TRƯỜNG ĐẠI HỌC SƯ PHẠM KỸ THUẬT VĨNH LONG
PHÒNG QUẢN TRỊ - THIẾT BỊ

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

Vĩnh Long, ngày 17 tháng 02 năm 2017

CHÍNH SÁCH, THỦ TỤC BẢO MẬT VÀ AN TOÀN THÔNG TIN

Căn cứ Quy định đảm bảo an toàn, bảo mật thông tin về đảm bảo chất lượng bên trong thuộc lĩnh vực công nghệ thông tin tại Trường Đại học Sư phạm Kỹ thuật Vĩnh Long;

Phòng Quản trị - Thiết bị ban hành một số Chính sách bảo mật và an toàn đối với hệ thống thông tin:

1. Chính sách bảo mật đối với hạ tầng mạng

- Xây dựng tài liệu mô tả toàn bộ hệ thống thông tin toàn trường. Trong tài liệu này phải đề cập đến các thiết bị, các kết nối giữa các thiết bị, các địa chỉ IP, MAC trên các thiết bị, định tuyến sử dụng trong mạng….
- Hệ thống mạng phải được bảo mật: Cần phải quản lý chi tiết việc truy cập vào dịch vụ mạng của các user như: các ứng dụng mạng được phép sử dụng, các trang web được phép truy cập, thời gian truy cập, ngăn chặn download các định dạng file cụ thể để tránh làm giảm hiệu năng mạng…. Ngoài ra , phải giám sát được hiệu suất của hệ thống mạng của trường, đảm bảo băng thông.
- Chính sách đảm bảo an toàn cho vùng DMZ cụ thể ở đây là web server nhằm hạn chế những cuộc tấn công từ bên ngoài vào như DOS, DDOS, spame email….
- Chính sách đảm bảo an toàn cho vùng server nội bộ: Các server nội bộ không public ra ngoài nên tránh được các cuộc tấn công từ bên ngoài. Các server nội bộ nằm trong một vùng Vlan riêng biệt phân quyền cho phép những người dùng nào có thể truy cập vào Vlan này.
- Sao lưu dữ liệu thường xuyên theo kế hoạch, sử dụng công cụ hỗ trợ sao lưu.
- Quản lý các file cấu hình của các thiết bị trong mạng: các file cấu hình trên router, switch, access point cần phải được quản lý sao lưu.
- Quản lý các đường định tuyến, các bảng routing table trên router cũng như switch nhằm tránh bị loop.
- Chính sách cho sinh viên: Có thể sử dụng mạng không dây. Hệ thống này nằm trong một VLAN riêng biệt và người dùng trong VLAN này chỉ có thể ra ngoài internet mà ko được phép truy cập đến các tài nguyên nội bộ như các server, các máy tính trong mạng cũng như các máy in, máy fax.

2. Chính sách quản lý thiết bị công nghệ thông tin

Tất cả cán bộ, giảng viên, sinh viên có quyền truy nhập vào hệ thống máy tính phải tuân thủ các chính sách được đề ra ở dưới đây nhằm bảo vệ hệ thống máy tính, mạng máy tính, sự toàn vẹn dữ liệu và an toàn thông tin của trường.

- Các cá nhân làm việc ở ví trí chứa thiết bị có trách nhiệm bảo quản, giám sát, bảo vệ các thiết bị đó.

- Các cá nhân được ủy quyền sử dụng các thiết bị di động, lưu trữ có trách nhiệm bảo quản các thiết bị đó. Không sử dụng các thiết bị đó lưu trữ các thông tin nội bộ, nhạy cảm mà không có sự cho phép.

3. Chính sách bảo mật thông tin

- **Đánh nhãn các thiết bị lưu trữ, tài liệu trên giấy tờ**: Tùy nhãn của chúng mà được lưu trữ trong những khu vực khác nhau.
- **Sử dụng, truy xuất các thiết bị lưu trữ: USB, Đĩa Mềm, CD/DVD**
  - Thông tin bình thường: có thể tùy ý sử dụng.
  - Thông tin nhạy cảm: Cần phải có sự đồng ý của cấp trên mới có thể sử dụng hay mang ra ngoài.
  - Thông tin mật: Cần được xác nhận của Phó Hiệu trưởng trở lên.
  - Thông tin tuyệt mật: Chỉ có Hiệu trưởng mới có thể quyết định.
- **Hủy dữ liệu trong các thiết bị: USB, Đĩa Mềm, CD, Băng Từ, HDD**
  - Thông tin bình thường: Xóa bình thường, không bắt buộc phải format.
  - Thông tin nhạy cảm: Thiết bị lưu trữ cần được format lại.
  - Thông tin mật: Phải ghi đè nhiều lần đảm bảo không thể khôi phục lại.
  - Thông tin tuyệt mật: Hủy cả dữ liệu lẫn thiết bị.

