UBND TỈNH ĐẮK LẮK
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 691 /STTTT-CNTT

V/v tăng cường công tác đảm bảo an toàn thông tin trong thời gian Đại hội Đảng toàn quốc lần thứ XII

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

Đắk Lắk, ngày 16 tháng 12 năm 2015

Kính gửi:
- Văn phòng Tỉnh ủy;
- Văn phòng Đoàn ĐBQH và HĐND tỉnh;
- Các sở, ban, ngành, đoàn thể của tỉnh;
- UBND các huyện, thị xã, thành phố.

Trong thời gian qua tình hình an toàn, an ninh thông tin mạng diễn biến phức tạp, Việt Nam không những bị ảnh hưởng mà còn là đối tượng trực tiếp phải chịu nhiều cuộc tấn công mạng. Đặc biệt, các cuộc tấn công mạng này có dấu hiệu gia tăng về số lượng cũng như mức độ nguy hiểm trong các sự kiện lớn của Việt Nam. Cụ thể, trong đợt 30/4-01/5 và kỳ nghỉ lễ Quốc khánh 02/9/2014 đã ghi nhận được hơn 1.000 Website có tên miền .vn bị tin tặc tấn công. Gần đây nhất, trong thời gian diễn ra Đối thoại Shangri-La 2015, hơn 1.000 Website Việt Nam đã bị tấn công thay đổi giao diện, trong đó có nhiều Website có tên miền .gov.vn. *(tên miền CQNN)*. Những cuộc tấn công mạng này đã ảnh hưởng lớn đến lợi ích, độ tin cậy của Việt Nam nói chung, cơ quan Chính phủ Việt Nam nói riêng trong không gian mạng và ảnh hưởng tới sự ổn định chính trị, phát triển kinh tế, xã hội và an ninh, quốc phòng.

Thực hiện chỉ đạo của UBND tỉnh, Bộ Thông tin và Truyền thông *(CV số 8545/UBND-CN ngày 18/11/2015 của UBND tỉnh, CV số 3586/BTTTT-CATTT ngày 04/11/2015 của Bộ TT&TT)* về việc tăng cường công tác đảm bảo an toàn thông tin trong thời gian Đại hội Đảng toàn quốc lần thứ XII. Sở Thông tin và Truyền thông đề nghị các sở, ban, ngành, đoàn thể; UBND các huyện, thị xã, thành phố thực hiện tốt những nội dung sau:

1. Tiếp tục quán triệt, thực hiện nghiêm Chỉ thị số 28-CT/TW ngày 16/9/2013 của Ban bí thư về tăng cường công tác bảo đảm an toàn thông tin mạng; Chỉ thị số 15/CT-TTg ngày 17/6/2014 của Thủ tướng Chính phủ về tăng cường công tác đảm bảo an toàn thông tin mạng trong tình hình mới tại cơ quan, đơn vị.

2. Tăng cường công tác tuyên truyền nâng cao nhận thức về công tác bảo đảm an toàn thông tin mạng, cảnh giác với những nguy cơ mất an toàn thông tin trong việc sử dụng máy tính, thiết bị di động và Internet hàng ngày đối với cán bộ công chức, viên chức.

3. Kiểm tra, bảo trì hệ thống máy tính, mạng máy tính tại các cơ quan, đơn vị, kịp thời loại bỏ việc lây nhiễm Virus, phần mềm mã độc ra khỏi hệ thống để đảm bảo cho công việc và trao đổi, thông tin nhằm hạn chế tối đa có thể xảy ra sự cố mất an toàn, an ninh thông tin mạng. Tất cả máy tính của cơ quan, đơn vị chỉ cài đặt các phần mềm để phục vụ công việc chuyên môn, không cài đặt các phần mềm không rõ nguồn gốc, không bản quyền.

4. Tăng cường công tác quản trị, theo dõi hệ thống cổng/trang thông tin điện tử của cơ quan 24/24 giờ hàng ngày; đồng thời, chú trọng công tác an toàn thông tin đối với tài khoản biên tập, đăng tải thông tin trên hệ thống nhằm phòng/chống, ngăn chặn và phát hiện kịp thời sự xâm nhập trái phép, tấn công vào hệ thống thông tin.

