

Đăk Lăk, ngày 23 tháng 10 năm 2019

CHỈ THỊ
Về việc tăng cường triển khai các hoạt động
đảm bảo an toàn thông tin mạng

Trong thời gian qua, tình hình mất an toàn thông tin số ở nước ta và trên thế giới vẫn diễn biến phức tạp, xuất hiện nhiều nguy cơ đe dọa nghiêm trọng đến việc ứng dụng công nghệ thông tin phục vụ phát triển kinh tế - xã hội và đảm bảo quốc phòng, an ninh. Các thế lực thù địch, phản động, tội phạm mạng tăng cường tấn công, thâm nhập hệ thống mạng thông tin trọng yếu của Đảng, Chính phủ, các Tập đoàn kinh tế, tài chính, ngân hàng để thu thập, đánh cắp thông tin bí mật Nhà nước, phát tán thông tin xấu, phá hoại, gây rối nội bộ... Theo kết quả đánh giá của Cục An toàn thông tin và Hiệp hội An toàn thông tin Việt Nam, chỉ số đánh giá mức độ bảo đảm an toàn thông tin mạng tỉnh Đăk Lăk năm 2018 thuộc nhóm C (quan tâm triển khai an toàn thông tin ở mức trung bình). Kết quả đánh giá cũng cho thấy nhiều hệ thống công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh, các công, trang thông tin điện tử có nhiều điểm yếu về an toàn thông tin, chưa được áp dụng các giải pháp đảm bảo an toàn và bảo mật thông tin cho phù hợp.

Để tăng cường khả năng phòng, chống các nguy cơ tấn công, xâm nhập hệ thống công nghệ thông tin và ngăn chặn, khắc phục kịp thời các sự cố an toàn thông tin mạng máy tính trên địa bàn tỉnh, Chủ tịch Ủy ban Nhân dân tỉnh chỉ đạo:

1. Thủ trưởng các Sở, ban, ngành; Chủ tịch UBND các huyện, thị xã, thành phố

- Triển khai các biện pháp tăng cường đảm bảo an toàn thông tin trên môi trường mạng ở mỗi cơ quan, đơn vị trong thẩm quyền quản lý của đơn vị, địa phương. Chịu trách nhiệm trước UBND tỉnh, Chủ tịch UBND tỉnh nếu để xảy ra sự cố lộ, lọt thông tin quan trọng của Nhà nước tại cơ quan, đơn vị, địa phương mình.

- Quán triệt, chỉ đạo thực hiện nghiêm túc Luật An toàn thông tin mạng năm 2015; Luật Bảo vệ bí mật nhà nước năm 2018 (có hiệu lực từ ngày 01/7/2020); 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; 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; Chỉ thị số 14/CT-TTg ngày 07/6/2019 của Thủ tướng Chính phủ về tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam và các văn bản khác có liên quan.

- 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 theo chỉ đạo tại Chỉ thị số 14/CT-TTg ngày 25/5/2018 của Thủ tướng Chính phủ và bảo đảm tương thích với giải pháp phòng, chống mã độc chung của tỉnh đã được Sở Thông tin và Truyền thông đầu tư.

- Phối hợp chặt chẽ với Đội ứng cứu sự cố an toàn thông tin mạng của tỉnh, Trung tâm Công nghệ thông tin và Truyền thông - Sở Thông tin và Truyền thông (Đơn vị chuyên trách về kỹ thuật an toàn thông tin mạng) để thực hiện giám sát, phòng ngừa và ứng cứu sự cố an toàn thông tin mạng, Cổng/Trang thông tin điện tử tại cơ quan, đơn vị mình. Khi phát hiện có sự cố hoặc có nguy cơ xảy ra sự cố về an toàn thông tin mạng, thực hiện quy trình theo Quy chế hoạt động của Đội ứng cứu sự cố an toàn thông tin mạng của tỉnh.

- Yêu cầu mọi tổ chức, cá nhân quản lý chặt chẽ khóa bí mật (USB token) của chữ ký số, các tài khoản được cấp để khai thác các hệ thống thông tin, phần mềm nghiệp vụ, bảo đảm tính bảo mật; tuân thủ quy định, quy chế sử dụng chữ ký số khi gửi, ban hành văn bản điện tử trên môi trường mạng.

