BỘ THÔNG TIN VÀ TRUYỀN THÔNG
TRUNG TÂM ỨNG CỨU
KHẨN CẤP MÁY TÍNH VIỆT NAM

Số: 232/VNCERT- ĐPƯC
V/v tăng cường kiểm tra rà soát hệ thống đảm bảo hệ thống an toàn thông tin

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

Hà Nội, ngày 30 tháng 7 năm 2016

Kính gửi:

- Các đơn vị chuyên trách về CNTT các Bộ, Ngành;
- Các Sở Thông tin và Truyền thông;
- Các thành viên mạng lưới ứng cứu sự cố Internet Việt Nam.

Ngày 29/7 đã xảy ra sự cố tấn công thay đổi giao diện website và các hệ thống thông tin thuộc sự quản lý của Tổng công ty Hàng không Việt Nam (Vietnam Airline) và một số đơn vị liên quan khác bị tấn công, xảy ra sự cố.

Tiếp theo cảnh báo số 1 lúc 14.50 ngày 29/7/2016 về "Yêu cầu kiểm tra và xử lý sự cố có mã độc khẩn cấp", nhằm phòng tránh các cuộc tấn công có thể xảy ra vào các hệ thống thông tin, Trung tâm VNCERT yêu cầu Lãnh đạo các đơn vị đặc biệt chú trọng công tác đảm bảo an toàn thông tin trên hệ thống do mình quản lý và chỉ đạo quyết liệt cho các phòng, ban có chức năng quản trị hệ thống cần thực hiện khẩn cấp các biện pháp sau:

- Thay đổi ngay các mật khẩu hiện tại, đồng thời thiết lập chính sách bắt buộc thay đổi mật khẩu trong chu kỳ 1 tháng, mật khẩu không được trùng nhau, đặt mật khẩu mạnh tối thiểu 8 ký tự bao gồm chữ, số, ký tự đặc biệt. Các mật khẩu bao gồm: mật khẩu máy chủ, mật khẩu đăng nhập ứng dụng, mật khẩu hệ điều hành, mật khẩu quản lý tên miền,…và các mật khẩu liên quan khác.

- Cô lập phân vùng các vùng máy chủ, thiết lập chính sách chỉ một vài địa chỉ IP, một số máy tính mới có quyền truy cập vào máy chủ được chỉ định.

- Rà soát mã độc trên các máy chủ, máy trạm để phát hiện và gỡ bỏ sớm các mã độc đã được cài cắm.

- Thiết lập tường lửa, hệ thống phát hiện xâm nhập để phát hiện và cảnh báo sớm các cuộc tấn công nhằm vào hệ thống.

- Danh sách mật khẩu các máy chủ không được lưu trên máy tính cá nhân đồng thời chỉ cho một số ít cán bộ có quyền nắm giữ danh sách mật khẩu này.

- Cập nhật thường xuyên các bản vá cho hệ điều hành, phần mềm dịch vụ trên các máy chủ, máy trạm.

- Cài đặt và để chế độ cập nhật tự động thường xuyên của chương trình diệt mã độc.

- Sao lưu thường xuyên các ứng dụng, mã nguồn, cơ sở dữ liệu để có phương án dự phòng, các bản sao lưu được tách khỏi máy chủ đang chạy dịch vụ về mặt vật lý.

- Chuẩn bị và thực hành các phương án đối phó đồng thời xây dựng quy trình ứng cứu xử lý sự cố nếu xảy ra sự cố.

- Chủ động cử các cán bộ tăng cường ứng trực trong thời gian tới để theo dõi hệ thống mạng của mình.

- Phổ biến nâng cao nhận thức về an toàn thư điện tử, an toàn internet cho các cán bộ sử dụng máy tính trong cơ quan, đơn vị mình. Phổ biến cho người dùng cảnh giác với các tập tin đính kèm trong các email.

- Báo cáo kịp thời cho Lãnh đạo, các đơn vị có chức năng để kịp thời phối hợp xử lý sự cố.

Trên đây là một số khuyến cáo nhằm tăng cường kiểm tra rà soát nhằm đảm bảo hệ thống an toàn, yêu cầu các đơn vị thực hiện nghiêm túc. Nếu có bất kỳ thông tin về sự cố, đề nghị báo ngay cho cơ quan điều phối ứng cứu quốc gia:

Đầu mối điều phối ứng cứu quốc gia:

Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT)

- Địa chỉ: 18 Nguyễn Du – Hai Bà Trưng – Hà Nội

- Điện thoại: 0436404423

- Điện thoại di động: 0934424009

- Hòm thư điện tử tiếp nhận sự cố: ir@vncert.gov.vn

Trân trọng./.

Nơi nhận:
- Như trên;
- Bộ trưởng (để b/c);
- Thứ trưởng Nguyễn Thành Hưng (để b/c);
- Giám đốc (để b/c);
- Lưu: VT, ĐPƯC.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

BỘ THÔNG TIN VÀ TRUYỀN THÔNG
TRUNG TÂM ỨNG CỨU KHẨN CẤP MÁY TÍNH VIỆT NAM

Nguyễn Khắc Lịch