THỦ TƯỚNG CHÍNH PHỦ	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
	Độc lập - Tự do - Hạnh phúc
Số: 897/CT-TTg	*Hà Nội, ngày 10 tháng 6 năm 2011*

CHỈ THỊ
Về việc tăng cường triển khai các hoạt động đảm bảo an toàn thông tin số

Thời gian gần đây, tình hình mất an toàn thông tin số ở nước ta diễn biến phức tạp, xuất hiện nhiều nguy cơ đe dọa nghiêm trọng đến việc ứng dụng công nghệ thông tin phục vụ phát triển kinh tế - xã hội và đảm bảo quốc phòng, an ninh. Theo số liệu thống kê, số vụ tấn công trên mạng và các vụ xâm nhập hệ thống công nghệ thông tin nhằm do thám, trục lợi, phá hoại dữ liệu, ăn cắp tài sản, cạnh tranh không lành mạnh và một số vụ việc mất an toàn thông tin số khác đang gia tăng ở mức báo động về số lượng, đa dạng về hình thức, tinh vi hơn về công nghệ. Kết quả nghiên cứu, khảo sát cũng cho thấy nhiều hệ thống công nghệ thông tin của các cơ quan nhà nước và doanh nghiệp, đặc biệt là các cổng, trang thông tin điện tử có nhiều điểm yếu về an toàn thông tin, chưa được áp dụng các giải pháp đảm bảo an toàn và bảo mật thông tin phù hợp. Để tăng cường khả năng phòng, chống các nguy cơ tấn công, xâm nhập hệ thống công nghệ thông tin và ngăn chặn, khắc phục kịp thời các sự cố an toàn thông tin trên mạng máy tính, Thủ tướng Chính phủ chỉ thị:

1. Các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương:

a) Kiểm tra và nghiêm túc thực hiện các quy định về bảo đảm an toàn thông tin số trên môi trường mạng tại các Điều 41, 42 Nghị định số 64/2007/NĐ-CP ngày 10 tháng 4 năm 2007 của Chính phủ về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước; bảo đảm các nguyên tắc an toàn thông tin trong quá trình thiết kế, xây dựng, vận hành, nâng cấp và hủy bỏ các hạ tầng kỹ thuật. Tăng cường công tác triển khai quản lý an toàn thông tin số theo Tiêu chuẩn quốc gia TCVN ISO/IEC 27001:2009.

b) Triển khai áp dụng các giải pháp đảm bảo an toàn thông tin, chống virus và mã độc hại cho các hệ thống thông tin và các máy tính cá nhân có kết nối mạng Internet. Đối với các hệ thống thông tin quan trọng, các cổng, trang thông tin điện tử quan trọng, nhất thiết phải áp dụng chính sách ghi lưu tập

trung biên bản hoạt động (log file) cần thiết để phục vụ công tác điều tra và khắc phục sự cố mạng với thời hạn lưu giữ theo hướng dẫn của Bộ Thông tin và Truyền thông, nhưng tối thiểu không ít hơn 3 tháng.

c) Bố trí cán bộ quản lý, cán bộ kỹ thuật phù hợp chịu trách nhiệm đảm bảo an toàn cho các hệ thống thông tin số. Lập kế hoạch đào tạo bồi dưỡng nghiệp vụ cho đội ngũ cán bộ an toàn thông tin số, đào tạo, phổ biến kiến thức, kỹ năng cho người dùng máy tính về phòng, chống các nguy cơ mất an toàn thông tin số khi sử dụng mạng Internet.

d) Bố trí kinh phí từ ngân sách nhà nước và các nguồn kinh phí hợp pháp khác để triển khai các hoạt động đảm bảo an toàn thông tin số. Đảm bảo kinh phí đầu tư và vận hành thường xuyên các hệ thống đảm bảo an toàn thông tin số.

đ) Xây dựng, triển khai kế hoạch đảm bảo an toàn thông tin số định kỳ hàng năm và 5 năm nhằm thực hiện các mục tiêu của Quy hoạch phát triển an toàn thông tin số quốc gia đến năm 2020 (Quyết định số 63/QĐ-TTg ngày 13 tháng 01 năm 2010 của Thủ tướng Chính phủ).

e) Các thông tin thuộc bí mật Nhà nước lưu trữ và truyền trên môi trường mạng phải được mã hóa và quản lý theo quy định của pháp luật về cơ yếu.

2. Bộ Thông tin và Truyền thông:

a) Hoàn thiện cơ chế, chính sách, môi trường pháp lý về an toàn thông tin số; nghiên cứu xây dựng Luật An toàn thông tin số để trình Quốc hội khóa XIII ban hành.

b) Nhanh chóng triển khai hệ thống giám sát an toàn thông tin trên mạng Internet Việt Nam nhằm sớm phát hiện các nguy cơ, dấu hiệu và nguồn gốc tấn công mạng.

c) Ban hành và chủ trì triển khai thực hiện cơ chế điều phối và phối hợp giữa các đơn vị nhằm đảm bảo an toàn thông tin trên mạng Internet. Xây dựng và tổ chức diễn tập các phương án hợp tác ứng cứu sự cố mạng máy tính.

d) Ban hành quy định hướng dẫn yêu cầu kỹ thuật đảm bảo an toàn thông tin cho các hệ thống thông tin số. Hướng dẫn đào tạo, bồi dưỡng nghiệp vụ cho đội ngũ cán bộ kỹ thuật phụ trách an toàn thông tin cho các cổng, trang thông tin điện tử của các đơn vị, cơ quan nhà nước.

