

Số: 17/CT-UBND

Đồng Nai, ngày 24 tháng 5 năm 2013

CHỈ THỊ

Về việc kiểm tra thiết bị điện tử, máy tính được sử dụng truyền và lưu trữ thông tin bí mật nhà nước trên địa bàn tỉnh Đồng Nai

Gần đây, tình hình lộ, lọt thông tin, tài liệu bí mật của Đảng và Nhà nước đã xuất hiện ở một số nơi, có trường hợp gây hậu quả nghiêm trọng. Trong đó có nguyên nhân cài đặt chip điện tử trái phép vào các thiết bị điện tử viễn thông, máy tính.

Việc cài các chip điện tử gián điệp vào thiết bị điện tử viễn thông trái phép, máy tính được gọi là cài đặt "Cửa hậu" (backdoor), việc này được tạo dễ dàng từ phía nhà sản xuất. Mục đích của cài đặt backdoor là để lấy cắp dữ liệu và truyền theo ý muốn của người tạo ra chúng. Việc cài đặt trái phép này thường có trong các thiết bị điện tử viễn thông như thiết bị 3G (USB 3G, Webcam 3G), điện thoại di động, máy tính và các thiết bị công nghệ thông tin khác. Hiện tại, kỹ thuật công nghệ tại Việt Nam vẫn chưa sản xuất được thiết bị điện tử viễn thông, máy tính, mà chủ yếu phải nhập khẩu từ nước ngoài.

Ngày 14/3/2013, Bộ Thông tin và Truyền thông cùng với công ty Microsoft Việt Nam đã tổ chức buổi Tọa đàm về An toàn thông tin số. Tại buổi Tọa đàm, Giám đốc An ninh thông tin Microsoft châu Á cho biết Việt Nam có ba hạng mục nguy cơ cao được phát hiện trong Quý II năm 2012 gồm: hạng mục phổ biến nhất tại Việt Nam là những phần mềm không mong muốn, có ảnh hưởng tới 64% máy tính; hạng mục phổ biến thứ hai là mã độc cửa hậu trong các chip điện tử (backdoor) có ảnh hưởng tới 41,3% máy tính; hạng mục phổ biến thứ ba là sâu/virus máy tính (worm), có ảnh hưởng tới 30,1% máy tính.

Qua thực tế trên, cho thấy tình hình bảo mật trong nước đang có nguy cơ bị đe dọa, tin tặc có thể lợi dụng cơ hội để đánh cắp các thông tin bí mật nhà nước. Để ngăn ngừa việc lộ, lọt thông tin, tài liệu bí mật nhà nước, UBND tỉnh Chỉ thị:

1. Giao Giám đốc các Sở, ban, ngành; UBND các huyện, thị xã Long Khánh, thành phố Biên Hòa có trách nhiệm sau:

a) Lập danh sách các thiết bị điện tử, điện tử viễn thông, máy tính được sử dụng để truyền và lưu trữ thông tin bí mật nhà nước (được quy định tại Khoản 1 Điều 9 của Luật Cơ yếu) gửi về Công an tỉnh Đồng Nai để phối hợp kiểm tra.

b) Phân công cán bộ quản lý, sử dụng; xây dựng quy trình khắc phục sự cố; có chính sách, biện pháp quản lý, kiểm soát chặt chẽ, nghiêm ngặt đối với phương tiện, thiết bị có lưu trữ bí mật nhà nước.

c) Quán triệt, giáo dục nâng cao ý thức về vấn đề bảo vệ bí mật nhà nước và an toàn an ninh thông tin trên địa bàn tỉnh; nghiên cứu và chỉ đạo thực hiện

theo các quy định như Pháp lệnh Bảo vệ bí mật nhà nước, Luật Cơ yếu, Nghị định số 33/2002/NĐ-CP ngày 28/3/2002 của Chính phủ Quy định chi tiết thi hành Pháp lệnh Bảo vệ bí mật nhà nước, Quyết định số 34/2009/QĐ-UBND ngày 21/5/2009 của UBND tỉnh về ban hành Quy chế đảm bảo an toàn, an ninh thông tin trong lĩnh vực ứng dụng công nghệ thông tin của các cơ quan, đơn vị quản lý hành chính nhà nước trên địa bàn tỉnh Đồng Nai

2. Cá nhân sử dụng có trách nhiệm:

a) Quản lý, kiểm soát chặt chẽ, nghiêm ngặt đối với phương tiện, thiết bị có chứa thông tin bí mật nhà nước; tuân thủ các quy định hiện hành về bảo vệ bí mật nhà nước và an toàn, an ninh thông tin.

