đầu cuối, các hệ thống thông trong cơ quan nhà nước, định kỳ hàng, quý báo cáo về Sở Thông tin và Truyền thông trước ngày 20 hàng tháng và ngày 20 của tháng cuối cùng trong quý.

h) Khi xảy ra sự cố mất an toàn an ninh thông tin tại cơ quan, đơn vị, địa phương cần khẩn trương ghi nhận sự cố và gửi cảnh báo về Sở Thông tin và Truyền thông, Đội Ứng cứu sự cố an toàn thông tin mạng tỉnh Đắk Nông để được hướng dẫn khắc phục sự cố theo quy định.

Nội dung các mục b, c, d, đ, e, g, h: Thời gian thực hiện hàng năm.

Đơn vị thực hiện: Các Sở, Ban, Ngành, UBND các huyện, thị xã và UBND các xã, phường, thị trấn.

5. Về cán bộ đảm nhiệm nhiệm vụ bảo đảm an toàn thông tin mạng

- Kiện toàn đội ngũ cán bộ chuyên trách về công nghệ thông tin tại cơ quan, đơn vị, địa phương theo Quyết định số 02/2017/QĐ-UBND ngày 24/01/2017 của UBND tỉnh để đảm nhiệm chuyên trách ứng cứu sự cố an toàn thông tin mạng tại đơn vị, chịu sự điều phối ứng cứu sự cố theo chỉ đạo từ Ban Chỉ đạo ứng cứu sự cố an toàn thông tin mạng tỉnh Đắk Nông theo Quyết định số 1340/QĐ-UBND ngày 15/8/2017 của UBND tỉnh và Quyết định số 25/QĐ-ĐỨCSCATTTM ngày 10/5/2018 của Đội trưởng Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Đắk Nông về việc ban hành Quy chế hoạt động của Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Đắk Nông.

- Cử cán bộ, công chức, viên chức tham gia các lớp tập huấn kiến thức, kỹ năng về phòng, chống các nguy cơ mất an toàn thông tin mạng do Sở Thông tin và Truyền thông tổ chức hàng năm hoặc đăng ký nhu cầu học tập với các trường, các tổ chức đào tạo có uy tín về đào tạo an toàn, an ninh thông tin trên cả nước.

- Ưu tiên bố trí kinh phí cho cán bộ, công chức được tham gia, học tập nâng cao trình độ chuyên môn, nghiệp vụ về an toàn, an ninh thông tin; bố trí kinh phí mua sắm các thiết bị bảo mật đảm bảo an toàn, phòng chống mã độc trong các cơ quan, đơn vị, địa phương theo quy định.

III. KINH PHÍ THỰC HIỆN

Nguồn kinh phí: Ngân sách tỉnh và kết hợp với nguồn ngân sách trung ương.

IV. TỔ CHỨC THỰC HIỆN

1. Sở Thông tin và Truyền thông

- Chủ trì, phối hợp với các cơ quan, đơn vị liên quan triển khai các nội dung Kế hoạch đề ra theo quy định.

- Hướng dẫn các cơ quan nhà nước trên địa bàn tỉnh tăng cường thực hiện công tác bảo đảm an toàn, an ninh thông tin, nâng cao năng lực phòng, chống phần mềm độc hại tại cơ quan, đơn vị, địa phương.

- Tổ chức các khóa tập huấn nâng cao nhận thức, kiến thức, kỹ năng về an toàn thông tin mạng cho cán bộ, công chức, viên chức chuyên trách về công nghệ thông tin cho các Sở, ban, ngành, UBND cấp huyện, UBND cấp xã.

- Chỉ đạo các cơ quan báo chí, phát thanh, truyền hình đẩy mạnh tuyên truyền, nâng cao nhận thức, kỹ năng xử lý các mối nguy hại của mã độc; công tác phòng, chống mã độc tại cơ quan, đơn vị, địa phương.

- Tăng cường công tác thanh tra, kiểm tra và xử lý các tổ chức, cá nhân vi phạm quy định về bảo đảm an toàn thông tin. Phối hợp với Công an tỉnh trong hoạt động phòng, chống tội phạm trong lĩnh vực công nghệ thông tin.

