UBND TỈNH NGHỆ AN
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số: 704 /STTTT-CĐS

V/v tăng cường bảo đảm an toàn thông tin mạng đối người dùng đầu cuối

Nghệ An, ngày 19 tháng 4 năm 2024

Kính gửi:
- Các Sở, ban, ngành cấp tỉnh;
- UBND các huyện, thành phố, thị xã;
- UBND các xã, phường, thị trấn;
- Mặt trận tổ quốc và các tổ chức đoàn thể CTXH;
- Viễn thông Nghệ An.

Hiện nay, tình trạng mất an toàn thông tin (ATTT) đối với người dùng đầu cuối (end-user) vẫn là một vấn đề nghiêm trọng. Dưới đây là một số tình trạng chính thường xuyên xảy ra:

1. Rủi ro từ mã độc và phần mềm độc hại: Người dùng đầu cuối đối mặt với sự xâm nhập của mã độc, phần mềm độc hại như virus, ransomware, spyware, và các ứng dụng độc hại khác. Những phần mềm này có thể lây nhiễm và gây thiệt hại đến hệ thống và dữ liệu cá nhân của người dùng.

2. Tấn công mạng và lừa đảo: Các cuộc tấn công mạng như phishing hoặc tấn công giữa người dùng (Man-in-the-Middle), có thể được sử dụng để đánh cắp thông tin cá nhân quan trọng, tài khoản đăng nhập.

3. Mất thông tin cá nhân: Việc mất mát hoặc rò rỉ thông tin cá nhân là một vấn đề lớn đối với người dùng đầu cuối. Điều này có thể xảy ra thông qua việc sử dụng các dịch vụ trực tuyến không an toàn, việc chia sẻ thông tin cá nhân với bên thứ ba không tin cậy hoặc thông qua các cuộc tấn công vào hệ thống lưu trữ dữ liệu.

4. Thiếu nhận thức an ninh thông tin: Một số người dùng đầu cuối vẫn thiếu nhận thức và hiểu biết về an ninh thông tin. Họ có thể sử dụng mật khẩu yếu, không cập nhật phần mềm bảo mật, hoặc không biết cách nhận diện các mối đe dọa an ninh.

Qua rà soát mức độ ATTT người dùng các hệ thống phần mềm dùng chung (như IOffice, Igate, …) tại các cơ quan nhà nước trên địa bàn tỉnh, nhiều tài khoản còn để mật khẩu yếu, không thay đổi mật khẩu định kỳ. Bên cạnh đó, nhận thức, trách nhiệm của người sử dụng về ATTT khi sử dụng các hệ thống hệ thống phần mềm dùng chung, đặc biệt về việc bảo mật thông tin tài khoản của cá nhân chưa đầy đủ, dẫn tới nguy cơ lộ lọt thông tin cao.

Trước tình hình an toàn thông tin mạng ở Việt Nam ngày càng diễn biến phức tạp, tăng mạnh về quy mô số lượng và mức độ tinh vi, nhằm nâng cao an

toàn bảo mật thông tin cho người sử dụng theo các quy định hiện hành, Sở Thông tin và Truyền thông kính đề nghị các đơn vị

1. Giám đóc các Sở, thủ trưởng các ban, ngành cấp tỉnh; Chủ tịch UBND các huyện, thành phố, thị xã; Chủ tịch UBND các xã, phường, thị trấn quán triệt cán bộ sử dụng các hệ thống thực hiện một số nội dung sau:

- Yêu cầu cán bộ, công chức, viên chức tại các đơn vị nâng cao hơn nữa nhận thức, trách nhiệm về ATTT khi sử dụng hệ thống, đặc biệt về việc bảo mật thông tin tài khoản của cá nhân.

- Mỗi cá nhân có trách nhiệm giữ bí mật các tài khoản, mật khẩu được cấp và chịu trách nhiệm khi để lộ lọt thông tin tài khoản, mật khẩu.

- Thay đổi mật khẩu cá nhân theo định kỳ (khuyến nghị 90 ngày/lần); đặt mật khẩu theo quy tắc khó đoán:

+ Mật khẩu phải có ít nhất 8 ký tự.

+ Mật khẩu phải có ít nhất 1 ký tự thường (VD: a,b,c,d,...).

+ Mật khẩu phải có ít nhất 1 ký tự hoa (VD: A,B,C,D,...).

+ Mật khẩu phải có ít nhất 1 ký tự đặc biệt (VD: @,#,$,...).

+ Mật khẩu phải có ít nhất 1 ký tự số (VD: 0,1,2,3...).

+ Mật khẩu không nên sử dụng 3 ký tự liền nhau trong từ điển

+ Không chứa các từ khóa dễ đoán liên quan tới thông tin cá nhân như họ tên, ngày sinh,…

- Hạn chế sử dụng tính năng lưu mật khẩu trên trình duyệt để giảm thiểu rủi ro bị lộ lọt thông tin.

- Không thực hiện lưu giữ, chia sẻ, gửi thông tin tài khoản mật khẩu qua các hệ thống email miễn phí, zalo, mạng xã hội,…

- Không ghi mật khẩu ra giấy, thiết bị lưu trữ dùng chung trừ khi giấy tờ và thiết bị này được lưu trữ tại vị trí lưu trữ riêng tư ví dụ tủ được khóa, chỉ được mở bởi người có trách nhiệm.