4. Chính sách quản lý khu vực

- **Mục tiêu của chính sách:**
  - Ngăn chặn các truy cập trái phép về vật lý, gây thiệt hại cho các thiết bị.
  - Những thiết bị chứa dữ liệu quan trọng,nhạy cảm của tổ chức phải được đặt trong vùng bảo mật có các cơ chế quản lý về an ninh, kiểm soát việc ra vào ở các khu vực đó.
  - Xác định rõ những nguy cơ, rủi ro có thể xảy ra từ đó có những quy định cụ thể phù hợp.
- **Các giải pháp đề xuất cụ thể:**
  - Đầu tiên về quản lý theo khu vực thì vấn đề đầu tiên là tách biệt về không gian, dành riêng một phòng để đặt các thiết bị quan trọng như server, các thiết bị đắt tiền.
  - Quản lý, giám sát việc ra vào tại những khu vực riêng biệt này. Chỉ cho phép những người có trách nhiệm liên quan mới được phép vào. Mỗi lần ra vào phải có ghi chép thời gian, lý do (bảo trì, sữa chữa,…). Lắp đặt các camera theo dõi và các hệ thống báo động để tránh việc đột nhập trái phép.
  - Lắp đặt máy quét vân tay kiểm tra trước khi vào nếu thấy cần mức độ bảo mật cao hơn.
  - Trong điều kiện kỹ thuật bị giới hạn, những thiết bị, dịch vụ không trực tiếp được quản lý bởi tổ chức mà bởi bên thứ ba nên để ở khu vực riêng.
  - Quản lý ra vào theo thời gian cụ thể là trong giờ hành chính thì mới có thể vào, ngoài giờ hành chính, mọi hành vi ra vào những khu vực trên phải có sự dám sát của người đại diện cao nhất trong tổ chức hoặc người được ủy quyền.

- Bảo vệ khu vực khỏi những nguy cơ như cháy nổ, ngập nước. Các chất dễ bắt lửa, gây cháy nổ phải để cách xa các khu vực được bảo vệ này.
- Các thiết bị dự phòng phải đặt cách xa nhau để tránh hư hỏng hàng loạt khi xảy ra sự cố.
- Trong các khu vực cần có các hệ thống báo cháy, bình cứu hỏa.

5. Chính sách quản lý truy cập

- **Mục tiêu của chính sách:**
  - Kiểm soát thông tin truy cập.
  - Đảm bảo người truy cập có quyền, tránh truy cập trái phép.
  - Áp đặt trách nhiệm cho người dùng với các tài khoản truy cập để tránh việc mất mát thông tin.
  - Ngăn chặn sử dụng trái phép các dịch vụ mạng từ bên trong lẫn bên ngoài.
  - Kiểm soát truy cập trái phép vào hệ điều hành.
  - Thiết lập các quyền được phép cho người dùng trên các ứng dụng.
  - Đảm bảo an toàn khi truy cập từ xa qua các thiết bị di động.
- **Giải pháp cụ thể:**
  - Quy định rõ quy tắc kiểm soát truy cập và quyền cho từng người và từng nhóm. Tạo các chính sách cho các user và OU trong domain theo từng phòng ban cụ thể. Qua đó đưa ra các mức độ cảnh cáo đối với các user cố tình sai quy định.
  - Xác định quyền cụ thể trên file server cho các phòng ban thông qua NTFS permission.
  - Quy định phòng ban này không được phép truy cập vào tài nguyên, tài liệu của phòng ban khác. Điều này tiềm ẩn nguy cơ về đánh cắp thông tin nên phải có mức độ cảnh cáo phù hợp.
  - Cấp ID cho nhân viên khi mới vào làm và xác định rõ các quyền mà user đó được phép làm và quy trách nhiệm về các hành động của user đó gây ra.
  - Cấp quyền phù hợp với user dựa vào vị trí của cán bộ, giảng viên trong đơn vị, và nhu cầu của công việc đó, và mức độ bảo mật của tổ chức.
  - Có văn bản ký kết giữa nhân viên được cấp ID với tổ chức về việc hiểu rõ các quyền mà ID đó được phép.
  - Khi các ID được tạo ra đảm bảo nó bị cấm trước khi được ký kết các điều khoản với người dùng.

Phòng Quản trị - Thiết bị

Nguyễn Quang Tuyến