UBND TỈNH QUẢNG NGÃI
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số: 703 /STTTT

Quảng Ngãi, ngày 12 tháng 7 năm 2019

V/v tăng cường các biện pháp bảo đảm an toàn, an ninh thông tin dữ liệu và các hệ thống thông tin

Kính gửi:
- Văn phòng Tỉnh ủy;
- Văn phòng UBND tỉnh;
- Các Sở, ban, ngành; Hội, đoàn thể;
- Các cơ quan Trung ương trên địa bàn tỉnh;
- UBND các huyện, thành phố.

Qua theo dõi tình hình an toàn thông tin trên không gian mạng, từ Cục an toàn thông tin, Trung tâm ứng cứu khẩn cấp máy tính Việt Nam (thuộc Bộ Thông tin và Truyền thông), các cơ quan nhà nước trên địa bàn tỉnh Quảng Ngãi, Sở Thông tin và Truyền thông nhận thấy các cuộc tấn công mạng ngày càng phức tạp, tăng mạnh về quy mô, cách thức, mức độ nguy hiểm, đặc biệt là các cuộc tấn công nhằm mã hóa, đánh cắp dữ liệu, tống tiền, đôi khi là phá hoại dữ liệu (Mã hóa toàn bộ dữ liệu của hệ thống thông, các máy chủ, máy tính đang sử dụng và hầu như không có khả năng khắc phục và khôi phục lại).

Để chủ động đối phó với các tình huống bị tấn công, bị mất, bị phá hoại, bị mã hóa dữ liệu, các đơn vị cần thực hiện nhiều biện pháp phòng ngừa, sao lưu dữ liệu dự phòng các hệ thống thông tin, đặc biệt là các hệ thống thông tin dùng chung, quan trọng của cơ quan, đơn vị như: Trung tâm dữ liệu, hệ thống Cổng thông tin điện tử, hệ thống thư điện tử, hệ thống quản lý văn bản (eOffice), các các file dữ liệu và cơ sở dữ liệu quan trọng,….

Kính đề nghị Thủ trưởng các cơ quan, đơn vị chỉ đạo các cá nhân/đơn vị chuyên trách về công nghệ thông tin/an toàn thông tin của đơn vị mình phối hợp với đơn vị chức năng để tiến hành rà soát, kiểm tra và triển khai thực hiện đầy đủ, kịp thời các biện pháp nhằm bảo đảm về an toàn, an ninh thông tin trên hệ thống thông tin của đơn vị như *Hướng dẫn kèm theo*.

Trân trọng./.

Nơi nhận:
- Như trên;
- Thành viên Đội ứng cứu sự cố tỉnh;
- Sở TT&TT: GĐ, PGĐ, các phòng ban;
- Trung tâm CN-TT&TT;
- Lưu: VT, CNTT$_{104}$.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Nguyễn Ngọc Trân

HƯỚNG DẪN TĂNG CƯỜNG CÁC BIỆN PHÁP BẢO ĐẢM AN TOÀN THÔNG TIN DỮ LIỆU VÀ CÁC HỆ THỐNG THÔNG TIN

(Kèm theo Công văn số: 703/STTTT ngày 12/7/2019 của Sở Thông tin và Truyền thông)

1.Tăng cường bảo đảm an toàn, an ninh hệ thống mạng:

a) Đối với hệ thống mạng trung tâm:

- Rà soát, kiểm tra thiết bị tường lửa (firewall) của hệ thống: Kiểm tra các lớp tường lửa trên toàn hệ thống, đảm bảo các lớp tường lửa được kích hoạt các chức năng đánh chặn, cấu hình đánh chặn các địa chỉ điều khiển mã độc được cảnh báo bởi Sở Thông tin và Truyền thông, Trung tâm ứng cứu khẩn cấp máy tính Việt Nam(Vncert).

- Trang bị bản quyền trên thiết bị và tường xuyên cập nhật bản vá của thiết bị.

- Chỉ mở những cổng (port) vừa đủ cho các dịch vụ cần sử dụng, hạn chế mở các port đã được cảnh báo như Remote Desktop (3389).

- Đảm bảo bảo mật về tài khoản quản trị: Tài khoản quản trị phải đảm bảo độ phức tạp (mật khẩu ít nhất là 08 ký tự bao gồm: chữ hoa, chữ thường, số và ký tự đặc biết, vd: soA2019**).

- Thường xuyên theo dõi hoạt động của thiết bị: Kiểm tra lưu lượng, tầng suất ra vào, hành vi hoạt động trên hệ thống.

- Sao lưu cài đặt cấu hình các thiết bị thành nhiều bản (ít nhất 02 bản) và cập nhật bản sao mỗi khi có sự thay đổi về cơ chế trên thiết bị nhằm đảm bảo khôi phục lại hệ thống khi cần thiết như: sao lưu ra ổ cứng di động, USB, hệ thống sao lưu dự phòng.

b) Đối với người dùng trong hệ thống:

- Cài đặt chương trình diệt virus trên tất cả các thiết bị tham gia vào hệ thống mạng của đơn vị.

- Phải đảm bảo truy cập mạng (duyệt web, mạng xã hội, email…) và sử dụng dữ liệu an toàn tránh tình trạng nhiễm virus dẫn đến lây lan trên hệ thống.

- Máy tính các nhân phải được đặt mật khẩu an toàn và thường xuyên cập nhật bản vá hệ điều hành, bản vá các ứng dụng đang được cài đặt và sử dụng.

2.Tăng cường an toàn an ninh máy chủ và cơ sở dữ liệu:

a) Đối với máy chủ:

- Cần sử dụng hệ điều hành bản quyền, đặc biệt đối với hệ điều hành máy chủ; cài đặt chương trình diệt virus.

- Thường xuyên cập nhật bản vá hệ điều hành, bản vá các ứng dụng trên máy chủ để tránh tình trạng các cuộc tấn công nhằm vào các lỗ hổng trên hệ điều hành và các ứng dụng.

- Bật các cơ chế tường lửa trên hệ điều hành, nhăm ngăn chặn các nguy cơ bị bị tấn công.

- Thường xuyên kiểm tra tình trạng hoạt động của các máy chủ vật lý để kịp thời phát nhiện và xử lý các lỗi về vật lý trên máy chủ.

b) Đối với các thông tin dữ liệu và cơ sở dữ liệu:

Đảm bảo các thông tin dữ liệu và cơ sở dữ liệu trên hệ thống được thực hiện sao lưu thường xuyên và định kỳ; được sao lưu thành nhiều bản (ít nhất 02 bản) và mỗi phiên bản cần lưu trữ trong ít nhất 7 ngày (tùy vào mức độ quan trọng của từng hệ thống) bằng các thiết bị như: hệ thống SAN, NAT… hoặc sao lưu qua các ổ đĩa rời và thực hiện lưu trữ ở nhiều nơi khác nhau./.

---o0o---