UBND TỈNH TÂY NINH
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập – Tự do – Hạnh phúc

Số: 758 /BC-STTTT

Tây Ninh, ngày 23 tháng 4 năm 2024

BÁO CÁO
Công tác đảm bảo an toàn thông tin (ATTT) tại Trung tâm tích hợp dữ liệu (TTTHDL) và trên địa bàn tỉnh

Kính gửi: Ủy ban nhân dân tỉnh

Căn cứ Công điện số 33/CĐ-TTg ngày 07/4/2024 của Thủ tướng Chính phủ về tăng cường đảm bảm an toàn thông tin mạng;

Căn cứ Công văn số 1465/BTTTT-CATTT ngày 17/4/2024 của Bộ Thông tin và Truyền thông về tăng cường công tác đảm bảo an toàn thông tin trong dịp Lễ 30/4, 01/5 và 70 năm chiến thắng Điện Biên Phủ;

Thực hiện chỉ đạo của Lãnh đạo UBND tỉnh tại Công văn số 3361/VP-TTCBTH ngày 22/4/2024, trong đó giao Sở Thông tin và Truyền thông chủ trì, phối hợp các đơn vị liên quan triển khai thực hiện các nội dung chỉ đạo của Bộ Thông tin và Truyền thông tại Công văn số 1465/BTTTT-CATTT,

Sở Thông tin và Truyền thông báo cáo UBND tỉnh một số nội dung về công tác đảm bảo an toàn thông tin cho người dùng và TTTHDL của tỉnh hiện nay, cụ thể như sau:

I. TÌNH HÌNH AN TOÀN THÔNG TIN THỜI GIAN QUA

Trong Quý I/2024, các hệ thống thông tin của tỉnh cơ bản hoạt động ổn định, xuyên suốt, không có xảy ra sự cố bị tấn công mạng làm ảnh hưởng đến các hệ thống thông tin đang hoạt động tại TTTHDL. Tuy nhiên qua nhật ký của hệ thống bảo mật, ghi nhận mỗi ngày trung bình phát hiện và ngăn chặn nhiều lượt dò quét, tấn công vào các hệ thống của tỉnh đang được công khai trên môi trường Internet *(tấn công từ chối dịch vụ (DDos) khoản 15.230.272 lượt, tấn công nhằm và các hệ cơ sở dữ liệu (SQL Injection) khoản 1.927.757 lượt,...)*. Qua đó cho thấy, mối đe dọa mất an toàn thông tin cho các hệ thống thông tin tại TTTHDL là rất lớn.

Phần mềm phòng chống mã độc triển khai cho các máy tính trên địa bàn tỉnh đạt hiệu quả, góp phần ngăn chặn tình trạng lây nhiễm mã độc cho người dùng tại các cơ quan,. Trong Quý I/2024, phần mềm phòng chống mã độc tập

trung phát hiện và đã xử lý 515 máy nhiễm mã độc và 82 máy thực hiện truy cập đến các địa chỉ độc hại.

Bên cạnh đó, Sở Thông tin và Truyền thông đã kịp thời thực hiện tiếp nhận và xử lý 4 văn bản cảnh báo lỗ hổng bảo mật từ Cục An toàn thông tin. Cụ thể:

+ *Công văn số 66/CATTT-NCSC về việc lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 01/2024.*

+ *Công văn số 210/CATTT-NCSC về việc lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 02/2024.*

+ *Công văn số 364/CATTT-NCSC về việc lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 03/2024.*

+ *Công văn số 424/CATTT-NCSC về việc rà soát dấu hiệu của các chiến dịch tấn công có chủ đích (APT).*

II. TÌNH HÌNH TUÂN THỦ CÁC QUY ĐỊNH VỀ ATTT

1. Đảm bảo ATTT theo cấp độ.

Hiện nay, TTTHDL của tỉnh đạt Hệ thống thông tin cấp độ 3 theo Quyết định số 137/QĐ-UBND của UBND tỉnh ban hành ngày 17/01/2019. Trong đó các tiêu chí đảm bảo an toàn, an ninh mạng tại Công văn số 708/BTTTTCATTT dành cho Hệ thống thông tin cấp độ 3 là 16 tiêu chí, TTTHDL của tỉnh cơ bản đáp ứng đủ 16 tiêu chí, tuy nhiên có một số tiêu chí chưa đảm bảo hiệu quả về tính năng. Cụ thể:

+ ***Tiêu chí đảm bảo an toàn cho máy chủ dữ liệu:*** đang triển khai dùng thử giải pháp phần mềm Imperva, đã hết hạn bản quyền dùng thử. Sở dự kiến xin ý kiến chủ trương thực hiện gia hạn hoặc đầu tư năm 2025.

