HỌC VIỆN BÁO CHÍ VÀ TUYÊN TRUYỀN
VĂN PHÒNG
*

ĐẢNG CỘNG SẢN VIỆT NAM

Hà Nội, ngày tháng năm 2023

TỔNG HỢP Ý KIẾN
Về xây dựng Quy định, Quy trình bảo mật hệ thống CNTT tại Học viện Báo chí và Tuyên truyền

1. Tăng cường công tác tuyên truyền, phổ biến về tình hình và các nguy cơ mất an toàn thông tin đối với người lãnh đạo, chỉ huy cũng như cán bộ, nhân viên trong việc sử dụng công nghệ thông tin - viễn thông;

2. Nâng cao năng lực đội ngũ chuyên trách về bảo mật hệ thống CNTT;

Hoạt động tấn công không gian mạng rất đa dạng như: làm mất kết nối Internet; giả mạo, đánh sập các website; phát tán mã độc tống tiền; tấn công có chủ đích.... Không những thế, các hoạt động này thường có xu hướng ngày càng tinh vi và biến đổi khó lường. Vì vậy, việc nâng cao năng lực đội ngũ chuyên trách phải được thực hiện bằng các hình thức đa dạng, phong phú và linh hoạt.

Mục tiêu nhằm trang bị cho cán bộ kỹ thuật kiến thức, kỹ năng, kinh nghiệm thực tế và sự nhanh nhạy, ứng phó xử lý tình huống khi xảy ra tấn công mạng, nguy cơ, mối đe dọa về an toàn đối với các hệ thống thông tin, góp phần tuyên truyền, phổ biến nâng cao nhận thức và trách nhiệm của các cơ quan, tổ chức và người sử dụng về an toàn thông tin. Qua đó, giúp cán bộ kỹ thuật có kinh nghiệm thực tiễn để tự tin hơn khi ứng phó, xử lý trước các cuộc tấn công mạng vào hệ thống chuyên ngành.

3. Nâng cao ý thức phòng tránh, tự vệ và sử dụng biện pháp kỹ thuật của người dùng cuối;

Ý thức chính trị, trách nhiệm, nghĩa vụ của cá nhân đối với nhiệm vụ bảo vệ không gian mạng cần được nâng cao. Mỗi người dùng cần nghiên cứu và sử dụng tốt các biện pháp kỹ thuật bảo đảm ATTT như: thường xuyên cập nhật phần mềm, hệ điều hành máy tính cá nhân lên phiên bản mới nhất; bảo vệ tài khoản cá nhân bằng xác

thực mật khẩu 2 lớp; tạo thói quen quét virus trước khi mở file; thực hiện sao lưu dự phòng trên ổ cứng ngoài, mạng nội bộ hoặc trên các dịch vụ lưu trữ đám mây.

Mỗi người dùng cũng cần tuân thủ các quy tắc an toàn thông tin như: tuyệt đối không tải các file đính kèm hoặc nhấp vào đường link không rõ nguồn gốc; Hạn chế kết nối các thiết bị ngoại vi (USB, ổ cứng) với máy tính cá nhân ở cơ quan...

4. Tăng cường các biện pháp nghiệp vụ, tổ chức diễn tập bảo đảm an toàn an ninh thông tin cho các Hệ thống thông tin của Học việnố; phối hợp chặt chẽ với các đơn vị lực lượng để chủ động phòng ngừa, xử lý các tình huống phát sinh trong lĩnh vực an toàn an ninh thông tin đối với các cơ sở hạ tầng mạng và Hệ thống thông tin;

5. Về kỹ thuật và công nghệ phải tăng cường các giải pháp kỹ thuật bảo đảm an toàn và bảo mật thông tin: từng bước triển khai các sản phẩm mã hóa thông tin; áp dụng giải pháp chứng thực điện tử và chữ ký số; triển khai hệ thống giám sát an toàn thông tin trên các mạng công nghệ thông tin trọng yếu;

VĂN PHÒNG