UBND TỈNH TÂY NINH
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 626 /STTTT-TTGSĐH
V/v tăng cường bảo đảm an toàn thông tin, nâng cao cảnh giác đối với các hình thức tấn công mã hoá tống tiền (Ransomware).

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

Tây Ninh, ngày 04 tháng 4 năm 2024

Kính gửi:
- Văn phòng Tỉnh ủy;
- Văn phòng Đoàn ĐBQH và HĐND tỉnh;
- Văn phòng UBND tỉnh;
- Các cơ quan tham mưu, giúp việc Tỉnh ủy;
- Mặt trận Tổ quốc và các Đoàn thể chính trị - xã hội;
- Các Sở, ban, ngành tỉnh;
- Các đơn vị ngành dọc;
- Các huyện, thị, thành ủy trực thuộc Tỉnh ủy;
- UBND các huyện, thị xã, thành phố;
- UBND các xã, phường, thị trấn.

Qua theo dõi, giám sát không gian mạng của Cục An toàn thông tin (Bộ Thông tin và Truyền thông) phát hiện xu hướng tấn công mạng, đặc biệt là mã hóa tấn công tống tiền (Ransomware) đang có dấu hiệu ngày càng tăng cao. Trong thời gian gần đây, đã có một số hệ thống thông tin của cơ quan, tổ chức, doanh nghiệp tại Việt Nam bị sự cố tấn công, gây gián đoạn hoạt động và thiệt hại về vật chất, hình ảnh của các cơ quan, tổ chức, doanh nghiệp, cũng như hoạt động bảo đảm an toàn không gian mạng quốc gia. Điển hình:

- Ngày 25/03/2024, hệ thống thông tin của Tổng công ty cổ phần Bảo hiểm bưu điện (PTI) và Công ty CP Chứng khoán VNDirect bị tấn công Ransomware.

- Ngày 02/4/2024, hệ thống thông tin của Tổng công ty Dầu Việt Nam (PVOIL) cũng bị tấn công với hình thức tương tự.

Ransomware là hình thức tấn công rất nguy hiểm. Các máy tính, hệ thống thông tin khi bị tấn công thành công sẽ bị mã hóa toàn bộ dữ liệu có trên máy tính và tin tặc sẽ tiếp tục thực hiện tấn công lây nhiễm mã hóa dữ liệu các máy tính khác trong cùng hệ thống mạng. Việc giải mã khôi phục lại dữ liệu cho máy tính khi đã bị mã hoá gần như không thể thực hiện, nếu muốn khôi phục người dùng sẽ phải bỏ ra một chi phí rất lớn để trả cho tin tặc.

Hậu quả tấn công Ransomware mang lại cho người dùng, các hệ thống thông tin là rất nghiệm trọng. Do đó, để tăng cường đảm bảo an toàn thông tin, nâng cao cảnh giác cho người dùng, hệ thống thông tin cơ quan đơn vị nói riêng và toàn bộ các hệ thống thông tin đang hoạt động tại Trung tâm tích hợp dữ liệu

của tỉnh nói chung, Sở Thông tin và Truyền thông đề nghị các đơn vị trên địa bàn tỉnh nghiêm túc thực hiện các công việc nội dung cụ thể như sau:

1. Tuyệt đối không thực hiện truy cập các trang web, đường link lạ qua trình duyệt web (Chrome, Firefox,…), qua email cá nhân hoặc bất kỳ hình thức nào khi chưa biết rõ chính xác thông tin.

2. Không cài đặt các phần mềm với các công cụ bẻ khóa không rõ nguồn gốc được tải trên mạng Internet cho máy tính người dùng, máy chủ.

3. Thực hiện cài đặt, cập nhật dữ liệu mới nhất cho phần mềm phòng chống mã độc; Thường xuyên thực hiện rà quyết mã độc cho máy tính người dùng, máy chủ các hệ thống.

4. Thực hiện sao lưu dữ liệu trên máy tính cá nhân, sao lưu dữ liệu các hệ thống thông tin trong phạm vi quản lý, lưu trữ tại nhiều nơi để có thể phục hồi khi máy tính hoặc hệ thống thông tin bị tấn công mã hóa dữ liệu.

5. Kiểm tra, cập nhật các bản vá lỗ hổng bảo mật mới nhất cho các hệ điều hành của máy tính, máy chủ đang sử dụng.

6. Thực hiện tuyên truyền, phổ biến tăng cường nâng cao cảnh giác cho người thân, gia đình và bạn bè.

7. Trường hợp phát hiện các tập tin máy tính bị mã hóa dữ liệu tống tiền (*tên tập tin hiển thị với dạng khác lạ*) người dùng thực hiện tắt ngay máy tính và liên hệ cán bộ phụ trách công nghệ thông tin hoặc Sở Thông tin và Truyền thông để cùng phối hợp kiểm tra.

Trong quá trình thực hiện nếu có vướng mắc liên hệ: Phòng Hạ tầng và An toàn thông tin mạng – Trung tâm Giám sát, điều hành kinh tế, xã hội tập trung - Điện thoại: 0276.3611169 – Email: hotro@tayninh.gov.vn

Trân trọng./.

Nơi nhận:
- Như trên;
- BGĐ Sở (để b/c);
- Lưu: VP, TTGSĐH.

KT.GIÁM ĐỐC
PHÓ GIÁM ĐỐC

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

Nguyễn Trung Hiếu