

Số: 1790/BTTTT-VNCERT

V/v tăng cường công tác đảm bảo an toàn thông tin cho công/trang thông tin điện tử

Hà Nội, ngày 20 tháng 6 năm 2011

Kính gửi:

- Đơn vị chuyên trách về CNTT của các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- Sở Thông tin và Truyền thông các tỉnh, thành phố trực thuộc Trung ương.

Thời gian gần đây, các hoạt động tấn công mạng nhằm vào các công/trang thông tin điện tử của các cơ quan nhà nước và các tổ chức tại Việt Nam có dấu hiệu gia tăng. Hai hình thức tấn công phổ biến được ghi nhận là tấn công thay đổi giao diện (defaced) và tấn công từ chối dịch vụ (DDoS). Đối tượng bị tấn công là những công/trang thông tin điện tử có lỗ hổng an toàn thông tin hoặc công/trang thông tin điện tử của cơ quan nhà nước và báo điện tử lớn.

Trước tình hình đó, Bộ Thông tin và Truyền thông đề nghị các đơn vị thực hiện một số biện pháp sau nhằm góp phần đề phòng, ngăn chặn các cuộc tấn công, tăng cường đảm bảo an toàn thông tin trong thời gian tới:

- Chủ động phối hợp cùng cơ quan chủ quản các công/trang thông tin điện tử của Bộ, ngành, địa phương mình tổ chức rà soát nhằm phát hiện và có biện pháp khắc phục các lỗ hổng bảo mật tồn tại trên hệ thống, đảm bảo áp dụng những biện pháp quan trọng như: thường xuyên quét sạch mã độc, vi-rút máy tính khỏi hệ thống bằng các công cụ tin cậy luôn được cập nhật mới; định kỳ thay đổi và quản lý bảo mật tốt danh sách tên tài khoản và mật khẩu của những người có quyền quản trị hệ thống.

- Chỉ đạo các doanh nghiệp cung cấp dịch vụ lưu trữ (hosting) trên địa bàn rà soát lại các máy chủ lưu trữ công/trang thông tin điện tử của các cơ quan, tổ chức; tiến hành giám sát, lưu trữ biên bản hoạt động (log file) để xử lý trong trường hợp xảy ra sự cố; trang bị/ nâng cấp/ rà soát các giải pháp áp dụng hệ thống tường lửa đủ năng lực lọc ngăn chặn các luồng tin tấn công có đích và sẵn sàng hỗ trợ khách hàng khi có sự cố.

- Tăng cường theo dõi, giám sát về mặt kỹ thuật hoạt động của các hệ thống thông tin nhằm phát hiện kịp thời các sự cố và các dấu hiệu tấn công. Trong

trường hợp phát hiện các dấu hiệu tấn công cần sớm có biện pháp tự khắc phục hoặc sử dụng dịch vụ của các tổ chức an toàn thông tin bên ngoài. Trong trường hợp sự cố nghiêm trọng hoặc xảy ra trên diện rộng cần thông báo ngay cho Bộ Thông tin và Truyền thông (Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam) để kịp thời có biện pháp điều phối xử lý.

- Nhanh chóng tổ chức triển khai thực hiện Chỉ thị số 897/CT-TTg ngày 10/6/2011 của Thủ tướng Chính phủ về việc tăng cường triển khai các hoạt động đảm bảo an toàn thông tin số trong phạm vi Bộ, ngành, địa phương mình.

Ngoài ra, Bộ Thông tin và Truyền thông cũng đề nghị các đơn vị có báo cáo đánh giá tình hình an toàn thông tin, các sự cố máy tính xảy ra từ đầu năm 2011 ở Bộ, ngành, địa phương mình và các kiến nghị, đề xuất (nếu có).

Đầu mối thông báo sự cố và tiếp nhận báo cáo: Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam, Điện thoại: 04 36404423, Fax: 04 36404425, Email: office@vncert.vn. Trong trường hợp khẩn cấp liên hệ: Ông Nguyễn Thành Đạt, Điện thoại di động: 0988612986, Email: ntdat@vncert.vn .

Trân trọng cảm ơn ./.

Nơi nhận:

- Như trên;
- PTTgCP Nguyễn Thiện Nhân (để b/c);
- Bộ trưởng Lê Doãn Hợp (để b/c);
- Các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- UBND các tỉnh, thành phố trực thuộc TW;
- Bộ TT&TT: Vụ CNTT, Cục UDCNTT, TTTT;
- Lưu: VT, VNCERT.

**KT. BỘ TRƯỞNG
THỨ TRƯỞNG**

(đã ký)

Nguyễn Minh Hồng