ỦY BAN NHÂN DÂN TỈNH QUẢNG TRỊ	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 4339/KH-UBND	*Quảng Trị, ngày 03 tháng 10 năm 2018*

KẾ HOẠCH

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

I. CĂN CỨ PHÁP LÝ

- Luật An toàn thông tin mạng ngày 19/11/2015;

- 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 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ về ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia;

- 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;

- 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 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ.

II. MỤC TIÊU

- Tạo sự chuyển biến sâu sắc trong nhận thức của cán bộ, công chức, viên chức và nhân dân về tầm quan trọng của công tác đảm bảo an toàn thông tin mạng.

- Bảo đảm an toàn thông tin mạng của các cơ quan nhà nước trong toàn 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; sẵn sàng các giải pháp phòng ngừa và ứng phó khi có sự cố về an toàn thông tin mạng.

- Nâng cao năng lực chuyên môn về an toàn, an ninh thông tin cho cán bộ chuyên trách công nghệ thông tin (CNTT) trong toàn tỉnh. Đảm bảo 100% các đơn vị có cán bộ chuyên trách CNTT được đào tạo chuyên sâu về an toàn, an ninh thông tin.

- Tuyên truyền, nâng cao nhận thức về an toàn thông tin mạng đến 100% cán bộ, công chức, viên chức toàn tỉnh.

- 100% cơ quan nhà nước được áp dụng phương án an toàn thông tin phù hợp, triển khai chuẩn hóa cấp độ an toàn của các hệ thống thông tin và tổ chức thực hiện nghiêm túc Quyết định số 35/2016/QĐ-UBND ngày 29/8/2016 của UBND tỉnh về việc ban hành Quy chế đảm bảo an toàn, an ninh thông tin trong hoạt động của các cơ quan nhà nước tỉnh Quảng Trị.

- 100% các hệ thống thông tin dùng chung, các hệ thống mạng LAN, máy chủ của các sở, ban, ngành cấp tỉnh, UBND cấp huyện và mạng chuyên dùng của các cơ quan nhà nước được trang bị giải pháp an toàn, bảo mật nhằm bảo đảm an toàn thông tin trên môi trường mạng.

- 100% cổng, trang thông tin điện tử của các cơ quan nhà nước được giám sát, sẵn sàng các biện pháp phòng ngừa, ngăn chặn tấn công gây mất an toàn thông tin và có phương án khắc phục sự cố đảm bảo hệ thống hoạt động liên tục 24/24.

III. NỘI DUNG

1. Tuyên truyền, nâng cao nhận thức về an toàn thông tin mạng

- Tổ chức quán triệt và thực hiện có hiệu quả Luật An toàn thông tin mạng, Luật An ninh mạng và các văn bản của Chính phủ, của tỉnh về an toàn thông tin mạng; nâng cao nhận thức, trách nhiệm cho đội ngũ cán bộ, công chức, viên chức về công tác an toàn thông tin mạng.

- Thực hiện tuyên truyền trên các phương tiện thông tin đại chúng như Báo Quảng Trị, Đài Phát thanh - Truyền hình tỉnh, hệ thống Đài truyền thanh các cấp và trên cổng, trang thông tin điện tử nhằm nâng cao nhận thức về an toàn thông tin cho người dân, doanh nghiệp.

2. Triển khai các giải pháp bảo đảm an toàn thông tin

- Triển khai các biện pháp đảm bảo an toàn thiết bị, hạ tầng viễn thông, CNTT trong đấu thầu, mua sắm, đặc biệt là các thiết bị quan trọng. Riêng các dự án về CNTT khi xây dựng bắt buộc phải có cấu phần mua sắm giải pháp phòng, chống mã độc, bảo đảm tuân thủ đúng quy định của pháp luật.

- Kiểm tra, đánh giá toàn diện về hiện trạng, đánh giá phân loại các nhóm nguy cơ, mức độ rủi ro, thiệt hại từ các sự cố an toàn thông tin; dự báo xu hướng phát triển của tội phạm công nghệ cao và đề xuất hệ thống giải pháp thực thi hiệu quả việc bảo đảm an toàn thông tin mạng trong toàn tỉnh.

