UBND TỈNH HƯNG YÊN
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số: 271/STTTT-CNTT
V/v cảnh báo lây nhiễm mã độc WannaCry trong hệ thống mạng

Hưng Yên, ngày 15 tháng 5 năm 2017

Kính gửi: - Văn phòng UBND tỉnh;
- Các sở, ban, ngành;
- UBND các huyện, thành phố.

Hiện nay, mã độc có tên là WannaCry chuyên khai thác một số lỗ hổng trên hệ điều hành Windows để tấn công vào các máy tính với mục tiêu mã hóa dữ liệu để đòi tiền chuộc gây ảnh hưởng tới nhiều cơ quan, tổ chức và cá nhân trên phạm vi toàn cầu trong tuần vừa qua và mã độc này đã xuất hiện tại Việt Nam. Trước nguy cơ có thể gây mất an toàn thông tin cho các máy tính tại Việt Nam, Cục An toàn thông tin – Bộ Thông tin và Truyền thông, Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam đã hướng dẫn thực hiện biện pháp xử lý khẩn cấp mã độc này và phát đi lệnh cảnh báo tới các tổ chức, cá nhân.

Để phòng ngừa, ngăn chặn việc tấn công của mã độc WannaCry trên diện rộng trong hệ thống mạng của các cơ quan nhà nước và các tổ chức, cá nhân trên địa bàn tỉnh. Sở Thông tin và Truyền thông đề nghị các sở, ban, ngành và UBND các huyện, thành phố khẩn trương triển khai một số biện pháp xử lý khẩn cấp nhằm đảm bảo an toàn, an ninh thông tin trong hoạt động của các cơ quan, đơn vị, cụ thể như sau:

1. Sử dụng chức năng "*Check for updates*" của hệ điều hành Windows để thực hiện cập nhật ngay đối với các phiên bản hệ điều hành Windows đang sử dụng. Riêng đối với các máy tính sử dụng hệ điều hành Windows XP, cập nhật bản vá lỗ hổng bảo mật EternalBlue (MS17-010) mới nhất hoặc tìm kiếm theo từ khóa bản cập nhật KB4012598 trên trang chủ của Microsoft. Cài đặt và cập nhật ngay các chương trình Antivius bản quyền cho các máy tính đang sử dụng.

2. Không mở thư điện tử (email) có đính kèm và các liên kết (link) lạ được gửi trong email, trên các mạng xã hội, công cụ gửi tin (chat)…cần thận trọng trước khi mở các file đính kèm ngay cả khi nhận được từ những địa chỉ người quen. Không mở các đường dẫn có đuôi .hta hoặc đường dẫn có cấu trúc không rõ ràng, các đường dẫn rút gọn link.

3. Sử dụng các ổ đĩa lưu trữ ngoài như ổ cứng cắm ngoài, ổ đĩa USB (không chứa vi rút) để lưu trữ các dữ liệu quan trọng trong máy tính. Sau khi sao lưu xong đưa ra cất giữ riêng và không kết nối vào internet.

4. Yêu cầu cán bộ chuyên trách công nghệ thông tin của đơn vị thực hiện kiểm tra, rà soát toàn bộ hệ thống mạng nội bộ bao gồm tất cả các máy chủ, máy trạm nhằm phát hiện và xử lý kịp thời sự cố xảy ra; nhanh chóng ngắt kết nối mạng và cô lập máy tính bị nhiễm. Đối với các máy chủ cần kiểm tra và tạm thời khóa (block) các dịch vụ đang sử dụng các cổng 445/137/138/139;

5. Có thể thực hiện các bước kiểm tra mã độc theo hướng dẫn tại địa chỉ *http://www.vncert.gov.vn/baiviet.php?id=59* hoặc công cụ miễn phí của Bkav (*được cung cấp trên trang http://bkav.com.vn*) để thực hiện quét các máy tính trong toàn bộ hệ thống mạng của đơn vị.

Đây là loại mã độc rất nguy hiểm, có thể đánh cắp thông tin và mã hóa toàn bộ hệ thống máy tính gồm cả máy chủ, máy trạm. Sở Thông tin và Truyền thông đề nghị các sở, ban, ngành và UBND các huyện, thành phố khẩn trương triển khai, tổ chức thực hiện ngay các yêu cầu trên. Trong quá trình triển khai, nếu có vướng mắc đề nghị liên hệ với Phòng Công nghệ thông tin, Sở Thông tin và Truyền thông, điện thoại: 03213.867093; thư điện tử: cntt.stttt@hungyen.gov.vn để được hướng dẫn, giải đáp./.

(Quý cơ quan tham khảo thêm thông tin chi tiết đăng tải trên Cổng thông tin điện tử của Sở Thông tin và Truyền thông http://sotttt.hungyen.gov.vn hoặc của Trung tâm ứng cứu khẩn cấp máy tính Việt Nam http://vncert.gov.vn)./.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HOÀ XH CHỦ NGHĨA VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH HƯNG YÊN

Đỗ Đình Quang

Nơi nhận:
- Như kính gửi;
- UBND tỉnh (b/c);
- Giám đốc; Phó Giám đốc(đ/c Quang);
- Trung tâm CNTT&TT (để p/h);
- Lưu: VT, CNTT.