+ ***Tiêu chí có phương án quản lý phần mềm phòng chống mã độc trên máy chủ/máy tính người dùng*:** đang sử dụng phần mềm phòng chống mã độc BKAV Endpoint, đã hết hạn bản quyền, việc gia hạn hoặc triển khai cài đặt mới Sở sẽ thực hiện năm 2024.

+ ***Tiêu chí có phương án, chống thất thoát dữ liệu:*** tích hợp cùng giải pháp BKAV Endpoint, đã hết hạn bản quyền, việc thực hiện gia hạn hoặc triển khai cài đặt mới năm 2024 cùng với phần mềm phòng chống mã độc.

Tại Chỉ thị số 09/CT-TTg ngày 23/02/2024 của Thủ tướng Chính phủ về việc tuân thủ quy định pháp luật và tăng cường bảo đảm an toàn hệ thống thông tin theo cấp độ. Theo đó, nhiều cơ quan, địa phương chưa thấy hết trách nhiệm,

tầm quan trọng trong việc tuân thủ quy định của pháp luật về bảo đảm ATTT theo cấp độ.

Sở Thông tin và Truyền thông đã ban hành văn bản hướng dẫn xây dựng hồ sơ đề xuất cấp độ, các quy định tiêu biểu về ATTT theo cấp độ. Tuy nhiên, còn nhiều cơ quan chưa triển khai các giải pháp để thực hiện, chưa quan tâm trong việc xây dựng đề xuất hồ sơ phê duyệt các hệ thống thông tin theo cấp độ.

2. Đảm bảo an toàn thông tin theo mô hình 04 lớp

Về lực lượng ứng cứu sự cố máy tính tại chỗ: Sở Thông tin và Truyền thông đã tham mưu UBND tỉnh kiện toàn Đội Ứng cứu sự cố an toàn thông tin mạng của tỉnh tại Quyết định số 436/QĐ-UBND ngày 10/3/2023 của UBND tỉnh với 56 thành viên, là lãnh đạo, cán bộ phụ trách công nghệ thông tin tại các cơ quan, đơn vị và một số doanh nghiệp trên địa bàn tỉnh.

Giám sát An toàn thông tin: Trung tâm giám sát an ninh mạng (SOC) thực hiện phương án giám sát hệ thống 24/7 nhằm kịp thời phát hiện và xử lý các hành vi tấn công mạng.

Kiểm tra, đánh giá an toàn thông tin các hệ thống tại TTTHDL: Sở thường xuyên tổ chức định kỳ kiểm tra, đánh giá an toàn thông tin cho các hệ thống thông tin đang hoạt động tại TTTHDL tỉnh. Việc đánh giá sẽ được tiếp tục thực hiện trong năm 2024.

Chia sẻ kết nối dữ liệu mã độc: Sở Thông tin và Truyền thông đã triển khai cài đặt hệ thống phần mềm phòng chống mã độc cho các đơn vị hành chính nhà nước trên toàn tỉnh, thực hiện chia sẻ dữ liệu mã độc với Trung tâm Giám sát không gian mạng ổn định. Việc chia sẻ tiếp tục thực hiện sau khi triển khai gia hạn hoặc cài mới phần mềm phòng chống mã độc năm 2024.

3. Công tác đảm bảo an toàn thông tin cho người dùng, TTTHDL

Trong giai đoạn tấn công mạng đang tăng cao như hiện nay, đặc biệt là tấn công mã hóa dữ liệu tống tiền (Ransomware). Sở Thông tin và Truyền thông cũng đã kịp thời ban hành Công văn số 626/STTTT-TTGSĐH ngày 04/4/2024 về việc tăng cường bảo đảm an toàn thông tin, nâng cao cảnh giác đối với các hình thức tấn công mã hoá dữ liệu. Qua đó giúp người dùng có thêm thông tin nâng cao cảnh giác cho việc đảm bảo ATTT của người dùng và cho các hệ thống của các đơn vị.

Sở Thông tin và Truyền thông tăng cường thực hiện giám sát, theo dõi hoạt động của các hệ thống. Khi có sự cố sẽ thực hiện quy trình ứng cứu sự cố theo quy định.

