UBND TỈNH ĐIỆN BIÊN
SỞ CÔNG THƯƠNG

Số: 1201/SCT-VP
V/v tăng cường phòng ngừa tấn công mạng bằng virus mã hóa dữ liệu và đòi tiền chuộc

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

Điện Biên, ngày 11 tháng 8 năm 2022

Kính gửi:
- Các phòng Chuyên môn nghiệp vụ Sở;
- Các đơn vị trực thuộc Sở.

Sở Công Thương nhận được văn bản số 2265/CV-TBATANM ngày 03 tháng 8 năm 2022 của Tiểu ban an toàn an ninh mạng về việc phòng ngừa tấn công mạng bằng virus mã hóa dữ liệu và đòi tiền chuộc.

Để kịp thời triển khai các giải pháp đảm bảo an toàn, an ninh mạng, chủ động phòng ngừa, ngăn chặn hoạt động tấn công mạng của các nhóm tin tặc, hacker. Sở Công Thương yêu cầu các phòng và đơn vị thực hiện các nội dung sau:

1. Tăng cường các biện pháp phòng ngừa, hạn chế tối đa khả năng bị nhiễm mã độc.

- Cài đặt hệ điều hành win 10 trở lên và thường xuyên cập nhật phiên bản mới nhất của hệ điều hành win 10;

- Cài đặt phần mềm diệt virus có bản quyền *(Kaspersky, Synmantec, Avast, AVG, MSE, BKAV, CMC,...)*, có chức năng đảm bảo an toàn khi truy cập mạng Internet và phát hiện mã độc trực tuyến. Thường xuyên cập nhật phiên bản mới nhất cho phần mềm diệt virus;

- Các máy tính đang sử dụng hệ điều hành win 10, đã cài đặt phần mềm diệt virus BKAV Endpoint đề nghị thường xuyên cập nhật phiên bản mới phần mềm diệt virus;

- Cần chú ý cảnh giác với các tệp tin đính kèm, các đường dẫn *(link)* được gửi đến qua thư điện tử hoặc tin nhắn, hạn chế tối đa việc truy cập vào các đường dẫn này vì tin tặc có thể đánh cắp hoặc giả mạo hòm thư điện tử người gửi phát tán các kết nối chứa mã độc.

- Sử dụng phần mềm diệt virus kiểm tra các tập tin được gửi qua thư điện tử, tải từ trên mạng về trước khi mở. Nếu không cần thiết hoặc không rõ nguồn gốc thì không mở các tập tin này.

Ví dụ: mở 01 trình duyệt đang sử dụng trên máy tính *(Chrome, Cốc Cốc, Firefox)* copy đường link sau: https://www.virustotal.com/gui/home/upload vào trình duyệt và truy cập. Nhấn "Choose file" chọn đến file cần quét (Trang virustotal.com sẽ kiểm tra file cần quét và cảnh báo nếu có chữa mã độc).

- Tắt chế độ tự động mở, chạy các tệp đính kèm theo thư điện tử.

2. Tiến hành sao lưu định kỳ thường xuyên để có thể khôi phục dữ liệu khi máy tính bị Ransomware gây hại.

- Sử dụng đĩa CD ROM, DVD ROM để sao lưu dữ liệu là phương pháp đơn giản và an toàn, tuy nhiên không được thuận tiện khi sử dụng lâu dài và thường xuyên.

- Sử dụng các ổ lưu trữ USB, ổ đĩa cắm ngoài, ổ chia sẻ mạng v.v... Cần chú ý dữ liệu trong các ổ lưu trữ này hoàn toàn có thể bị ảnh hưởng nếu kết nối vào máy tính đã bị nhiễm mã độc Ransomware. Do vậy phải đảm bảo máy chưa bị nhiễm mã độc trước khi sao lưu hoặc khởi động máy tính từ ổ đĩa khởi động ngoài khi thực hiện sao lưu để đảm bảo an toàn.

- Sử dụng các công cụ, giải pháp chuyên dụng để sao lưu như: các máy chủ quản lý tệp 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 mà khi xảy ra sự cố có thể khôi phục lại từ thời điểm trước đó.

3. Xử lý khi phát hiện bị lây nhiễm mã độc: Khi mã độc Ransomware lây nhiễm vào máy tính bị hại, mã độc sẽ tiến hành mã hóa các tệp tin dữ liệu, khóa máy tính của người dùng để người dùng không can thiệp để tắt tiến trình đang chạy. Do quá trình mã hóa cần sẽ được thực hiện trong thời gian dài chính vì vậy việc phản ứng nhanh chóng khi phát hiện ra sự cố sẽ giúp giảm thiểu thiệt hại cho các dữ liệu chứa trên máy bị nhiễm và giúp các chuyên gia có thể khôi phục các dữ liệu bị mã hóa. Do đó, đối với các máy tính cá nhân khi phát hiện ra dấu hiệu bị lây nhiễm mã độc Ransomware cần phải nhanh chóng thực hiện các thao tác sau:

- Nhanh chóng tắt máy tính (Tắt nguồn điện, không sử dụng chức năng shutdown của hệ điều hành).

- Phải sử dụng khởi động từ hệ thống sạch khi thực hiện sao lưu các dữ liệu chưa bị mã hóa.

- Trong trường hợp không cần cứu dữ liệu, cần format ổ cứng và cài đặt lại toàn bộ hệ thống, cài phần mềm diệt virus cập nhật phiên bản mới nhất và tiến hành quét toàn bộ dữ liệu trên máy tính trước khi sao chép lại các dữ liệu vào máy tính.

Khi phát hiện xảy ra sự cố về mã độc Ransomware cần liên hệ với Công an tỉnh (qua phòng An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao Công an tỉnh, số điện thoại: 0692.489.489).

Trong quá trình thực hiện nếu có vướng mắc các phòng, đơn vị kịp thời thông tin về Sở (trực tiếp liên hệ với đ/c Trần Khánh Toàn, chuyên viên Văn phòng Sở) điện thoại cơ quan 0215.3.826.933; di động 0834272613 để được hỗ trợ./.

Nơi nhận:
- Như trên;
- Tiêu ban an toàn an ninh mạng;
- Các đ/c Lãnh đạo Sở;
- Lưu: VT, VP.

GIÁM ĐỐC

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ CÔNG THƯƠNG
TỈNH ĐIỆN BIÊN

Vũ Hồng Sơn