VIỆN KIỂM SÁT NHÂN DÂN TỐI CAO

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

Số: 03 /CT-VKSTC

Hà Nội, ngày 03 tháng 07 năm 2017

CHỈ THỊ
Về tăng cường công tác đảm bảo an ninh, an toàn thông tin trong ngành Kiểm sát nhân dân

Thời gian qua, qua kiểm tra, các cơ quan chức năng đã xác định nhiều thiết bị kỹ thuật không đảm bảo an ninh và an toàn thông tin; phát hiện hàng trăm lỗ hổng bảo mật và mã độc nguy hiểm, trong đó có nhiều loại mã độc thực hiện hoạt động gián điệp, thu thập thông tin, kết nối, trao đổi dữ liệu với máy chủ điều khiển ở nước ngoài; phát hiện nhiều tài liệu thuộc danh mục bí mật nhà nước được lưu trữ, soạn thảo trên máy tính kết nối mạng Internet...

Tình hình an ninh, an toàn thông tin ở nhiều đơn vị trong ngành Kiểm sát nhân dân chưa tốt. Về nhận thức, đa số lãnh đạo, công chức, viên chức còn coi nhẹ an ninh, an toàn thông tin, việc sử dụng các phần mềm không có bản quyền, sử dụng các dịch vụ thư điện tử miễn phí (gmail, yahoo...) để trao đổi tài liệu chuyên môn còn phổ biến; không kiểm tra thiết bị trước khi sử dụng, không sử dụng phần mềm diệt virus; kinh phí đầu tư cho bảo đảm an ninh, an toàn thông tin trong ngành Kiểm sát nhân dân còn hạn chế, chưa đáp ứng yêu cầu...

Để nâng cao khả năng đảm bảo an ninh, an toàn thông tin trong ngành Kiểm sát nhân dân, Viện trưởng Viện kiểm sát nhân dân tối cao yêu cầu:

1. Thủ trưởng đơn vị thuộc Viện kiểm sát nhân dân tối cao, Viện trưởng Viện kiểm sát nhân dân cấp cao, Viện trưởng Viện kiểm sát quân sự Trung ương, Viện trưởng Viện kiểm sát nhân dân tỉnh, thành phố trực thuộc Trung ương, Viện trưởng Viện kiểm sát nhân dân cấp huyện, trong phạm vi nhiệm vụ của mình:

a) Tuyên truyền, nâng cao nhận thức, trách nhiệm cho lãnh đạo, công chức, viên chức về công tác đảm bảo an ninh, an toàn thông tin. Quán triệt và thực hiện nghiêm túc các quy định về an ninh, an toàn thông tin.

b) Tổ chức kiểm tra, rà soát, đánh giá bảo đảm an ninh, an toàn thông tin của hệ thống thông tin, máy chủ, máy trạm, thiết bị mạng, phần cứng, phần mềm hệ thống, phần mềm ứng dụng... Áp dụng các biện pháp, giải pháp để dò tìm và phát hiện kịp thời các điểm yếu, lỗ hổng về mặt kỹ thuật của hệ thống công nghệ thông tin. Thường xuyên kiểm tra, phát hiện những kết nối, trang thiết bị và phần mềm cài đặt bất hợp pháp vào mạng Internet.

c) Triển khai các giải pháp đảm bảo an toàn thông tin đối với thiết bị công nghệ thông tin, mạng máy tính như sau:

- Kiểm soát truy cập đối với mạng máy tính; máy tính phải cài đặt mật khẩu, gỡ bỏ các chương trình không cần thiết, kích hoạt chức năng tường lửa bảo vệ cá nhân, các phần mềm ứng dụng, hệ điều hành, phần mềm điều khiển thường xuyên cập nhật phiên bản, các bản vá mới nhất. Không sử dụng những phiên bản hệ điều hành, phần mềm đã lỗi thời không được nhà sản xuất hỗ trợ kỹ thuật. Từng bước có kế hoạch cài đặt 100% máy trạm có bản quyền hệ điều hành và phần mềm diệt virus. Trước mắt, máy chủ, máy tính soạn thảo tài liệu mật, máy tính truyền file phải được cài đặt hệ điều hành bản quyền và phần mềm diệt virus có bản quyền; máy tính soạn thảo, lưu trữ tài liệu mật tuyệt đối không được kết nối mạng Internet, mạng nội bộ. Ghi lại nhật ký truy cập của máy chủ để xác định nguyên nhân, thiếu sót và đánh giá mức độ thiệt hại khi xảy ra lộ, lọt thông tin bí mật, thiết lập hệ thống tường lửa vào, ra.

- Quản lý chặt chẽ việc sử dụng thiết bị lưu trữ ngoài (USB, thẻ nhớ, ổ cứng di động...); không được sử dụng các thiết bị có lưu trữ tài liệu mật để kết nối với máy tính truy cập Internet.

- Đối với thiết bị mạng cần phải cấu hình, thiết lập chế độ làm việc để hệ thống hoạt động an toàn, phát huy tác dụng.

- Đối với mạng không dây (WIFI), người dùng phải cài đặt mật khẩu mạnh và không để tính năng tự động kết nối.