b) Mọi thông tin có nội dung liên quan đến bí mật nhà nước được truyền và lưu trữ trên các phương tiện thông tin, thiết bị điện tử viễn thông, tin học phải được mã hóa theo quy định về cơ yếu.

c) Không sử dụng thiết bị điện tử, máy tính có kết nối Internet (kể cả lúc kết nối và không kết nối) để soạn thảo, lưu trữ, sao chép, in ấn các văn bản có chứa nội dung bí mật nhà nước hoặc sử dụng internet để gửi các loại văn bản có chứa nội dung bí mật nhà nước từ nơi này sang nơi khác; không được lưu trữ các văn bản, tài liệu mật vào máy tính cá nhân và các thiết bị lưu trữ khác không an toàn.

d) Không được mang micro vô tuyến và điện thoại di động, các thiết bị 3G, thiết bị có tính năng ghi âm, thu phát tín hiệu trong các cuộc họp có nội dung bí mật nhà nước dưới mọi hình thức. Không trao đổi thông tin có nội dung bí mật nhà nước qua bộ đàm, điện thoại di động, máy fax, trên Internet dưới bất kỳ hình thức nào.

đ) Không sử dụng các trang thiết bị kỹ thuật thông tin liên lạc do các tổ chức, cá nhân nước ngoài tài trợ, tặng để phục vụ cho hoạt động công vụ khi chưa được kiểm tra, kiểm định.

3. Công an tỉnh có trách nhiệm:

a) Chủ trì xây dựng quy trình thủ tục kiểm tra, dán tem kiểm định; hướng dẫn các đơn vị quản lý, sử dụng sau khi được kiểm tra để bảo vệ thông tin bí mật nhà nước.

b) Chuẩn bị điều kiện về cơ sở vật chất kỹ thuật, nhân lực để triển khai thực hiện kiểm tra.

c) Phối hợp với Sở Thông tin và Truyền thông và các đơn vị liên quan hướng dẫn, kiểm tra, đôn đốc các đơn vị, địa phương trong việc thực hiện Chỉ thị này; báo cáo kết quả thực hiện Chỉ thị này cho UBND tỉnh.

4. Sở Thông tin và Truyền thông có trách nhiệm:

Chủ trì, phối hợp với Văn phòng UBND tỉnh, Công an tỉnh và các đơn vị có liên quan tiến hành công tác kiểm tra việc thực hiện Chỉ thị này tại các đơn vị. Kế hoạch kiểm tra được lồng ghép vào kế hoạch kiểm tra hàng năm theo Quyết

định số 34/2009/QĐ-UBND ngày 21/5/2009 của UBND tỉnh về ban hành Quy chế đảm bảo an toàn, an ninh thông tin trong lĩnh vực công nghệ thông tin của các cơ quan, đơn vị quản lý hành chính nhà nước trên địa bàn tỉnh Đồng Nai.

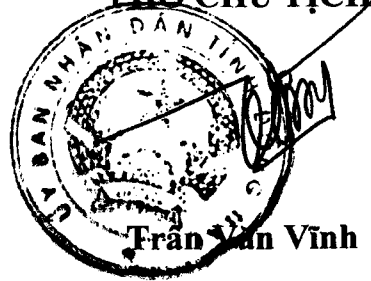
Chủ tịch UBND tỉnh yêu cầu Giám đốc các Sở, ban, ngành; Chủ tịch UBND các huyện, thị xã Long Khánh, thành phố Biên Hòa phối hợp chặt chẽ với Công an tỉnh thực hiện nghiêm túc Chỉ thị này nhằm đảm bảo công tác bảo vệ bí mật nhà nước đạt kết quả tốt.

Chỉ thị này có hiệu lực kể từ ngày 01/6/2013./.

Nơi nhận:

- VP TW Đảng;
- Thường trực Tỉnh ủy;
- Thường trực UBND tỉnh;
- Chủ tịch và các Phó Chủ tịch UBND tỉnh;
- Các cơ quan Đảng, Đoàn thể, Mặt trận Tổ quốc;
- Các Sở, ban ngành;
- Chủ tịch UBND các huyện, TX.Long Khánh, TP.Biên Hòa;
- Chánh, các Phó Văn phòng UBND tỉnh;
- Lưu VT (TTTH, HC-TC, NC).

**TM. ỦY BAN NHÂN DÂN
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH**



Trần Văn Vĩnh