Kịp thời thực hiện các thông báo, hướng dẫn liên quan về công tác đảm bảo an toàn thông tin của Bộ Thông tin và Truyền thông cho các đơn vị trên địa bàn tỉnh, TTTHDL của tỉnh:

+ *Công văn số 216/STTTT-TTGSĐH ngày 29/01/2024 về việc cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 01/2024.*

+ *Công văn số 390a/STTTT-TTGSĐH ngày 01/3/2024 về việc cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 02/2024.*

+ *Công văn số 556/STTTT-TTGSĐH ngày 25/3/2024 về việc cảnh báo lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 3/2024.*

+ *Công văn số 424/CATTT-NCSC ngày 22/3/024 của Cục An toàn thông tin về việc rà soát dấu hiệu của các chiến dịch tấn công có chủ đích (APT).*

+ *Công văn số 738/STTTT-TTGSĐH ngày 22/4/2024 về việc cảnh báo lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 4/2024*

Giám sát chặt chẽ, công việc thực hiện sao lưu dữ liệu các hệ thống đề phòng trường hợp khi có sự cố xảy ra liên quan đến dữ liệu các hệ thống TTTHDL.

Thực hiện lập kế hoạch rà soát, các chính sách truy cập ra vào các hệ thống của TTTHDL; Cập nhật bản vá cho hệ điều hành các hệ thống; Thay đổi mật khẩu quản trị các hệ thống, thiết bị, phần mềm; Quét mã độc cho các hệ thống.

III. TỒN TẠI HẠN CHẾ.

Người dùng chưa đánh giá hết khả năng mức độ thiệt hại của các cuộc tấn công tiềm ẩn nguy hiểm như ransomware,... dẫn đến việc còn chủ quan trong công tác đảm bảo ATTT.

Các hệ thống thông tin đôi khi bị gián đoạn khi TTTHDL bị tấn công từ chối dịch vụ (DDos) với quy mô lớn. Dù đã đầu tư thiết bị phòng chống nhưng chưa đảm bảo hiệu năng.

Công tác phòng ngừa mất ATTT đối với các hệ thống triển khai cài đặt mới tại TTTHDL chưa đảm bảo, do cán bộ quản trị chưa đủ công cụ để thực hiện đánh giá.

Kinh phí dành cho ATTT *(bản quyền thiết bị bảo mật, dịch vụ đánh giá ATTT, tổ chức diễn tập thực chiến, đánh giá ATTT các hệ thống hoạt động tại TTTHDL,...)* còn hạn chế dẫn đến cho các giải pháp dịch vụ, đầu tư công cụ, thiết bị cho ATTT chưa đạt hiệu quả cao.

Các thành viên Đội Ứng cứu sự cố an toàn thông tin mạng của tỉnh phải thực hiện kiêm nhiệm nhiệm vụ; Không có cán bộ chuyên trách có chuyên môn, kiến thức sâu về lĩnh vực ATTT nên công tác ứng cứu sự cố còn nhiều bất cập.

Cán bộ quản trị trực tiếp TTTHDL phải thực hiện nhiệm vụ kiêm nhiệm, dẫn đến công tác thực hiện nhiệm vụ chuyên môn bị ảnh hưởng.

IV. GIẢI PHÁP THỰC HIỆN

Trong thời gian tới, Sở Thông tin và Truyền thông sẽ tham mưu UBND thực hiện các giải pháp nhằm đảm bảo ATTT cho các hệ thống đang hoạt động tại TTTHDL để đáp ứng các tiêu chí hệ thống thông tin cấp độ 3 theo quy định của Bộ TTTT. Qua đó đảm bảo công tác ATTT cho TTTHDL..

Bên cạnh đó, để tăng cường vai trò cán bộ quản trị của các đơn vị trên địa bàn tỉnh. Sở Thông tin và Truyền thông cũng sẽ tham mưu UBND tỉnh các quy chế liên quan về việc phân cấp, phân quyền quản trị các hệ thống mạng tại các đơn vị trong thời gian tới.

Về phía người dùng, Sở sẽ tăng cường công tác tuyên truyền, phổ biến trên nhiều kênh truyền thông *(mạng xã hội, báo chí,...)* qua đó giúp người dùng dễ dàng tiếp cận các vấn đề liên quan đến ATTT hiện nay..

Trên đây là báo cáo công tác đảm bảo an toàn thông tin (ATTT) tại Trung tâm tích hợp dữ liệu (TTTHDL) và trên địa bàn tỉnh của Sở Thông tin và Truyền thông. Kính báo cáo UBND tỉnh.

***Nơi nhận*:**
- BCĐ đột phá tỉnh (báo cáo);
- Cục ATTT - Bộ TTTT (báo cáo);
- BCĐ Chuyển đổi số tỉnh (b/c);
- Sở, ban, ngành tỉnh;
- UBND huyện, thị xã, thành phố;
- Lưu: VT, TTGSĐH.

GIÁM ĐỐC

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH TÂY NINH

Nguyễn Tấn Đức