đ) Chỉ đạo các cơ quan báo chí, phát thanh, truyền hình đẩy mạnh tuyên truyền, nâng cao nhận thức an toàn thông tin số, quảng bá các hoạt động, sự kiện về an toàn thông tin số trong nước và quốc tế.

e) Tăng cường công tác thanh tra, kiểm tra và xử lý các tổ chức, cá nhân vi phạm quy định về đảm bảo an toàn thông tin. Phối hợp với Bộ Công an trong hoạt động phòng chống tội phạm trong lĩnh vực công nghệ thông tin.

g) Kịp thời đề xuất các chính sách và biện pháp quản lý nhà nước phù hợp nhằm đảm bảo an toàn thông tin số.

3. Bộ Công an:

a) Phối hợp với các Bộ, ngành liên quan đề xuất việc bổ sung vào Bộ Luật Tố tụng hình sự quy định về chứng cứ điện tử và trình tự, thủ tục tố tụng hình sự đối với việc thu thập và giám định chứng cứ điện tử.

b) Chủ trì phối hợp với các Bộ, ngành liên quan xây dựng Nghị định của Chính phủ quy định về phòng ngừa, đấu tranh chống tội phạm và vi phạm pháp luật trong lĩnh vực sử dụng công nghệ cao.

c) Tăng cường công tác phòng ngừa, phát hiện, điều tra xử lý tội phạm trong lĩnh vực công nghệ thông tin.

d) Phối hợp với các cơ quan chức năng trong việc đảm bảo an toàn hệ thống, an ninh dữ liệu mạng thông tin quốc gia.

đ) Tăng cường công tác tuyên truyền, phổ biến pháp luật về xử lý tội phạm trong lĩnh vực công nghệ thông tin.

e) Chú trọng công tác hợp tác quốc tế trong lĩnh vực đấu tranh phòng, chống tội phạm sử dụng công nghệ cao.

4. Bộ Quốc phòng:

a) Chủ trì đẩy mạnh nghiên cứu phòng, chống chiến tranh thông tin trong lĩnh vực quốc phòng.

b) Tham gia các hoạt động chung trong việc bảo đảm an toàn thông tin số, chống tội phạm và chống khủng bố trên mạng.

5. Ban Cơ yếu Chính phủ, Bộ Nội vụ:

a) Chủ trì triển khai các hệ thống bảo mật, an toàn thông tin dùng mật mã cho các cơ quan nhà nước. Đẩy mạnh hoạt động của hệ thống chứng thực điện tử chuyên dùng phục vụ cho các cơ quan thuộc hệ thống chính trị. Xây dựng các văn bản hướng dẫn triển khai chứng thực và áp dụng chữ ký số chuyên dùng cho các cơ quan thuộc hệ thống chính trị.

b) Tăng cường công tác quản lý nhà nước về mật mã, thúc đẩy ứng dụng mật mã phục vụ phát triển kinh tế - xã hội cho các hoạt động ứng dụng công nghệ thông tin và dịch vụ công nghệ thông tin trên mạng; hoàn thiện và hiện đại hóa hạ tầng cơ sở mật mã quốc gia.

c) Chủ trì, phối hợp với các cơ quan liên quan triển khai hệ thống giám sát an toàn thông tin trên mạng công nghệ thông tin trọng yếu của các cơ quan Đảng, Chính phủ. Nghiên cứu, đề xuất ban hành các tiêu chuẩn, quy chuẩn kỹ thuật cho các sản phẩm mật mã. Đẩy mạnh hoạt động kiểm định, đánh giá sản phẩm mật mã.

6. Bộ Kế hoạch và Đầu tư, Bộ Tài chính có trách nhiệm:

Bố trí kinh phí từ ngân sách nhà nước để triển khai các hoạt động đảm bảo an toàn thông tin số theo quy định của Luật Ngân sách nhà nước.

7. Các Hiệp hội hoạt động trong lĩnh vực liên quan đến an toàn thông tin số:

a) Tăng cường các hoạt động tuyên truyền quảng bá, nâng cao nhận thức cộng đồng về an toàn thông tin số. Vận động các hội viên, doanh nghiệp an toàn thông tin tích cực thúc đẩy phát triển và áp dụng các công cụ sản phẩm, giải pháp mới về an toàn thông tin số.

b) Tham gia các hoạt động tư vấn và đẩy mạnh đào tạo kỹ thuật, nghiệp vụ về an toàn thông tin số.

c) Tổ chức điều tra khảo sát, đánh giá thực trạng an toàn thông tin số trong các tổ chức, doanh nghiệp trên phạm vi cả nước để công bố trong sự kiện thường niên "Ngày An toàn thông tin Việt Nam" và báo cáo Bộ Thông tin và Truyền thông.

8. Các doanh nghiệp:

a) Tăng cường các biện pháp đảm bảo an toàn thông tin số, chú trọng triển khai ứng dụng các giải pháp công nghệ thông tin sử dụng chữ ký số và chứng thực số trong các hoạt động của doanh nghiệp, đặc biệt với các doanh nghiệp hoạt động trong lĩnh vực tài chính, ngân hàng và thương mại điện tử.

b) Các doanh nghiệp cung cấp hạ tầng mạng và dịch vụ Internet phải thiết lập đầu mối liên lạc để phối hợp và tuân thủ sự điều phối của cơ quan chức năng và tham gia vào công tác ứng cứu và khắc phục sự cố cho các hệ thống thông tin quan trọng.