- Trường hợp nghi ngờ tài khoản của cá nhân bị lộ lọt thông tin, cần thực hiện thay đổi mật khẩu và thông báo cho cán bộ chuyên trách/phụ trách CNTT của đơn vị mình để kịp thời có biện pháp xử lý.

2. Đề nghị Cổng Thông tin điện tử Nghệ An

a) Tham mưu, xây dựng kế hoạch ứng phó các sự cố an toàn thông tin đối với hệ thống thông tin do đơn vị mình được giao quản lý.

c) Tổ chức kiểm tra, rà soát, kịp thời có phương án xử lý đối với các hệ thống hiện đang chủ trì quản trị kỹ thuật.

c) Bố trí cán bộ kỹ thuật thường xuyên theo dõi hệ thống, hỗ trợ người sử

dụng khi có nhu cầu.

3. Giao Trung tâm CNTT&TT Nghệ An

a) Tổ chức kiểm tra, rà soát, kịp thời có phương án xử lý đối với các hệ thống hiện đang chủ trì quản trị kỹ thuật, đặc biệt hệ thống mạng máy tính của Sở Thông tin và Truyền thông.

b) Tham mưu, xây dựng kế hoạch ứng phó các sự cố an toàn thông tin, sự cố đối với hệ thống thông tin của tỉnh trình Đội trưởng đội ứng cứu sự cố tỉnh Nghệ An và UBND tỉnh phê duyệt theo thẩm quyền.

c) Bố trí đủ cán bộ thuộc bộ phận ứng cứu sự cố sẵn sàng thực hiện nhiệm vụ khi có điều động.

d) Nghiên cứu giải pháp hỗ trợ các đơn vị khắc phục sự cố khi có yêu cầu.

e) Thường xuyên, liên tục sử dụng các Nền tảng về an toàn thông tin do Cục An toàn thông tin (Bộ Thông tin và Truyền thông) phát triển, cung cấp để hỗ trợ các cơ quan, tổ chức, doanh nghiệp: Sử dụng Nền tảng Điều phối xử lý sự cố an toàn thông tin mạng quốc gia (IRLab) để được hướng dẫn, nhận các cảnh báo sớm và hỗ trợ xử lý sớm nguy cơ, sự cố; Sử dụng Nền tảng Hỗ trợ điều tra số (DFLab) trong trường hợp phù hợp để tổ chức ứng cứu sự cố và được sự hỗ trợ từ cơ quan nhà nước, các chuyên gia đầu ngành về an toàn thông tin.

4. Viễn thông Nghệ An

- Tuân thủ các quy định pháp lý hiện hành và các điều khoản thuộc hợp đồng thuê dịch vụ có liên quan đến công tác an toàn thông tin để đảm bảo hoạt động ổn định, an toàn các hệ thống thông tin hiện đang cung cấp dịch vụ cho tỉnh Nghệ An.

- Cài đặt mặc định các hệ thống do đơn vị mình cung cấp tài khoản trên địa bàn tỉnh Nghệ An thay đổi mật khẩu cá nhân theo định kỳ (khuyến nghị 90 ngày/lần); đặt mật khẩu theo quy tắc khó đoán. Thực hiện khóa các tài khoản đang đặt mật khẩu mặc định các hệ thống và yêu cầu đổi mật khẩu đối với các tài khoản này.

- Khai thác các chức năng của Trung tâm Giám sát an ninh mạng SOC tỉnh Nghệ An để kịp thời cảnh báo, ngăn chặn, hỗ trợ xử lý các sự cố mạng trong các cơ quan nhà nước của tỉnh.

Trong quá trình thực hiện, nếu có khó khăn vướng mắc hoặc trường hợp cần hỗ trợ giám sát, xử lý, ứng cứu sự cố đề nghị liên hệ thông qua các đầu mối:

- Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT/CC), điện thoại 024.3640.4421 hoặc số điện thoại trực đường dây nóng ứng cứu sự cố 086.9100.317, thư điện tử: ir@vncert.vn;

- Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), điện thoại: 024.32091.616 hoặc số điện thoại trực đường dây nóng hỗ trợ giám sát,

cảnh báo sớm 038.9942.878, thư điện tử: ais@mic.gov.vn.

- Phòng An toàn hệ thống thông tin, Cục An toàn thông tin (hướng dẫn công tác bảo đảm an toàn hệ thống thông tin theo cấp độ), điện thoại: 0369596886, thư điện tử: athttt@mic.gov.vn.

- Đội Ứng cứu sự cố an toàn thông tin mạng tỉnh Nghệ An, điện thoại: 02383.500027.

Trân trọng!./.

Nơi nhận:
- Như trên;
- Cục ATTT, Bộ TT&TT (b/c);
- UBND tỉnh Nghệ An (b/c);
- Ban Giám đốc Sở;
- Cổng TTĐT Nghệ An;
- TrT. CNTT&TT Nghệ An;
- Lưu: VT, CĐS (đ/c Hợi).

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH NGHỆ AN

Võ Trọng Phú