

Số: /SCT-VP

Đồng Nai, ngày tháng 7 năm 2024

V/v triển khai hướng dẫn bảo đảm an toàn thông tin mạng cho các Hệ thống thông tin thuộc phạm vi quản lý của Sở Công Thương.

Kính gửi: các phòng, đơn vị trực thuộc Sở.

Sở Công Thương nhận được Văn bản số 2176 /STTTT-CDS của Thông tin và Truyền thông về việc triển khai hướng dẫn bảo đảm an toàn thông tin mạng cho các Hệ thống thông tin thuộc phạm vi quản lý cấp tỉnh.

Sở Công Thương triển khai đến các phòng, đơn vị các nội dung sau:

1. Xác định các hệ thống thông tin thuộc phạm vi quản lý:

Các hệ thống thông tin (Website) thuộc Sở quản lý bao gồm (06 trang):

- Có Server đặt tại Datacenter của tỉnh:

01 trang thông tin điện tử của Sở, 01 trang thông tin điện tử của Trung tâm XTMM; 01 trang thông báo khuyến mại tỉnh Đồng Nai.

- Có Server đặt tại các công ty cho thuê, vận hành Server:

01 trang thông tin điện tử của Trung tâm Khuyến công và Tư vấn phát triển Công nghiệp; 01 trang cơ sở dữ liệu ngành công thương; 01 trang sàn thương mại điện tử tỉnh Đồng Nai.

- Đối với các hệ thống trên, Sở không thực hiện xây dựng hồ sơ cho các hệ thống này. Tuy nhiên, Sở yêu cầu các phòng, đơn vị chủ trì vận hành **hệ thống thông tin có Server đặt tại các công ty cho thuê, vận hành Server** thuộc phạm vi quản lý của đơn vị mình phải triển khai đến đơn vị, công ty cho thuê Server có phương án đảm bảo công tác bảo đảm an toàn thông tin Bộ Thông tin và Truyền thông tại các văn bản: số 2517/BTTTT-CATTT ngày 27/6/2024 về việc hướng dẫn một số giải pháp tăng cường bảo đảm an toàn hệ thống thông tin, số 2596/BTTTT-ATTT ngày 02/7/2024 về việc hướng dẫn bảo đảm an toàn thông tin mạng cho các hệ thống thông tin thuộc phạm vi quản lý cấp bộ, tỉnh. Đồng thời, gửi về Văn phòng Sở để tổng hợp trong tháng 8/2024.

2. Triển khai các biện pháp bảo vệ theo phương án được phê duyệt trong Hồ sơ đề xuất cấp độ:

Đến thời điểm hiện tại, Mạng nội bộ của Sở đã xây dựng hồ sơ đề xuất cấp độ cho Hệ thống thông tin mạng nội bộ và đã được Sở Thông tin và Truyền thông phê duyệt cấp độ an toàn hệ thống thông tin: 02 (cấp độ hai) tại Quyết định số 165/QĐ-STTTT ngày 27/12/2023.

Giao Văn phòng Sở đề xuất, thực hiện các phương án an toàn cho Hệ thống mạng nội bộ, đảm bảo dữ liệu lưu trữ có bản sao lưu dự phòng, kể cả sao lưu dự phòng tại Máy mật trước 15/8/2024.

3. Giao Văn phòng Sở chủ trì, phối hợp với các phòng, đơn vị bảo đảm an toàn thông tin mạng theo mô hình 4 lớp:

- Lực lượng tại chỗ - Lớp 1: Rà soát kiện toàn lực lượng tại chỗ; chỉ định bộ phận chuyên trách về an toàn thông tin thuộc đơn vị; kịp thời cử cán bộ thay thế và thông báo cho Sở Thông tin và Truyền thông để phối hợp thực hiện các nhiệm vụ của Đội Ứng cứu sự cố (Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Đồng Nai được thành lập theo Quyết định số 890/QĐ-UBND ngày 04/4/2024 của Chủ tịch UBND tỉnh Đồng Nai) khi có thay đổi nhân sự.

- Giám sát bảo vệ - Lớp 2: Triển khai đầy đủ biện pháp bảo đảm an toàn thông tin yêu cầu đối với cấp độ của Hệ thống thông tin thuộc phạm vi quản lý của đơn vị theo quy định tại Điều 9, Điều 10 Thông tư 12/2022/TT-BTTTT và theo hướng dẫn tại mục 4.3 phần IV tài liệu Hướng dẫn gửi kèm văn bản số 2596/BTTTT-CATTT.

