ỦY BAN NHÂN DÂN **HUYỆN GIA LÂM**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 2377 /UBND-VHTT V/v cảnh báo rủi ro an toàn thông tin liên quan đến phần mềm của hãng CrowdStrike	*Gia Lâm, ngày 29 tháng 7 năm 2024*

Kính gửi:
- Các phòng, ban, đơn vị, trường học thuộc Huyện;
- UBND các xã, thị trấn.

Căn cứ Công văn số 2100/STTTT-ATTTT&GDĐT ngày 23/7/2024 của Sở Thông tin và Truyền thông Hà Nội về việc cảnh báo rủi ro an toàn thông tin liên quan đến phần mềm của hãng CrowdStrike. Nhằm đảm bảo an toàn thông tin cho các hệ thống, UBND huyện yêu cầu các cơ quan, đơn vị, trường học, UBND các xã, thị trấn thuộc Huyện thực hiện một số nội dung sau:

1. Kiểm tra, rà soát hệ thống thông tin đang sử dụng có khả năng bị ảnh hưởng bởi rủi ro an toàn thông tin trên. Chủ động theo dõi các thông tin liên quan nhằm thực hiện khắc phục rủi ro trong trường hợp bị ảnh hưởng *(tham khảo phụ lục gửi kèm)*.

2. Chủ động, tăng cường giám sát và sẵn sàng phương án xử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng; đồng thời thường xuyên theo dõi kênh cảnh báo của các cơ quan chức năng và các tổ chức lớn về an toàn thông tin để phát hiện kịp thời các nguy cơ tấn công mạng.

3. Trong quá trình tổ chức thực hiện, nếu có khó khăn vướng mắc đề nghị các đơn vị liên hệ:

Phòng An toàn thông tin và Giao dịch điện tử (điện thoại: 024.35123035, thư điện tử: patttgddt_sotttt@hanoi.gov.vn).

Đội ứng cứu sự cố an toàn thông tin mạng Thành phố Hà Nội (điện thoại trực 24/24: 024.35124010, thư điện tử: ttdl_sotttt@hanoi.gov.vn).

UBND Huyện yêu cầu các đơn vị triển khai thực hiện./.

Nơi nhận: - Như trên; - Đ/c Trương Văn Học-PCT UBND huyện; - Lưu: VT, VHTT.	**TM. ỦY BAN NHÂN DÂN** **CHỦ TỊCH** **Đặng Thị Huyền**

Phụ lục

THÔNG TIN CHI TIẾT VỀ RỦI RO AN TOÀN THÔNG TIN

(Kèm theo Công văn số /UBND-VHTT ngày /7 /2024 của UBND huyện Gia Lâm)

1. Thông tin chi tiết về rủi ro an toàn thông tin liên quan đến sản phẩm của CrowdStrike

Cục An toàn thông tin đã phát hiện rủi ro an toàn thông tin liên quan đến sản phẩm của CrowdStrike. Cụ thể, các máy tính chạy hệ điều hành Windows 10 và cài đặt phần mềm Falcon Sensor của hãng CrowdStrike đều gặp lỗi màn hình xanh (Blue Screen Of Death - BSOD) và không thể khởi động lại để hoạt động bình thường. Điều này gây ảnh hưởng tới hệ thống thông tin và hoạt động của cá nhân, cơ quan, tổ chức. Nhà phát triển CrowdStrike đã đưa ra thông báo xác nhận rủi ro và thực hiện khôi phục phần mềm Falcon Sensor để tránh gây thêm ảnh hưởng tới thiết bị của người dùng.

Hướng dẫn khắc phục đối với các thiết bị đã bị ảnh hưởng:

Bước 1: Khởi động lại máy tính và vào chế độ Safe Mode hoặc Windows Recovery Environment.

Bước 2: Truy cập thư mục "C:\Windows\System32\drivers\CrowdStrike"

Bước 3: Xóa bỏ các tập tin có định dạng "C-00000291*.sys" (tập tin có định dạng .sys và tên bắt đầu bằng chuỗi C-00000291)

Bước 4: Khởi động lại máy tính và sử dụng như bình thường.

2. Tài liệu tham khảo

https://supportportal.crowdstrike.com/s/article/Tech-Alert-Windows-crashes-related-to-Falcon-Sensor-2024-07-19