- Đầu tư nâng cao hệ thống trang thiết bị lưu trữ dữ liệu, sao lưu dự phòng cho các máy chủ và máy trạm, sao lưu dữ liệu cho các hệ thống phần mềm dùng chung như phần mềm điều hành tác nghiệp, hệ thống một cửa điện tử, các hệ thống thông tin và cơ sở dữ liệu chuyên ngành... đảm bảo an toàn dữ liệu ở mức cao nhất cho các hệ thống.

- Thường xuyên kiểm tra, rà soát các lỗ hổng bảo mật, an toàn thông tin trên cổng/ trang thông tin điện tử các cơ quan nhà nước trên địa bàn tỉnh; xây dựng các giải pháp và tổ chức khắc phục lỗ hổng, điểm yếu có rủi ro gây mất an toàn thông tin.

- Triển khai các giải pháp đảm bảo an toàn thông tin cho các dịch vụ cung cấp trên cổng/trang thông tin điện tử các cơ quan nhà nước trên địa bàn tỉnh; hệ thống thư điện tử của tỉnh; phần mềm quản lý điều hành của tỉnh, huyện; hệ thống một cửa điện tử của các cơ quan nhà nước, Cổng dịch vụ công trực tuyến của tỉnh.

- Thực hiện đồng bộ các biện pháp phòng, chống mã độc, bảo vệ 100% máy trạm, thiết bị đầu cuối liên quan tại các sở, ban ngành, UBND các huyện, thị xã, thành phố theo Chỉ thị số 14/CT-TTg ngày 25/5/2018 của Thủ tướng Chính phủ.

- Áp dụng quy trình quản lý an toàn hạ tầng kỹ thuật tại các đơn vị bao gồm:

+ Các giải pháp bảo vệ nhằm ngăn chặn và phát hiện sớm việc truy cập trái phép vào mạng máy tính hay thiết bị lưu trữ dữ liệu; theo dõi thường xuyên tình trạng lây nhiễm và thực hiện loại bỏ phần mềm độc hại ra khỏi hệ thống;

+ Áp dụng các công nghệ xác thực, cơ chế quản lý quyền truy cập và cơ chế ghi biên bản hoạt động của hệ thống để quản lý và kiểm tra việc truy cập mạng;

+ Kiểm soát chặt chẽ việc cài đặt các phần mềm mới lên máy chủ và máy trạm;

+ Áp dụng quy trình sao lưu, dự phòng (backup) dữ liệu, bảo đảm an toàn dữ liệu, đầu tư các thiết bị lưu trữ dữ liệu an toàn từ tỉnh đến các sở, ngành, huyện, thị xã, thành phố;

+ Các quy trình quản lý an toàn hạ tầng kỹ thuật khác.

3. Triển khai các nội dung xử lý sự cố an toàn thông tin

- Tổ chức thực hiện xác định cấp độ an toàn các hệ thống thông tin của cơ quan nhà nước trên địa bàn tỉnh theo quy định tại 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.

- Tham gia diễn tập bảo đảm an toàn thông tin và ứng cứu sự cố mạng.

- Triển khai thực hiện Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ và Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng toàn quốc.

- Triển khai các phương pháp bảo vệ sau xử lý sự cố.

4. Tích cực triển khai ứng dụng chữ ký số trong gửi nhận văn bản điện tử

- Tổ chức quản lý, đăng ký, cấp phát, thu hồi, thay đổi thông tin chứng thư số theo quy định tại Quyết định số 10/2017/QĐ-UBND ngày 21/7/2017 của UBND tỉnh về việc ban hành Quy chế quản lý và sử dụng chữ ký số, chứng thư số chuyên dùng trên địa bàn tỉnh Quảng Trị và Kế hoạch số 3061/KH-UBND ngày 11/7/2017 của UBND tỉnh về việc triển khai ứng dụng chữ ký số chuyên dùng trong hoạt động của các cơ quan nhà nước tỉnh Quảng Trị giai đoạn 2017-2020.

- Tăng cường ứng dụng, sử dụng chữ ký số trong gửi nhận văn bản điện tử giữa các cơ quan nhà nước trên địa bàn tỉnh.