- Chủ trì theo dõi, đôn đốc, kiểm tra việc thực hiện Kế hoạch, tổng hợp, báo cáo kết quả thực hiện.

2. Công an tỉnh

- Tăng cường công tác phòng ngừa, phát hiện, điều tra xử lý tội phạm trong lĩnh vực công nghệ thông tin.

- Phối hợp với Sở Thông tin và Truyền thông tiến hành kiểm tra và xử lý các tổ chức, cá nhân vi phạm quy định về bảo đảm an toàn, an ninh thông tin.

- Chủ động phối hợp với Sở Thông tin và Truyền thông tham mưu cho các cơ quan, đơn vị trên địa bàn tỉnh tổ chức rà soát, kiểm tra, đánh giá an toàn, an ninh thông tin: kịp thời phát hiện và ngăn chặn các hoạt động sử dụng các phần mềm độc hại trên máy tính của cơ quan, đơn vị.

3. Sở Nội vụ

- Chủ trì, phối hợp với các Sở, ban, ngành, UBND các huyện, thị xã rà soát, bố trí cán bộ, công chức, viên chức chuyên trách CNTT tại cơ quan, đơn vị.

- Phối hợp với Sở Thông tin và Truyền thông căn cứ kết quả thực hiện Kế hoạch để tham mưu UBND tỉnh đánh giá mức độ hoàn thành nhiệm vụ hàng năm của Lãnh đạo các Sở, ban, ngành, UBND các huyện, thị xã.

4. Sở Tài chính

Tham mưu, đề xuất UBND tỉnh bố trí kinh phí thực hiện Kế hoạch và phối hợp thực hiện Kế hoạch theo chức năng, nhiệm vụ được giao.

5. Thủ trưởng các Sở, ban, ngành; Chủ tịch UBND các huyện, thị xã; Chủ tịch UBND các xã, phường, thị trấn

- Bố trí công chức, viên chức làm công tác chuyên trách về công nghệ thông tin để thực hiện, bảo đảm an toàn thông tin theo Quyết định số 02/2017/QĐ-UBND ngày 24/01/2017 của Ủy ban nhân dân tỉnh về việc ban hành Quy chế quản lý chuyên môn nghiệp vụ đối với cán bộ, công chức, viên chức chuyên trách công nghệ thông tin tại các cơ quan nhà nước tỉnh Đắk Nông; Quyết định số 13/2017/QĐ-UBND ngày 04/7/2017 của Ủy ban nhân dân tỉnh về việc ban hành Quy định về phân cấp, quản lý tổ chức bộ máy, biên chế và cán bộ, công chức, viên chức tỉnh Đắk Nông.

- Gương mẫu, tích cực sử dụng ký số trong việc gửi nhận văn bản điện tử giữa các cơ quan nhà nước trên địa bàn tỉnh.

- Thủ trưởng các đơn vị thực hiện các nội dung trong Kế hoạch và phối hợp với Sở Thông tin và Truyền thông triển khai thực hiện Kế hoạch này.

Trong quá trình thực hiện nếu có khó khăn, vướng mắc kịp thời báo cáo UBND tỉnh (qua Sở Thông tin và Truyền thông) để xem xét, chỉ đạo./.

Nơi nhận:

- Văn phòng Chính phủ (b/c);
- Bộ Thông tin và Truyền thông (b/c);
- Thường trực Tỉnh ủy (b/c);
- Thường trực HĐND tỉnh (b/c);
- Chủ tịch, các Phó Chủ tịch UBND tỉnh;
- Văn phòng Tỉnh ủy;
- Đảng ủy Khối các cơ quan tỉnh;
- Công an tỉnh;
- Các Sở, ban, ngành;
- UBND các huyện, thị xã;
- CVP, các PCVP UBND tỉnh;
- Lưu: VT, TTĐT.

13

**KT. CHỦ TỊCH
PHÓ CHỦ TỊCH**



Cao Huy