BỘ THÔNG TIN VÀ TRUYỀN THÔNG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
	Độc lập - Tự do - Hạnh phúc
Số: 4327/BTTTT-CATTT	*Hà Nội, ngày 21 tháng 12 năm 2018*

Vv đôn đốc tăng cường bảo đảm an toàn thông tin trong dịp Tết Dương lịch và Tết Kỷ Hợi 2019

Kính gửi:
- Các Bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ;
- UBND các tỉnh, thành phố trực thuộc Trung ương;
- Các doanh nghiệp cung cấp dịch vụ viễn thông, Internet;
- Các tập đoàn kinh tế, tổng công ty nhà nước;
- Các Ngân hàng TMCP; Các tổ chức tài chính.

Qua công tác theo dõi, giám sát không gian mạng, Bộ Thông tin và Truyền thông (Bộ TT&TT) ghi nhận trong 06 tháng cuối năm 2018: Có hơn 6 triệu địa chỉ IP (6,189,778 địa chỉ IP) của Việt Nam có kết nối đến các tên miền hoặc IP phát tán/điều khiển mã độc trên thế giới, chủ yếu là các kết nối tới các mạng botnet lớn như: conficker, mirai, ramnit, sality, cutwai, zeroaccess .v.v...; trong đó có nhiều trường hợp là các địa chỉ IP của các bộ, ngành, địa phương có kết nối tới máy chủ điều khiển mã độc APT; Tình hình lộ, lọt thông tin xác thực cũng diễn biến phức tạp, chủ yếu liên quan tới các tài khoản thư điện tử, hệ thống dịch vụ công, cụ thể là có khoảng 1,809 tài khoản trên 512 tên miền gov.vn bị lộ, lọt thông tin xác thực.

Trần Ngọc Thuận

Thực tế những năm trở lại đây tình hình an toàn thông tin tại Việt Nam thường có các diễn biến phức tạp, đặc biệt trong khoảng thời gian diễn ra các sự kiện lớn của đất nước và những dịp nghỉ lễ. Do đó, nhằm bảo đảm an toàn thông tin trong thời gian Tết Dương lịch và Tết Nguyên đán Kỷ Hợi 2019, Bộ TT&TT yêu cầu các cơ quan, doanh nghiệp nhà nước:

1. Chủ động rà soát các điểm yếu, lỗ hổng trên hệ thống; tăng cường triển khai các giải pháp bảo đảm an toàn thông tin cho các hệ thống thông tin của cơ quan, tổ chức mình.

2. Thủ trưởng cơ quan, doanh nghiệp chỉ đạo đơn vị trực thuộc tiến hành rà soát, kiểm tra, thực hiện đầy đủ, kịp thời các quy định về bảo đảm an toàn thông tin, đặc biệt là trong công tác phòng, chống, gỡ bỏ phần mềm độc hại, phần mềm gián điệp (APT);

3. Tăng cường theo dõi, giám sát, chủ động phát hiện sớm các nguy cơ, dấu hiệu tấn công mạng, kịp thời xử lý các vấn đề phát sinh. Cử cán bộ kỹ thuật trực theo dõi, giám sát liên tục hệ thống trong kỳ nghỉ.

4. Khi phát hiện dấu hiệu của các chiến dịch tấn công mạng, thông báo về cơ quan chức năng liên quan của Bộ Thông tin và Truyền thông (Cục An toàn thông tin, VNCERT) để có biện pháp xử lý kịp thời, giảm thiểu thiệt hại;

5. Thường xuyên cập nhật thông tin cảnh báo, khuyến nghị về an toàn thông tin được Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) thuộc Cục An toàn thông tin chia sẻ.

Khi triển khai các nội dung nêu trên, trong trường hợp cần thiết, Quý đơn vị có thể liên hệ với Cục An toàn thông tin, số điện thoại: 0243.3943.6684, thư điện tử ais@mic.gov.vn để được phối hợp, hỗ trợ.

Trân trọng./.

Nơi nhận:
- Như trên;
- Thủ tướng Chính phủ (để b/c);
- Phó TTg CP Vũ Đức Đam (để b/c);
- Văn phòng TW Đảng;
- Văn phòng Quốc hội;
- Văn phòng Chính phủ;
- Cơ quan TW các đoàn thể;
- Toà án nhân dân tối cao;
- Kiểm toán nhà nước;
- Bộ trưởng (để b/c);
- Thứ trưởng Nguyễn Thành Hưng;
- Đơn vị chuyên trách CNTT các Bộ, cơ quan ngang Bộ, cơ quan chính phủ (qua email);
- Sở TT&TT các tỉnh, TP thuộc TW (qua email);
- VNCERT;
- Lưu: VT, CATTT.

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

Nguyễn Thành Hưng