5. Đào tạo nguồn nhân lực an toàn thông tin

- Phổ biến, đào tạo, tập huấn nâng cao nhận thức an toàn thông tin cho cán bộ, công chức, viên chức các cơ quan nhà nước, cơ quan Đảng trên địa bàn tỉnh. Hỗ trợ cán bộ chuyên trách CNTT tham gia các lớp tập huấn chuyên ngành về an toàn thông tin do các bộ, ngành Trung ương tổ chức.

- Đào tạo vận hành hệ thống an toàn thông tin cho 100% đội ngũ cán bộ chuyên trách CNTT cấp tỉnh, cấp huyện. Tổ chức thực hiện chương trình đào tạo nâng cao trình độ chuyên môn, nghiệp vụ cho cán bộ thực hiện nhiệm vụ chuyên trách CNTT cấp xã; hình thành đội ngũ cán bộ chuyên trách an toàn thông tin từ cấp tỉnh đến cấp huyện. Đào tạo nâng cao nhận thức an toàn thông tin cho lãnh đạo CNTT (CIO) các cấp.

IV. GIẢI PHÁP

1. Chỉ đạo điều hành

- Ban Chỉ đạo CNTT tỉnh, Ban Chỉ đạo CNTT các huyện, thành phố, thị xã tăng cường công tác chỉ đạo bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng CNTT của các cơ quan nhà nước trên địa bàn.

- Tiếp tục hoàn thiện bộ máy quản lý nhà nước về an toàn thông tin mạng từ cấp tỉnh đến cấp huyện, trong đó chú trọng nâng cao năng lực, trình độ chuyên môn nghiệp vụ cho cán bộ chuyên trách công nghệ thông tin, đội ngũ cán bộ làm nhiệm vụ quản trị an toàn thông tin, ứng cứu sự cố mạng máy tính; nâng cao vai trò, trách nhiệm của đơn vị chuyên trách ứng cứu sự cố mạng máy tính của tỉnh.

2. Giải pháp về tài chính

- Tranh thủ sự hỗ trợ từ các bộ, ngành Trung ương, chương trình quốc gia về CNTT và nguồn vốn ODA; tăng cường huy động các nguồn vốn xã hội hóa và thực hiện việc thuê các dịch vụ CNTT.

- Tăng cường kiểm tra, giám sát đối với các dự án về CNTT, an toàn thông tin nhằm đảm bảo tính hiệu quả của quá trình đầu tư và phát huy tối đa hiệu quả khai thác các nguồn vốn.

- Hàng năm, cân đối, bố trí nguồn ngân sách của tỉnh cho công tác đảm bảo an toàn thông tin mạng theo từng nội dung công việc cụ thể.

3. Giải pháp môi trường chính sách

- Tiếp tục tổ chức thực hiện có hiệu quả Luật An toàn thông tin mạng, Luật An ninh mạng; 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 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ về ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia; 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.

- Tổ chức thực hiện hiệu quả cơ chế, chính sách hiện hành về ứng dụng và phát triển CNTT trên địa bàn tỉnh, trong đó chú trọng các nội dung về bảo đảm an toàn thông tin. Xây dựng, ban hành một số quy định, phụ cấp ưu đãi cho đội ngũ cán bộ chuyên trách công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh.

- Hoàn thiện các văn bản quy định về thuê dịch vụ CNTT; quy trình thử nghiệm, vận hành thử và nghiệm thu, công nhận đảm bảo an toàn đối với các hệ thống thông tin dùng chung trên địa bàn.

4. Các giải pháp khác

- Đổi mới công tác tuyên truyền, tăng cường tuyên truyền trực tuyến, trực quan, phát huy hiệu quả các cổng/ trang thông tin điện tử, hệ thống truyền thanh cơ sở.

- Đẩy mạnh nghiên cứu khoa học, áp dụng công nghệ mới trong việc bảo đảm an toàn thông tin, ưu tiên các đề tài nghiên cứu khoa học về bảo đảm an toàn thông tin, đặc biệt là bảo đảm an toàn thông tin trong các cơ quan nhà nước.