- Chỉ sử dụng các hệ thống thông tin dùng chung của tỉnh: Hệ thống thư điện tử công vụ; hệ thống quản lý văn bản và điều hành,... để gửi nhận, trao đổi văn bản, tài liệu công vụ (trừ văn bản mật).

- Ưu tiên sử dụng sản phẩm, giải pháp, dịch vụ của doanh nghiệp trong nước đáp ứng yêu cầu về an toàn, an ninh mạng theo quy định của pháp luật đối với các hệ thống thông tin cấp độ 3 trở lên, các hệ thống thông tin phục vụ Chính phủ điện tử;

- Bảo đảm tỷ lệ kinh phí chi cho các sản phẩm, dịch vụ an toàn thông tin mạng đạt tối thiểu 10% trong tổng kinh phí triển khai kế hoạch ứng dụng công nghệ thông tin hàng năm. Đồng thời phối hợp với Sở Thông tin và Truyền thông và các đơn vị liên quan trước khi triển khai việc đầu tư, mua sắm các sản phẩm, dịch vụ về an toàn thông tin mạng.

- 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 về bảo đảm an toàn hệ thống thông tin theo cấp độ, Thông tư số 03/2017/TT-BTTTT ngày 24/02/2017 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 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ. Khẩn trương phân loại, xác định cấp độ an toàn hệ thống thông tin (đối với các hệ thống thông tin chưa được xác định cấp độ an toàn 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. Báo cáo đầy đủ và kịp thời về tình hình bảo đảm an toàn thông tin mạng tại cơ quan, đơn vị, địa phương theo định kỳ hàng năm hoặc khi có yêu cầu.

2. Sở Thông tin và Truyền thông

- Chủ trì, phối hợp với các cơ quan liên quan nghiên cứu tham mưu UBND tỉnh ban hành các văn bản, các kế hoạch bảo đảm an toàn thông tin mạng ngắn và dài hạn. trong hoạt động của cơ quan nhà nước tỉnh Đăk Lăk.

- Tổ chức kiểm tra, đánh giá mức độ bảo đảm an toàn thông tin mạng đối với hệ thống thông tin cấp độ 3 theo hướng dẫn của Bộ Thông tin và Truyền thông; Triển khai hoạt động Đội ứng cứu sự cố an toàn thông tin mạng của tỉnh theo chức năng, nhiệm vụ; Tổ chức đào tạo, tập huấn, nâng cao kỹ năng nghiệp vụ, diễn tập ứng cứu

sự cố an toàn thông tin mạng trên địa bàn tỉnh; Tham mưu, đề xuất UBND tỉnh trong việc mua sắm các trang thiết bị cần thiết đảm bảo Đội hoạt động hiệu quả và đúng quy định.

- Phối hợp, hướng dẫn và hỗ trợ các Sở, ban, ngành cấp tỉnh, UBND cấp huyện trong việc mua sắm các thiết bị về an toàn thông tin, giám sát, rà soát, quét lỗ hổng bảo mật, ứng cứu sự cố đối với Cổng thông tin điện tử và các hệ thống thông tin đang được ứng dụng tại các cơ quan, đơn vị theo quy định.

- Xây dựng phương án, giải pháp bảo đảm an toàn thông tin mạng đối với Trung tâm tích hợp dữ liệu, các hệ thống thông tin dùng chung của tỉnh đang được cài đặt, quản trị, vận hành tại đơn vị (Cổng thông tin điện tử, Hệ thống gửi nhận văn bản, Hệ thống thư điện tử, ...). Đồng thời, xây dựng phương án, kế hoạch để tập trung các cổng/trang thông tin điện tử, các phần mềm, ứng dụng của các cơ quan, đơn vị Nhà nước của tỉnh đang thuê lưu trữ, vận hành ở các doanh nghiệp bên ngoài về lưu trữ, vận hành tại Trung tâm tích hợp dữ liệu của tỉnh.

- Chủ trì triển khai đồng bộ giải pháp kỹ thuật thực hiện giám sát an toàn thông tin tập trung cho các hệ thống thông tin của cơ quan nhà nước tại địa phương; đảm bảo có thể chia sẻ thông tin, dữ liệu thống kê tình hình tấn công mạng, 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 và quy định của pháp luật.