- Kiểm tra, đánh giá an toàn thông tin - Lớp 3: Cơ quan, đơn vị thực hiện kiểm tra, đánh giá an toàn thông tin theo quy định tại Điều 11, 12 Thông tư số 12/2022/TT-BTTTT và hướng dẫn cụ thể tại mục 4.4 phần IV tài liệu Hướng dẫn gửi kèm văn bản số 2596/BTTTT-CATTT.

- Kết nối, chia sẻ dữ liệu - Lớp 4: Tiếp tục triển khai thực hiện cài đặt hệ thống phòng, chống mã độc và duy trì liên tục, ổn định kết nối, chia sẻ thông tin với Trung tâm Giám sát an toàn không gian mạng quốc gia trực thuộc Cục An toàn thông tin, Bộ Thông tin và Truyền thông theo chỉ đạo của Chủ tịch UBND tỉnh tại văn bản số 12839/UBND-KGVX ngày 28/11/2023.

4. Sử dụng các nền tảng quốc gia hỗ trợ bảo đảm an toàn thông tin mạng.

- Giao Văn phòng Sở chủ trì triển khai, kết nối, sử dụng Nền tảng hỗ trợ quản lý bảo đảm an toàn hệ thống thông tin theo cấp độ (<https://capdo.ais.gov.vn/>) và Nền tảng điều phối xử lý sự cố an toàn thông tin mạng quốc gia và Nền tảng hỗ trợ điều tra số (<https://irlab.vn/>)

Đề nghị Văn phòng Sở triển khai hướng dẫn các phòng, đơn vị vận hành hệ thống thông tin thuộc phạm vi quản lý của mình tạo tài khoản trên ứng dụng Oneconnect; đồng thời tổng hợp danh sách (theo mẫu đính kèm) gửi về Sở Thông tin và Truyền thông để kết nối sử dụng các nền tảng trên.

5. Triển khai 06 giải pháp trọng tâm để tăng cường hiệu quả công tác bảo đảm an toàn thông tin và phục hồi nhanh hoạt động sau sự cố.

- Định kỳ thực hiện sao lưu dữ liệu ngoại tuyến “offline”. Với chiến lược sao lưu dữ liệu theo nguyên tắc 3-2-1: có ít nhất 03 bản sao dữ liệu, lưu trữ bản sao trên 02 phương tiện lưu trữ khác nhau, với 01 bản sao lưu ngoại tuyến

“offline” (sử dụng tape/USB/ổ cứng di động,...). Dữ liệu sao lưu offline phải được tách biệt hoàn toàn, không kết nối mạng, cô lập để phòng chống tấn công leo thang vào hệ thống lưu trữ.

- Triển khai giải pháp để sẵn sàng phục hồi nhanh hoạt động của hệ thống thông tin khi gặp sự cố, đưa hoạt động của hệ thống thông tin trở lại bình thường trong vòng 24 tiếng hoặc theo yêu cầu nghiệp vụ.


- Triển khai các giải pháp, đặc biệt là giải pháp giám sát an toàn thông tin, để ngăn ngừa, kịp thời phát hiện sớm nguy cơ tấn công mạng đối với cả 3 giai đoạn: (1) xâm nhập vào hệ thống; (2) nằm gián điệp trong hệ thống; (3) khởi tạo quá trình phá hoại hệ thống.

- Phân tách, kiểm soát truy cập giữa các vùng mạng và chuyên đổi, nâng cấp các ứng dụng, giao thức, kết nối lạc hậu, không còn được hỗ trợ kỹ thuật sang phương án sử dụng các nền tảng, ứng dụng để giảm thiểu nguy cơ tấn công mạng leo thang.

- Tăng cường giám sát, quản lý các tài khoản quan trọng, tài khoản quản trị để phòng ngừa, giảm thiểu thiệt hại trong trường hợp kẻ tấn công có được tài khoản quản trị.

- Rà soát, khắc phục và không để xảy ra các lỗi cơ bản dẫn đến mất an toàn hệ thống thông tin. *(Hướng dẫn chi tiết tại phụ lục kèm theo công văn số 2517/BTTTT-CATT ngày 27/6/2024 của Bộ Thông tin và Truyền thông).*

Sở Công Thương triển khai cho các phòng, đơn vị biết, tổ chức thực hiện đảm bảo an toàn hệ thống thông tin./.

Đính kèm: Văn bản số 2517/BTTTT-CATT ngày 27/6/2024, số 2596/BTTTT-CATT ngày 02/7/2024 của Bộ Thông tin và Truyền thông. 

Nơi nhận:

- Như trên;
 - Sở TTTT (báo cáo);
 - Ban Giám đốc Sở;
 - Lưu: VT, CNTT.
- Thuymtt

GIÁM ĐỐC

Phạm Văn Cường