UBND THÀNH PHỐ HẢI PHÒNG
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 2648 /STTTT-CNTT
V/v đảm bảo an toàn thông tin trong sử dụng dịch vụ chữ ký số chuyên dùng Chính phủ

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

Hải Phòng, ngày 25 tháng 12 năm 2020

Kính gửi:
- Các Sở, ban, ngành thành phố;
- Các cơ quan Trung ương tổ chức theo ngành dọc;
- Ủy ban nhân dân các quận, huyện.

Ngày 16/12/2020, Cục Chứng thư số và Bảo mật thông tin, Ban Cơ yếu Chính phủ có công văn số 458/CTSBMTT-QTHT về việc đảm bảo an toàn thông tin trong sử dụng dịch vụ chữ ký số chuyên dùng Chính phủ *(gửi kèm văn bản)*.

Để đảm bảo an toàn thông tin cho các hoạt động ứng dụng dịch vụ chứng thực chữ ký số chuyên dùng Chính phủ, Sở Thông tin và Truyền thông trân trọng đề nghị các cơ quan, đơn vị thực hiện:

- Phổ biến đến các cán bộ, công chức, viên chức, người lao động trong đơn vị nâng cao nhận thức về an toàn thông tin mạng nói chung và cảnh giác với các nguy cơ tấn công mạng có chủ đích nói riêng.

- Thường xuyên thực hiện đánh giá, rà quét mã độc các máy tính của cơ quan, đơn vị. Triển khai cài đặt phần mềm quét virus có bản quyền. Các đơn vị không cài đặt phần mềm quét virus có bản quyền, có thể tải công cụ được Cục Chứng thư số và Bảo mật thông tin cấp để kiểm tra, rà quét mã độc tại địa chỉ: http://av.bcy.gov.vn.

- Thực hiện theo hướng dẫn đảm bảo an toàn thông tin trong sử dụng dịch vụ chứng thực chữ ký số chuyên dùng Chính phủ của Cục Chứng thư số và Bảo mật thông tin *(gửi kèm theo)* tại địa chỉ: https://ca.gov.vn.

- Phổ biến, hướng dẫn thực hiện các nội dung trên tới 100% các đơn vị trực thuộc.

Sở Thông tin và Truyền thông cử ông Nguyễn Đông Huy (Trưởng Phòng Hạ tầng kỹ thuật và An toàn thông tin - Trung tâm Thông tin và Truyền thông, số điện thoại 098.4462472) là đầu mối phối hợp, trao đổi thông tin.

Trân trọng./.

Nơi nhận:
- Như trên;
- UBNDTP (để b/c);
- Ban 114 (để b/c);
- GĐ, các PGĐ Sở;
- TT TT&TT;
- Cổng TTĐT Sở, Cổng Tin tức TP;
- Lưu: VT, CNTT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HOÀ X.H.C.N VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
THÀNH PHỐ HẢI PHÒNG

Lê Văn Kiên

Hướng dẫn đảm bảo an toàn thông tin cho người dùng sử dụng chữ ký số Chuyên dùng Chính phủ *(tại địa chỉ: https://dvc.ca.gov.vn/-/huong-dan-am-bao-an-toan-thong-tin-cho-nguoi-dung-su-dung-chu-ky-so-chuyen-dung-chinh-phu)*

(Thứ năm, 17/12/2020 18:32)

Trong thời gian gần đây thông qua hệ thống theo dõi, giám sát và phân tích mã độc của Trung tâm CNTT và Giám sát An ninh mạng - Ban Cơ yếu Chính phủ đã phát hiện nhiều chiến dịch tấn công có chủ đích sử dụng mã độc vào máy tính người dùng tại các cơ quan Đảng và Nhà nước, trong đó có các máy tính sử dụng chữ ký số chuyên dùng Chính phủ phục vụ các hoạt động điều hành, xử lý công việc trên môi trường mạng. Các loại mã độc hay được sử dụng: *Trojan-Dropper, Trojan-Spy, Trojan-Downloader, Backdoor.win32, ...* Tin tặc thực hiện các chiến dịch tấn công bằng nhiều hình thức khác nhau như thông qua email, tấn công trực tiếp vào các Cổng thông tin điện tử của các bộ ngành, các website cung cấp dịch vụ công và thực hiện chèn mã độc vào các tài liệu, các tập tin cài đặt chương trình đang có sẵn trên các Cổng thông tin điện tử của các bộ ngành và các website cung cấp dịch vụ công. Khi người dùng thực hiện tải về sử dụng, máy tính sẽ nhiễm mã độc, bị kiểm soát và các tài liệu trên máy sẽ bị đánh cắp.

Chữ ký số là giải pháp đảm bảo an toàn thông tin được ứng dụng để đảm bảo tính xác thực, toàn vẹn và chống chối bỏ. Tuy nhiên gần đây các nhà nghiên cứu từ đại học Ruhr Bochum (Đức) đã tiết lộ các phương thức tấn công mới có tên là Shadow Attack lên các tập tin PDF được ký số. Các kỹ thuật tấn công này cho phép tin tặc ẩn và thay thế nội dung trong tài liệu PDF đã ký số mà không làm vô hiệu chữ ký. Tin tặc có thể tạo một tài liệu với hai nội dung khác nhau, một nội dung mà người ký thấy và một nội dung khác mà người nhận tài liệu nhìn thấy. Do đó, mục đích của hướng dẫn này là giúp các cán bộ, công chức, viên chức đã, đang và sẽ sử dụng chữ ký số chuyên dùng Chính phủ bổ sung những kiến thức và công cụ cơ bản để sử dụng chữ ký số một cách an toàn.

1. Các nguy cơ mất an toàn thông tin và nguyên nhân

Các phần mềm độc hại, gián điệp phát tán theo tệp văn bản, ảnh động, đường link đính kèm thông qua thư điện tử, tin nhắn... hoặc tự động lây lan khi người sử dụng cắm USB đã bị nhiễm từ máy tính này sang máy tính khác. Chúng có thể thu thập các thông tin quan trọng rồi tự động gửi về các máy chủ ở nước ngoài.

Máy tính của người dùng có thể bị xâm nhập trái phép thông qua các lỗ hổng bảo mật của hệ điều hành và các ứng dụng nhằm toàn quyền điều khiển, khai thác, lấy cắp và sử dụng thông tin cá nhân cho các mục đích khác.

Việc mất mát, thất lạc laptop, thiết bị lưu trữ di động, điện thoại di động... trong đó có chứa các dữ liệu quan trọng.

Các nguyên nhân chủ yếu đó là người sử dụng chưa có hiểu biết hoặc chủ quan, mất cảnh giác với các nguy cơ gây mất an toàn thông tin; chưa thực hiện đúng các quy trình kỹ thuật; máy tính, mạng máy tĩnh chưa được thiết lập các chính sách đảm bảo an toàn thông tin, công tác quản lý, giám sát kỹ thuật còn nhiều sơ hở.