5. Một số biện pháp kỹ thuật phòng chống tấn công cần thiết

a) Đối với người quản trị, vận hành hệ thống công nghệ thông tin:

- Để vận hành máy chủ an toàn, việc cần lưu ý đầu tiên là luôn cập nhật phiên bản mới và bản vá lỗi mới nhất cho hệ thống.

- Tăng cường khả năng xử lý của hệ thống: Tối ưu hóa các thuật toán sử lý, mã nguồn của máy chủ Web; nâng cấp hệ thống máy chủ; nâng cấp đường truyền và các thiết bị liên quan; cập nhật kịp thời các bản vá lỗi cho hệ điều hành và các phần mềm công dụng khác để phòng ngừa khả năng bị lỗi tràn bộ đệm, cướp quyền điều khiển,...

- Hạn chế số lượng kết nối tại thiết bị tường lửa tới mức an toàn hệ thống cho phép. Sử dụng các tường lửa cho phép lọc nội dung thông tin (tầng ứng dụng) để ngăn chặn các kết nối tấn công vào hệ thống.

- Phân tích luồng tin (Traffic) để phát hiện các dấu hiệu tấn công và cài đặt các tường lửa cho phép lọc nội dung thông tin ngăn chặn theo các dấu hiệu đã phát hiện.

- Tùy khả năng đầu tư cổng/trang thông tin điện tử có thể trang bị giải pháp hoặc sử dụng dịch vụ chống DoS/DDoS với các công cụ kỹ thuật: Sử dụng hệ thống thiết bị, phần mềm hoặc dịch vụ giám sát an toàn mạng (đặc biệt về lưu lượng) để phát hiện sớm các tấn công từ chối dịch vụ, sử dụng thiết bị bảo vệ mạng có dịch vụ chống tấn công DDoS chuyên nghiệp kèm theo, như: Arbor, Checkpoint, Imperva,...

b) Đối với người sử dụng

- Trên máy tính cá nhân:

+ Khóa các tài khoản (User) không sử dụng.

+ Tắt chức năng Remote Desktop.

+ Cài đặt chương trình diệt Virus có bản quyền.

- Trên thiết bị thông minh như Smart Phone, máy tính bảng Tablets,...:

+ Thiết lập một hệ thống mật mã an toàn trên thiết bị.

+ Không lưu những thông tin quan trọng trên thiết bị.

+ Định kỳ nên sao lưu và kiểm tra thông tin thiết bị; hạn chế kết nối với các mạng di động công cộng không có tường lửa; khi cài đặt các phần mềm ứng dụng cần biết rõ nguồn gốc.

+ Chỉ kết nối thiết bị vào máy vi tính khi chắc chắn máy không bị nhiễm Virus; tắt và vô hiệu hóa các kênh kết nối như hồng ngoại (IR), Bluetooth trên thiết bị khi không sử dụng.

Sở thông tin và Truyền thông đề nghị Thủ trưởng các sở, ban, ngành và đoàn thể; Chủ tịch UBND các huyện, thị xã, thành phố triển khai, quán triệt thực hiện văn bản này đến các cơ quan, đơn vị thuộc cấp, ngành quản lý; Văn phòng Tỉnh ủy triển khai cho các cơ quan, đơn vị trong hệ thống tổ chức Đảng các cấp của tỉnh để thực hiện.

Các sự cố xảy ra về công tác an toàn thông tin mạng tại các cơ quan, đơn vị hoặc các vướng mắc, cần phối hợp,... liên hệ Phòng Công nghệ thông tin - Sở Thông tin và Truyền thông; điện thoại: 0500.355.7.888; email: phongcntt@tttt.daklak.gov.vn để được phối hợp và hướng dẫn./.

Nơi nhận:
- UBND tỉnh; (để b/c);
- Như trên;
- GĐ, các PGĐ Sở;
- VP, các Phòng thuộc Sở;
- TT CNTT&TT;
- TT.QLCTTĐT tỉnh;
- Phòng VHTT các huyện, TX, TP;
- Lưu VT, CNTT.

GIÁM ĐỐC

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH ĐẮK LẮK

Trần Trung Hiền