V. TỔ CHỨC THỰC HIỆN

1. Sở Thông tin và Truyền thông

- Chủ trì, phối hợp với các cơ quan, đơn vị có liên quan tổ chức triển khai thực hiện Kế hoạch; hướng dẫn, theo dõi, kiểm tra, đôn đốc việc triển khai Kế hoạch này;

- Phối hợp với Cục An toàn thông tin thuộc Bộ Thông tin và Truyền thông hướng dẫn các cơ quan kết nối các giải pháp phòng, chống mã độc ở các cơ quan với các hệ thống kỹ thuật phòng, chống mã độc của các cơ quan liên quan.

- Tổ chức đào tạo, bồi dưỡng cập nhật kiến thức, nâng cao năng lực về an toàn thông tin cho đội ngũ lãnh đạo CNTT, cán bộ chuyên trách CNTT, cán bộ thuộc Đơn vị chuyên trách ứng cứu sự cố an toàn thông tin mạng của tỉnh.

- Hướng dẫn, theo dõi, kiểm tra, đôn đốc việc triển khai các chương trình, dự án ứng dụng CNTT, bảo đảm về an toàn thông tin.

- Phối hợp với các cơ quan liên quan tham mưu cho UBND tỉnh thu hút nguồn lực và các nguồn hỗ trợ từ Trung ương để thực hiện thành công Kế hoạch.

- Tích hợp và ứng dụng chữ ký số vào việc cung cấp thông tin trên Cổng dịch vụ công trực tuyến của tỉnh, hệ thống gửi nhận văn bản điện tử, hệ thống thư điện tử công vụ.

- 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 trong đơn vị.

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

2. Văn phòng UBND tỉnh

Bảo đảm an toàn thông tin, phòng chống mã độc cho các hệ thống thông tin, các cơ sở dữ liệu dùng chung của tỉnh đang được Văn phòng UBND tỉnh quản lý, vận hành.

3. Công an tỉnh, Bộ Chỉ huy Quân sự tỉnh

- Phối hợp với Sở Thông tin và Truyền thông, tăng cường công tác tuyên truyền, phổ biến pháp luật và xử lý tội phạm trong lĩnh vực CNTT, truyền thông.

- Chủ trì, phối hợp với Sở Thông tin và Truyền thông tổ chức kiểm tra, đánh giá thực trạng an toàn, an ninh thông tin mạng trong các cơ quan nhà nước trên địa bàn tỉnh; phát hiện, đấu tranh, ngăn chặn mọi âm mưu, thủ đoạn hoạt động sử dụng không gian mạng của các thế lực thù địch, tội phạm mạng nhằm xâm phạm an ninh

quốc gia, trật tự an toàn xã hội và gây mất an toàn thông tin mạng. Điều tra, xử lý kịp thời các vi phạm về an ninh, an toàn thông tin mạng.

- Thường xuyên thông báo, cảnh báo cho các cơ quan nhà nước, người dân và doanh nghiệp về phương thức, thủ đoạn mới của các loại tội phạm gây mất an toàn thông tin để có biện pháp phòng ngừa, đấu tranh, ngăn chặn.

4. Sở Kế hoạch và Đầu tư, Sở Tài chính

Căn cứ khả năng ngân sách hằng năm, bố trí kinh phí để triển khai các hoạt động đảm bảo việc nâng cao năng lực phòng, chống phần mềm độc hại theo quy định của Luật Ngân sách nhà nước.

5. Báo Quảng Trị, Đài Phát thanh - Truyền hình tỉnh

- Thực hiện tuyên truyền, đăng phát và đưa tin về các hoạt động đảm bảo an toàn thông tin nhằm nâng cao nhận thức về an toàn thông tin mạng.

- Tăng cường các bài viết chương trình, dành thời lượng thích hợp để tuyên truyền, phổ biến về tác hại và phương thức phòng, chống mã độc.

6. Các sở, ban, ngành cấp tỉnh; UBND các huyện, thị xã, thành phố

- Tổ chức xác định cấp độ và xây dựng Hồ sơ đề xuất cấp độ an toàn hệ thống thông tin theo văn bản hướng dẫn số 677/STTTT-CNTT ngày 15/8/2018 của Sở Thông tin và Truyền thông; Thường xuyên kiểm tra đánh giá tổng thể về an toàn thông tin theo quy định tại Nghị định số 85/2016/NĐ-CP ngày 01/72016 của Chính phủ, Thông tư số 03/2017/TT-BTTTT ngày 24/4/2017 của Bộ Thông tin và Truyền thông. Tiến hành xác định hệ thống thông tin cấp độ 4, cấp độ 5 theo quy định tại Nghị định 85/2016/NĐ-CP quy định về bảo đảm an toàn hệ thống thông tin theo cấp độ thời hạn hoàn thành trước ngày 15/11/2018.

