UBND TỈNH ĐẮK LẮK
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 665 /STTTT-CNTT
V/v cảnh báo hình thức lây, nhiễm của mã độc mã hóa tài liệu tống tiền (ransomware)

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

Đắk Lắk, ngày 07 tháng 10 năm 2016

Kính gửi:

- Văn phòng Tỉnh ủy;
- Văn phòng Đoàn ĐBQH và HĐND tỉnh;
- Văn phòng UBND tỉnh;
- Các Sở, ban, ngành và đoàn thể của tỉnh;
- UBND các huyện, Thị xã, Thành phố.

Trong thời gian qua tình hình lây nhiễm mã độc mã hóa tài liệu và tống tiền (ransomware) trong máy tính cá nhân và máy chủ trên địa bàn tỉnh đang diễn biến phức tạp, hiện tại ngày càng gia tăng. Sở Thông tin và Truyền thông đã ghi nhận, phát hiện nhiều trường hợp bị nhiễm, việc phục hồi tài liệu cho các máy bị nhiễm không thể thực hiện được nếu không có khóa để giải mã tài liệu.

Các cơ quan, đơn vị đã bị lây, nhiễm được ghi nhận trong thời gian qua trên địa bàn tỉnh là: Văn phòng UBND tỉnh, các Sở: Tài nguyên và Môi trường, Ngoại vụ, Thông tin và Truyền thông... Để bảo đảm công tác an toàn thông tin dữ liệu trong hoạt động ứng dụng công nghệ thông tin của các cơ quan, đơn vị trên địa bàn tỉnh, Sở Thông tin và Truyền thông đề nghị các cơ quan, đơn vị phổ biến, thực hiện một số biện pháp sau để phòng tránh sự lây, nhiễm của loại vi rút mã độc này như sau:

1. Phòng ngừa, hạn chế tối đa khả năng bị nhiễm mã độc:

- Cài đặt và thường xuyên cập nhật cho hệ điều hành, phần mềm chống mã độc như Kaspersky, Symantec, Avast, AVG, MSE, Bkav, CMC,...;
- Chú ý cảnh giác với các tập tin đính kèm, các đường liên kết ẩn được gửi đến trong thư điện tử người dùng (kể cả người gửi từ trong nội bộ);
- Thực hiện các biện pháp kỹ thuật nhằm kiểm tra xác thực người dùng trên máy chủ gửi email của đơn vị, tránh bị giả mạo người gửi từ nội bộ, không mở những tập tin đính kèm lạ, khả nghi.
- Tắt các chế độ tự động mở, chạy tập tin đính kèm theo thư điện tử.

2. Thực hiện sao lưu dữ liệu định kỳ: sử dụng các ổ đĩa lưu trữ như Ổ cứng cắm ngoài, Ổ đĩa USB để lưu trữ các dữ liệu quan trọng trong máy tính. Sau khi sao lưu xong đưa ra cất giữ riêng. Sử dụng các công cụ, giải pháp chuyên dụng để sao lưu dữ liệu như các máy chủ quản lý tập tin, máy chủ sao lưu từ xa, các công cụ lưu trữ đám mây cho phép khôi phục lịch sử thay đổi của tập tin.

3. Xử lý khi phát hiện lây nhiễm mã độc: Khi mã độc lây nhiễm vào máy tính, mã độc sẽ tiến hành quét và mã hóa các tập tin trong một khoảng thời gian. Do đó, việc phản ứng nhanh khi phát hiện ra sự cố có thể giúp giảm thiểu thiệt

hại cho dữ liệu trên máy tính và tăng khả năng khôi phục dữ liệu bị mã hóa. Cụ thể, cần thực hiện các thao tác sau:

- Bước 1: Nhanh chóng tắt máy tính bằng cách ngắt nguồn điện.
- Bước 2: Không được khởi động lại máy tính theo cách thông thường mà phải khởi động từ hệ điều hành sạch khác (khuyến nghị hệ điều hành Linux) như từ ổ đĩa CD, USB.
- Bước 3: Thực hiện kiểm tra các tập tin dữ liệu và sao lưu các dữ liệu chưa bị mã hóa; các tập tin đã bị mã hóa tương đối khó để giải mã, tuy nhiên trong một số trường hợp có thể sử dụng phần mềm khôi phục dữ liệu như FTK, EaseUs, R-STUDIO,...để khôi phục các tập tin nguyên bản đã bị xóa.
- Bước 4: Cài đặt lại hệ điều hành cho máy tính bị nhiễm, cài đặt phần mềm diệt virus đồng thời thiết lập chế độ cập nhật phiên bản tự động.

Trong quá trình thực hiện, nếu có vướng mắc xin liên hệ: Phòng Công nghệ thông tin, Sở Thông tin và Truyền thông; địa chỉ: 08 Lý Thái Tổ, Tp. Buôn Ma Thuột; ĐT: 0500.3557888; Email: phongcntt@tttt.daklak.gov.vn./.

Nơi nhận:
- Như trên;
- GĐ, các PGĐ;
- Phòng VHTT các huyện, TX, TP;
- Lưu VT, CNTT.

GIÁM ĐỐC

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH ĐẮK LẮK

Trần Trung Hiếu