UBND HUYỆN CẦN GIỜ
PHÒNG GIÁO DỤC VÀ ĐÀO TẠO

Số: 1306/GDĐT
V/v cảnh báo rủi ro an toàn thông tin liên quan đến sản phẩm của CrowdStrike

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

Cần Giờ, ngày 23 tháng 8 năm 2024

Kính gửi: Hiệu trưởng các trường mầm non, tiểu học, trung học cơ sở và Chuyên biệt Cần Thạnh.

Căn cứ Công văn số 6038/UBND ngày 20 tháng 8 năm 2024 của Ủy ban nhân dân huyện về việc cảnh báo rủi ro an toàn thông tin liên quan đến sản phẩm của CrowdStrike;

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin tại trường học. Phòng Giáo dục và Đào tạo đề nghị Hiệu trưởng các trường triển khai một số nội dung như 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.

2. 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 tổ chức lớn về an toàn thông tin để phát hiện kịp thời các nguy cơ tấn công mạng.

3. Đầu mối hỗ trợ.

Đội ứng cứu sự cố an toàn thông tin mạng thành phố:
- Số điện thoại hotline 24/7: 0889490111.
- Số điện thoại trong giờ hành chính: 38233717 ext: 111.

Thư điện tử: ATTT@tphcm.gov.vn.

Phòng Giáo dục và Đào tạo đề nghị Hiệu trưởng các trường khẩn trương triển khai thực hiện./.

Nơi nhận:
- Như trên;
- Ban lãnh đạo Phòng GD&ĐT;
- Phòng GD&ĐT (Ông Phụng);
- Lưu: VT.

TRƯỞNG PHÒNG

PHÒNG GIÁO DỤC VÀ ĐÀO TẠO

Võ Thị Diễm Phượng

PHỤ LỤC
THÔNG TIN CHI TIẾT VỀ RỦI RO AN TOÀN THÔNG TIN

(Kèm theo Công văn số 608/UBND ngày 20 tháng 8 năm 2024 của Ủy ban nhân dân huyện)

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