- Xây dựng, ban hành các quy chế nội bộ về đảm bảo an toàn thông tin tại các đơn vị, địa phương. Tăng cường công tác tuyên truyền nâng cao nhận thức về an toàn thông tin mạng cho cán bộ, công chức, viên chức, người dân và doanh nghiệp trên địa bàn, thuộc phạm vi quản lý.

- Chủ động thực hiện các biện pháp bảo đảm an toàn thông tin cho các hệ thống thông tin đang triển khai, ứng dụng tại đơn vị mình. Phối hợp kịp thời với Sở Thông tin và Truyền thông về ứng cứu sự cố an toàn thông tin mạng của tỉnh trong việc giám sát, phòng ngừa và xử lý các sự cố về an toàn thông tin.

- Chủ động bố trí kinh phí tăng cường cơ sở hạ tầng đảm bảo an toàn thông tin, thiết bị tường lửa, phần mềm chống mã độc, rà soát kiểm tra lỗ hổng bảo mật, an ninh trên các dịch vụ công trực tuyến, cổng/trang thông tin điện tử của các đơn vị, địa phương; tạo điều kiện cho cán bộ tham dự các lớp đào tạo về an toàn thông tin.

- Thực hiện cài đặt phần mềm tường lửa/phần mềm phát hiện các mã độc cho các máy chủ, máy trạm tại đơn vị. Bảo đảm có giải pháp phòng, chống mã độc bảo vệ cho 100% 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 hạn hoàn thành trước 12 năm 2018.

- Trong các dự án đầu tư ứng dụng 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 mua sắm các thiết bị điện tử có kết nối Internet (như camera giám sát, router, modem DSL, v.v...) cần thực hiện rà soát, kiểm tra, đánh giá về an toàn thông tin; trước khi đưa vào sử dụng cần thiết lập cấu hình an toàn thông tin phù hợp với quy định, tuyệt đối không sử dụng cấu hình mặc định. Lưu ý, quy trình triển khai áp dụng theo Quyết định số 80/QĐ-TTg ngày30/12/2014 của Thủ tướng Chính phủ quy định thí điểm về thuê dịch vụ công nghệ thông tin trong cơ quan Nhà nước; Thông tư số 21/2010/TT-BTTTT ngày 08/9/2010 của Bộ Thông tin và Truyền thông quy định về lập đề cương và dự toán chi tiết đối với hoạt động ứng dụng công nghệ thông tin sử dụng nguồn vốn ngân sách nhà nước nhưng không yêu cầu phải lập dự án.

- Căn cứ kế hoạch đề ra, hàng năm xây dựng dự toán ngân sách từ nguồn chi thường xuyên để triển khai các hoạt động liên quan đến giải pháp bảo đảm an toàn thông tin, giải pháp phòng, chống mã độc.

- Tích cực triển khai ứng dụng chữ ký số trong gửi nhận văn bản điện tử giữa các cơ quan nhà nước theo Kế hoạch số 3061/KH-UBND ngày 11/7/2017 của UBND tỉnh về việc triển khai ứng dụng chữ ký số chuyên dùng trong hoạt động của các cơ quan nhà nước tỉnh Quảng Trị, giai đoạn 2017- 2020 đảm bảo thời gian, lộ trình thực hiện./.

Nơi nhận:
- Văn phòng Chính phủ;
- Bộ Thông tin và Truyền thông;
- TT/Tỉnh ủy, TT/HĐND Tỉnh;
- Chủ tịch, các PCT UBND tỉnh;
- Các Sở, ban, ngành cấp tỉnh;
- UBND các huyện, thị xã, thành phố;
- Trung tâm Tin học tỉnh;
- Lưu: VT, VX.

TM. ỦY BAN NHÂN DÂN
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Mai Thức