- Phòng chống mã độc (khi lây lan vào máy tính có thể lấy cắp dữ liệu, theo dõi hoạt động, bị lợi dụng tấn công đối tượng khác và phá hoại dữ liệu của người dùng) bằng cách: không mở các tệp tin đính kèm thư điện tử nhận được từ một người lạ, không sử dụng các phần mềm bẻ khóa, không có bản quyền, không truy cập các trang web không liên quan đến công việc…

- Không sử dụng dịch vụ trực tuyến trên mạng Internet để lưu trữ tài liệu thuộc bí mật nhà nước; việc trao đổi thông tin bí mật nhà nước trên mạng phải thực hiện theo qui định tại Khoản 1 Điều 9 Luật Cơ yếu: "Thông tin bí mật nhà nước được truyền bằng các phương tiện thông tin, viễn thông phải được mã hóa bằng mật mã của cơ yếu". Đẩy mạnh việc triển khai, sử dụng chứng thực chữ ký số tất cả các văn bản điện tử của cơ quan.

- Việc trao đổi văn bản, tài liệu điện tử của cơ quan (kể cả tài liệu tham khảo) chỉ thực hiện trên hệ thống phần mềm quản lý văn bản và hồ sơ công việc đã được triển khai hoặc sử dụng hệ thống thư điện tử công vụ của Ngành hoặc trên các phần mềm ứng dụng của Ngành; không sử dụng hòm thư điện tử cá nhân đăng ký ở các dịch vụ thư điện tử miễn phí như gmail, yahoo... để trao đổi tài liệu chuyên môn.

d) Xây dựng và triển khai các phương án phòng ngừa:

- Tăng cường bảo mật các website, phần mềm tự xây dựng của đơn vị bằng cách thức bảo mật nhiều lớp (lớp mạng, lớp ứng dụng, lớp cơ sở dữ liệu).

- Thường xuyên tổ chức kiểm tra, đánh giá công tác an ninh, an toàn thông tin đối với hệ thống thông tin của cơ quan, đơn vị để phát hiện và xử lý kịp thời các sự cố.

- Đối với phần mềm ứng dụng, cán bộ quản trị cấp quyền theo đúng đối tượng qui định. Người sử dụng phải giữ bí mật tài khoản được giao, không để chế độ tự động đăng nhập, không lưu mật khẩu cho đăng nhập lần sau.

- Khi họp trực tuyến có nội dung bảo mật cần phải bật chức năng mã hóa cuộc họp.

- Khi phát hiện hoặc nghi vấn sự cố về an ninh, an toàn thông tin mạng trong hệ thống thông tin của cơ quan, phải khẩn trương triển khai các giải pháp kỹ thuật để khắc phục và kịp thời báo cáo Lãnh đạo đơn vị và Viện kiểm sát nhân dân tối cao (Cục Thống kê tội phạm và Công nghệ thông tin).

e) Khi đầu tư trang thiết bị CNTT phải đảm bảo nguồn gốc xuất xứ rõ ràng; trước khi sử dụng phải kiểm tra thiết bị để chắc chắn không bị cài đặt các phần mềm gián điệp.

2. Cục Thống kê tội phạm và Công nghệ thông tin:

a) Hướng dẫn, kiểm tra các đơn vị, Viện kiểm sát địa phương về an ninh, an toàn thông tin.

b) Chủ trì, phối hợp với các cơ quan liên quan xây dựng các quy chế về quản lý, sử dụng hệ thống công nghệ thông tin trong toàn Ngành.

c) Chủ trì, phối hợp với các cơ quan có liên quan tham mưu, đề xuất Viện trưởng Viện kiểm sát nhân dân tối cao đầu tư trang bị các thiết bị, phần mềm bảo mật chuyên dùng để đáp ứng phương tiện, công cụ nâng cao năng lực đảm bảo an ninh, an toàn thông tin trong hoạt động của ngành Kiểm sát nhân dân.

d) Xây dựng chương trình, kế hoạch và tổ chức đào tạo bồi dưỡng kiến thức, kỹ năng về an ninh, an toàn thông tin cho đội ngũ cán bộ chuyên trách công nghệ thông tin của các đơn vị trong ngành Kiểm sát nhân dân.

3. Cục Kế hoạch - Tài chính:

Chủ trì, phối hợp với Cục Thống kê tội phạm và Công nghệ thông tin, các đơn vị liên quan tham mưu, báo cáo Lãnh đạo Viện kiểm sát nhân dân tối cao nguồn kinh phí đảm bảo cho các hoạt động đảm bảo an ninh, an toàn thông tin mạng tại các đơn vị trong ngành Kiểm sát nhân dân.

Thủ trưởng đơn vị thuộc Viện kiểm sát nhân dân tối cao, Viện trưởng Viện kiểm sát nhân dân cấp cao, Viện trưởng Viện kiểm sát quân sự Trung ương, Viện trưởng Viện kiểm sát nhân dân các tỉnh, thành phố trực thuộc Trung ương, Viện trưởng Viện kiểm sát nhân dân cấp huyện trong phạm vi quản lí của mình, tổ chức chỉ đạo thực hiện nghiêm túc chỉ thị này./.

Nơi nhận:
- Lãnh đạo VKSNDTC;
- Các đơn vị thuộc VKSNDTC;
- Các VKSND cấp cao, VKSQS TW, VKSND tỉnh, thành phố trực thuộc TW;
- Bộ Thông tin và truyền thông (để biết);
- Lưu: VT, Cục 2.

VIỆN TRƯỞNG

Lê Minh Trí