- Tăng cường năng lực của Trung tâm Công nghệ thông tin và Truyền thông để đáp ứng các nhiệm vụ về hỗ trợ, tư vấn xây dựng các giải pháp an toàn thông tin mạng, tư vấn xây dựng hồ sơ cấp độ an toàn thông tin,... cho các cơ quan, đơn vị nhà nước của tỉnh.

- Chỉ đạo các cơ quan Báo chí, Đài Phát thanh và Truyền hình trên địa bàn tăng cường thời lượng phát sóng, bài viết tuyên truyền, phổ biến nâng cao nhận thức cho các tổ chức, người dân về các quy định của pháp luật liên quan đến bảo vệ thông tin cá nhân, đồng thời, luôn cảnh giác, tự bảo vệ mình để tránh bị lợi dụng.

- Tăng cường hoạt động thanh tra, kiểm tra và xử lý nghiêm các hành vi phát tán mã độc, thu thập, lưu trữ, sử dụng trái phép, làm lộ, lọt thông tin cá nhân người dùng trên mạng thuộc địa bàn quản lý.

- Chủ trì đôn đốc, theo dõi thực hiện Chỉ thị này và tổng hợp, báo cáo Chủ tịch UBND tỉnh, UBND tỉnh kết quả thực hiện hàng năm và theo quy định.

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

Chủ trì, phối hợp với Sở Thông tin và Truyền thông, Đội ứng cứu sự cố an toàn thông tin mạng của tỉnh và các cơ quan liên quan thực hiện công tác bảo đảm an ninh mạng trên địa bàn tỉnh. Chủ động thực hiện các nhiệm vụ về đảm bảo an toàn, an ninh mạng theo chức năng.

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

Hàng năm, trên cơ sở dự toán, đề xuất của các cơ quan, đơn vị và khả năng cân đối của ngân sách; Sở Tài chính, Sở Kế hoạch và Đầu tư tham mưu UBND tỉnh xem xét bố trí kinh phí cho hoạt động đảm bảo an toàn thông tin mạng của các cơ quan nhà nước trên địa bàn tỉnh và hoạt động của Đội ứng cứu sự cố an toàn mạng của tỉnh theo quy định.

5. Các Doanh nghiệp cung cấp dịch vụ viễn thông, Internet (ISP) trên địa bàn tỉnh

- Thiết lập, kiện toàn đầu mối đơn vị chuyên trách an toàn thông tin mạng trực thuộc để bảo vệ hệ thống, khách hàng của mình; tham gia hỗ trợ các cơ quan, tổ chức nhà nước giám sát, bảo vệ, kiểm tra, đánh giá an toàn thông tin mạng dưới sự điều phối, hướng dẫn của Bộ Thông tin và Truyền thông, Sở Thông tin và Truyền thông.
- Triển khai các biện pháp kỹ thuật bảo vệ trẻ em trên môi trường mạng theo hướng dẫn của Bộ Thông tin và Truyền thông.

Yêu cầu Thủ trưởng các Sở, ban, ngành; Chủ tịch UBND các huyện, thị xã, thành phố, Giám đốc các Doanh nghiệp cung cấp dịch vụ viễn thông, Internet trên địa bàn tỉnh thực hiện nghiêm túc Chỉ thị này./*bs*

Nơi nhận:

- Bộ TT&TT (b/c);
- Cục An toàn thông tin;
- Thường trực Tỉnh ủy (b/c)
- Thường trực HĐND tỉnh (b/c);
- Chủ tịch, các PCT UBND tỉnh;
- BCĐ xây dựng CQĐT tỉnh;
- Các Sở, ban, ngành cấp tỉnh;
- UBND các huyện, TX, TP;
- Các DN NN trên địa bàn tỉnh
- Lãnh đạo Văn phòng UBND tỉnh;
- Trung tâm TTCB;
- Các DN BCVT trên địa bàn tỉnh;
- Các phòng thuộc Văn phòng: KT, TH, HCTC, Trung tâm TTCB;
- Lưu: VT, KGVX (HVN-60b).

**KT. CHỦ TỊCH
PHÓ CHỦ TỊCH**



Nguyễn Tuấn Hà